

UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA EN COMPUTACION



**“INVESTIGACIÓN DE LA CONSECUENCIA DEL DESARROLLO
DE LA COMPUTACIÓN CUÁNTICA EN LOS SISTEMAS DE
SEGURIDAD QUE USAN CRIPTOGRAFÍA ASIMÉTRICA
EN EL SALVADOR”.**

**TRABAJO DE GRADUACIÓN PARA OPTAR
AL GRADO DE INGENIERO EN CIENCIAS
DE LA COMPUTACIÓN**

PRESENTADO POR:

**RODOLFO ANTONIO ALBERTO LUNA
HUGO NELSON AVILES LOPEZ
ROSA VILMA JOVEL MELARA**

CIUDADELA DON BOSCO

SEPTIEMBRE 2003

**UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA EN COMPUTACIÓN**



AUTORIDADES

RECTOR:

ING. FEDERICO MIGUEL HUGUET RIVERA

SECRETARIA GENERAL:

HNO. MARIO HOLMOS

DECANO DE LA FACULTAD DE INGENIERIA:

ING. CARLOS GUILLERMO BRAN

ASESOR DE TRABAJO DE GRADUACIÓN:

ING. CARLOS HUMBERTO LOPEZ LINARES

JURADO EVALUADOR:

ING. REINA ELIZABETH DE ALVARADO

ING. CARLOS ALFREDO HERCULES

ING. ARNOLDO RIVAS

UNIVERSIDAD DON BOSCO
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA EN COMPUTACIÓN



**“INVESTIGACIÓN DE LA CONSECUENCIA DEL DESARROLLO
DE LA COMPUTACIÓN CUÁNTICA EN LOS SISTEMAS DE
SEGURIDAD QUE USAN CRIPTOGRAFÍA ASIMÉTRICA
EN EL SALVADOR”.**

JURADO EVALUADOR DE TRABAJO DE GRADUACIÓN

Licda. Reina Elizabeth de Alvarado
Jurado

Ing. Carlos Alfredo Hércules Castro
Jurado

Ing. Arnoldo Rivas
Jurado

Ing. Carlos Humberto López
Asesor

AGRADECIMIENTOS

A Dios Todopoderoso, por darme la vida, por acompañarme durante cada paso que doy, por ayudarme a seguir adelante en todos los momentos difíciles que existieron durante esta etapa y durante mi vida, a ti Dios te doy las gracias por haberme dado unos excelentes amigos para realizar el proceso de trabajo de graduación. Gracias Dios por todo lo hermoso que eres con todas las personas y bendice a todos aquellos que estuvieron cerca de nosotros dando ánimos y también a los que no estuvieron cerca pero nos apoyaban con sus oraciones.

A Mis Padres, Rodolfo Antonio Alberto Hernández y María Antonieta Luna de Alberto, por enseñarme que en la vida hay que tener éxitos, pero sin olvidarnos de lo más esencial, éxitos junto a nuestro amigo Jesucristo, y amor a Dios y a Nuestra Madre María Santísima. Por entregarme siempre todo su amor y cariño, por haberme apoyado durante todo este proceso y todas las situaciones de mi vida, por sus regaños, consejos, por toda esa sabiduría que me han transmitido. Gracias Padres por hacer tan excelente su labor en algo que no existe un manual, más que solo el verdadero sentimiento del amor que los ha llevado a desempeñar bien el papel de Padres.

A Rosy y Hugo, gracias por todas las situaciones que ocurrieron durante este proceso, regaños, consejos, alegrías, tremendas preocupaciones, etc., que me enseñaron más acerca de la importancia de lo que es tener unos verdaderos amigos y no solamente unos compañeros, gracias por dar todo su cariño y comprensión, además por dar todo ese esfuerzo que incluyo varias desveladas que nos permitieron terminar una etapa más en nuestras vidas, alcanzándola con éxito. Disfruten amigos este nuevo éxito obtenido, pero siempre no se olviden de Jesucristo, les deseo bendiciones en las nuevas metas planteadas en su vida.

A Mi Tía Lupe, por haberme ayudado para poder finalizar el proceso de trabajo de graduación, por acompañarme siempre y estar pendiente de mí en cada momento de esta etapa.

A Mis Familiares, por estar pendiente de cada una de las etapas que abarcaron este proceso y darme palabras de animo para seguir adelante.

A Mis Amigos, por apoyarme en cada instante de este proceso, por la amistad incondicional que me brindan día a día, y darme esas palabras que son necesarias para seguir tomando fuerzas.

A Ing. Carlos Humberto López, nuestro asesor, por darnos siempre una guía para poder culminar con éxito nuestro trabajo de graduación, y además por ser un gran amigo que nos dio todo su apoyo.

A Ing. Jaime Anaya, nuestro tutor, por darnos el acompañamiento necesario para poder realizar cada uno de las partes que componen este proceso de trabajo de graduación.

A Todos los que forman parte de la Universidad Don Bosco, jefes, docentes, ordenanzas, vigilantes, secretarías, etc., porque realmente han representado un factor importante para alcanzar este éxito, ya que durante todo el tiempo en que nosotros estudiábamos y durante también este proceso de graduación, nos apoyado de diferentes maneras para llegar a concluirlo. Que Dios los bendiga a todos y los acompañe siempre.

Rodolfo Antonio Alberto Luna

A DIOS Todopoderoso, por darme la vida y toda su bondad siendo motivo de aliento e inspiración en todo mi recorrido.

A mi madre (QDDG): Ana Gladis López, que a pesar de su ausencia corporal siempre fue un gran motivo de inspiración.

A mis abuelos maternos (QDDG): Marco Antonio y Josefina, por su gran amor, paciencia y dedicación, ya que fueron ellos quienes desempeñaron el papel de padre y madre durante gran parte de mi vida, y a ellos debo gran parte de lo que ahora soy.

A mi hermano: Edgardo, por su apoyo incondicional durante toda mi vida.

A Helena Godoy y mis tías, María Elena, Ana Hilda, por su orientación, consejos, apoyo y bondad incondicionales.

A Dinora Flores y mi tía Ana María Lemus, por ser partícipes para poder alcanzar mi meta.

A Karen Reyna, por su amor, paciencia y apoyo incondicional.

A mis compañeros y amigos de Universidad: Joaquín, Rodolfo y Rosa Vilma, por todas las reuniones de estudios y apoyo mutuo que me brindaron durante los años en la Universidad y trabajo de graduación.

A mis primos y hermanos: Miguel, Karla, David, Leonardo y Francisco, por su apoyo y ayuda incondicional.

Hugo Nelson Avilés López

A DIOS Todopoderoso, por estar siempre conmigo, dándome fuerzas para seguir adelante, guiándome por el buen camino y ayudándome a obtener este éxito que representa la primera de mis grandes metas. Gracias Dios por todas las bondades que nos das, bendice a todos mis seres queridos y a todos aquellos que hicieron alguna oración por nosotros para que todo saliera bien.

Dedico este éxito obtenido a mis padres: Alfredo Jovel Rodríguez y Rosa Melara de Jovel, por haberme brindado todo su cariño y su gran esfuerzo por sacar adelante a mí y a mis hermanos, ya que nos han apoyado incondicionalmente. Papás infinitamente les agradezco todo lo que han hecho y por toda la confianza que han depositado en mí.

A mi abuelita (QDDG) María Isabel Merino: por haber sido un ejemplo de sabiduría, lucha y emprendimiento en la vida, porque sé que desde donde se encuentre me esta cuidando y bendiciendo siempre. **Gracias Mamaría.**

A mis hermanos Carlos, Luis y Jorge: por aguantarme en mis momentos más difíciles del trayecto de mi carrera y porque de alguna forma han aportado una ayuda incondicional para que este éxito pudiera ser realizado.

A mi tía Ing. Rosa Alicia Jovel: por haberme brindado su apoyo en el transcurso de mi carrera y haber estado siempre pendiente de mí, sirviéndome de ejemplo para recordarme que no debo darme por vencida ante circunstancias no gratas que siempre suceden en la vida. Gracias infinitas.

A mis demás familiares: por siempre estar pendientes y desear lo mejor de mí y que de alguna manera contribuyeron con esta meta.

A Hugo y Rodolfo: por haber puesto todo de su parte para que este éxito pudiera ser realizado, por haber demostrado su compañerismo y amistad

sincera, por haberme brindado su apoyo incondicional y sobre todo por aguantarme en tantas noches de desvelo.

A mis amigos y amigas: que con su amistad y apoyo incondicional me han demostrado que en esta vida todas nuestras metas pueden llegar a culminar en un éxito total. Yo les digo ánimos!! y sigamos adelante con fe y esperanza en Dios. A todos agradezco infinitamente.

Rosa Vilma Jovel Melara

INDICE

INTRODUCCIÓN.....	1
CAPÍTULO I. DEFINICIÓN Y OBJETIVOS.....	4
1.1 DEFINICIÓN DEL TEMA.....	4
1.2 ANTECEDENTES DEL TEMA.....	4
1.3 OBJETIVOS.....	9
1.3.1 OBJETIVO GENERAL.....	9
1.3.2 OBJETIVOS ESPECIFICOS.....	9
1.4 JUSTIFICACIÓN.....	10
1.5 DEFINICIÓN DE CONCEPTOS.....	11
1.5.1 CONCEPTOS BÁSICOS SOBRE CRIPTOGRAFÍA.....	11
1.5.2 CONCEPTOS BÁSICOS SOBRE COMPUTACIÓN CUANTICA.....	15
CAPÍTULO II. METODOLOGÍA.....	21
2.1 OBJETIVO.....	21
2.2 METODOLOGÍA DE INVESTIGACION.....	21
2.2.1 MÉTODO CIENTÍFICO.....	21
2.2.2 MÉTODO DEDUCTIVO.....	23
2.2.3 TIPO DE ESTUDIO.....	23
2.2.4 TÉCNICAS DE INVESTIGACIÓN.....	24
2.2.5 MARCO MUESTRAL.....	26
2.3 INTERPRETACION DE LOS RESULTADOS.....	28
CAPÍTULO III. MARCO TEÓRICO.....	30
3.1 FUNDAMENTOS TEÓRICOS DE LA CRIPTOGRAFÍA.....	30
3.1.1 TEORÍA DE LA INFORMACIÓN.....	30
3.1.2 INTRODUCCIÓN A LA COMPLEJIDAD ALGORÍTMICA.....	31
3.1.3 ALGORITMOS POLINOMIALES, EXPONENCIALES Y SUBEXPONENCIALES.....	35
3.1.4 FUNDAMENTOS DE ARITMÉTICA MODULAR.....	38
3.1.5 IMPORTANCIA DE LOS NÚMEROS PRIMOS.....	42
3.1.6 ALGORITMOS DE FACTORIZACIÓN.....	44
3.1.7 TESTS DE PRIMALIDAD.....	49
3.1.8 ANILLOS DE POLINOMIOS.....	51
3.2 ALGORITMOS DE CIFRADO ASIMÉTRICO.....	54
3.2.1 INTRODUCCIÓN.....	54
3.2.2 APLICACIONES DE LOS ALGORITMOS ASIMÉTRICOS.....	54
3.2.3 ALGORITMO RSA.....	57
3.3 OTROS ALGORITMOS ASIMÉTRICOS.....	60
3.3.1 ALGORITMO DE DIFFIE-HELLMAN.....	60
3.3.2 ALGORITMO DE ELGAMAL.....	62
3.3.3 ALGORITMO DE RABIN.....	62

3.3.4 ALGORITMO DSA.....	63
3.4 LOS PROTOCOLOS SSL Y TLS.....	65
3.5 METODOS DE AUTENTIFICACIÓN.....	77
3.6 FUNDAMENTOS TEÓRICOS DEL ALGORITMO DE SHOR.....	84
3.6.1 ALGORITMO CUÁNTICO DE FACTORIZACIÓN DE SHOR.....	84
CAPÍTULO IV. DESARROLLO DE LA INVESTIGACIÓN	88
4.1 FORMULACION DE HIPÓTESIS.....	88
4.2 FUNCIONAMIENTO DE SISTEMA CRIPTOGRAFICO ASIMÉTRICO	89
4.2.1 CONFIGURACIÓN DEL SERVIDOR SEGURO APACHE HTTP CON RED HAT LINUX.....	89
4.2.2 CONFIGURACIÓN DEL SSL EN EL APACHE WEB SERVER PARA WIN32.....	102
4.2.3 GENERAR UNA PETICIÓN DE CERTIFICADO (CSR) EN UN SERVIDOR MICROSOFT IIS 5.X / 6.X.....	106
4.2.4 ¿ CÓMO OBTENER UN CERTIFICADO DIGITAL ?.....	115
4.2.5 AUTORIDADES DE CERTIFICACIÓN (AC).....	115
4.2.6 AUTORIDAD CERTIFICADORA EN EL SALVADOR.....	119
4.2.7 COSTOS PARA LA OBTENCIÓN DE CERTIFICADOS DIGITALES	123
4.3 CRIPTOANÁLISIS	125
4.3.1 CRIPTOANÁLISIS UTILIZANDO EL ALGORITMO DE SHOR.....	125
4.3.2 FUNCIONAMIENTO DE ALGORITMO CUANTICO DE SHOR.....	126
4.3.3 FLUJOGRAMA. ALGORITMO DE SHOR.....	128
4.3.4 EJEMPLO DEL ALGORITMO DE SHOR.....	129
4.3.5 CÓDIGO FUENTE DEL ALGORITMO DE SHOR.....	131
4.4 ANÁLISIS DE RESULTADOS (SOBRE EL IMPACTO EN LA EMPRESA SALVADOREÑA).....	134
4.4.1 INTERPRETACIÓN DE LOS RESULTADOS DE ENCUESTAS.....	134
4.4.2 ANÁLISIS DE LOS RESULTADOS OBTENIDOS.....	162
4.5 VALIDACIÓN DE RESULTADOS	166
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES.....	169
CONCLUSIONES	169
RECOMENDACIONES	175
GLOSARIO DE TERMINOS	179
BIBLIOGRAFÍA.....	186
CÁMARA DE COMERCIO E INDUSTRIA DE EL SALVADOR A TRAVÉS DE.....	7
RESPONSABILIDADES	19
EXCLUYENTES.....	20

ANEXOS	189
---------------------	------------

INTRODUCCIÓN

El documento tiene como objetivo principal determinar las consecuencias del desarrollo de la computación cuántica en los sistemas de seguridad que usan criptografía asimétrica en El Salvador, para lo cual se pretende dar la información necesaria para entender en forma básica el funcionamiento de lo que es la criptografía asimétrica, la computación cuántica y la gran relación que existe entre éstos tópicos, por lo que se dará una información precisa de lo que se quiere determinar con la investigación.

Capítulo I

Las definiciones y objetivos de la investigación.

La estructura del proyecto contiene en primer lugar los antecedentes del tema que se encuentra dividido en dos grandes partes:

- Los antecedentes de la computación cuántica y
- Los antecedentes de la criptografía

Se consideró así ya que a pesar de que los dos se encuentran relacionados, sus principios y estudios iniciales no dependen uno del otro.

En la parte de la justificación del tema se da a conocer la importancia del estudio de la computación cuántica, y la razón del porqué es necesario hacer una relación con los métodos de criptografía asimétrica.

Capítulo II.

Las partes correspondientes a la metodología de la investigación y las técnicas a utilizar, que se enfocan principalmente en lo que es la investigación, el desarrollo y el análisis se detallan en este capítulo.

Capítulo III.

En el marco teórico se presenta toda la teoría correspondiente a la Criptografía Asimétrica y a la Computación Cuántica, como también los fundamentos matemáticos correspondientes a los algoritmos y teoremas para poder tener un mayor entendimiento de los principios en que están basados métodos de cifrado y el algoritmo de Shor.

Capítulo IV.

En el desarrollo de la investigación primeramente se presenta la formulación de la hipótesis, a continuación se presentan los pasos necesarios para configurar un servidor web seguro, la generación de las llaves pública y privada, la generación del requerimiento de certificación; y luego como criptoanálisis la presentación de los pasos para evaluar el problema de la factorización de números primos del Algoritmo de Shor. Además se presenta la interpretación y el análisis de las encuestas realizadas.

Capítulo V.

Las conclusiones y las recomendaciones de la investigación.

Glosario de términos.

Las palabras o frases que han sido utilizadas en el documento.

Bibliografía.

Las referencias que han sido utilizadas para el desarrollo de la investigación.

Anexos.

Información que servirá de complemento para la apreciación y comprensión de la investigación.

CAPÍTULO I

DEFINICIÓN Y OBJETIVOS

CAPÍTULO I. DEFINICIÓN Y OBJETIVOS

1.1 DEFINICIÓN DEL TEMA

“Investigación de la consecuencia del desarrollo de la Computación Cuántica en los sistemas de seguridad que usan Criptografía Asimétrica en El Salvador”.

1.2 ANTECEDENTES DEL TEMA

Antecedentes de la Computación Cuántica:

La Computación Cuántica se refiere a los fenómenos que tendrá que enfrentar la tecnología de las computadoras cuando el tamaño de sus componentes (transistores, circuitos, etc.) rebase un límite inferior determinado, para el que las leyes de la física son fundamentalmente diferentes a las que se aplican en el mundo macroscópico.

A principios del siglo pasado (1900's), con el avance en el conocimiento de los mecanismos internos del átomo; físicos de la talla de Niels Bohr, Max Planck, Werner Heisenberg¹, etc. llegaron a la conclusión de que la física newtoniana - también llamada mecánica clásica- no podía aplicarse al mundo subatómico, en el cual las leyes del movimiento responden a principios diferentes que en ocasiones contradicen nuestro sentido común. Esto los llevó a fundar una nueva rama de la física: **La Mecánica Cuántica**.

Un ejemplo sencillo: la mecánica newtoniana es capaz de establecer con una gran precisión, la velocidad y la posición de objetos de mayor tamaño que el átomo; en este sentido se puede establecer con objetividad la trayectoria que por ejemplo siguen la Luna o el Sol, y ésta determinación es independiente del método de estudio empleado; es decir, la observación que se haga no influye

¹ Físicos, (Ver anexo 1)

en forma significativa en las conclusiones que se obtienen sobre el movimiento estudiado.

Sin embargo, cuando se trata de observar y estudiar objetos del tamaño del átomo o menores, la mecánica cuántica sostiene que es imposible hacer observaciones objetivas, en el sentido que no perturben de manera importante el objeto de estudio. Se aplica aquí un principio denominado ***Principio de Incertidumbre de Heisenberg***².

Este principio simplemente establece que hay un límite en la precisión de cualquier observación que se haga del mundo atómico o subatómico. En este sentido, se puede conocer con bastante precisión la posición actual de una partícula subatómica, pero a costa de perder precisión en el conocimiento de otras variables (por ejemplo su velocidad), ya que nuestra observación de su posición afecta de manera no controlable el equilibrio atómico (incluso una observación demasiado precisa podría destruirlo).

En forma inversa, se puede establecer con gran aproximación la velocidad de, por ejemplo, un electrón (el electrón es la partícula que transporta la electricidad), pero renunciando a conocer con precisión su posición actual o futura. En este sentido, las trayectorias objetivas a las que se está acostumbrado en la vida diaria, pierden validez en el mundo del átomo.

Lo anterior nos lleva a leyes fundamentalmente diferentes, leyes que se establecen en términos probabilísticos y ya no determinísticos. Así por ejemplo, el movimiento de un electrón ya no se describe mediante una trayectoria nítida (una línea recta o curva), sino que al considerarlo, el electrón se tiene que tratar no sólo como partícula, sino también como una **onda** que se propaga y cuya forma nos da información sobre las diferentes probabilidades de posición del

² Principio de Incertidumbre de Heisenberg. (Ver anexo 2)

electrón. Es un poco como si el electrón estuviera "desparramado" en el espacio: una parte aquí, otra más allá.

A lo largo del último medio siglo, las computadoras han ido duplicando su velocidad cada dos años, al tiempo que el tamaño de sus componentes se reducía a la mitad. Los circuitos actuales contienen transistores y líneas de conducción cuya anchura es sólo una centésima parte de la de un cabello humano. Las máquinas de nuestros días son millones de veces más potentes que sus rudimentarios antepasados a causa de tan explosivo progreso. Actualmente por ejemplo, IBM puede fabricar chips de un cuarto de micrón, conteniendo cerca de 200 millones de transistores.

El incremento del poder de las computadoras se debe esencialmente a la miniaturización incesante del componente más elemental de la computadora, el transistor. Cuando los transistores se reducen de tamaño y se logran integrar en un solo microchip se incrementa el poder computacional. Sin embargo, las técnicas de integración de microcircuitos están empezando a tropezar con sus límites.

La ciencia de la computación en busca de una alternativa más allá de la tecnología del transistor, ha iniciado el estudio de la mecánica cuántica y su aporte para la creación de nuevas computadoras. Es así como han surgido las disciplinas: Nano-Computación y Computación Mecánico-Cuántica.

Las nano-computadoras tendrán componentes cuyo funcionamiento se rigen por los principios de la mecánica cuántica, pero los algoritmos que ellas ejecuten probablemente no involucren un comportamiento cuántico; mientras que las computadoras cuánticas buscan una posibilidad más excitante, usar la mecánica cuántica en un nuevo tipo de algoritmo que sería fundamentalmente más poderoso que cualquier otro esquema clásico. Una computadora que

puede ejecutar este tipo de algoritmo, será una verdadera computadora cuántica.

Una Computadora Cuántica es un nuevo dispositivo que puede resolver ciertos problemas importantes muy eficazmente. Una computadora cuántica proporciona paralelismo masivo aprovechando la naturaleza exponencial de la mecánica cuántica. Una computadora cuántica puede almacenar una cantidad exponencial de datos, y realizar un número exponencial de operaciones usando recursos polinomiales. Este paralelismo cuántico no es fácil de aprovechar. Sin embargo, unos algoritmos cuánticos descubiertos en 1993 (Algoritmo de Shor) han creado un interés en el potencial de las computadoras cuánticas.

La computación cuántica tiene básicamente dos efectos en la tecnología de las computadoras:

- A nivel de hardware
- A nivel de los algoritmos utilizados

En términos de hardware, a medida que la información pase a ser representada por unas cuantas partículas subatómicas, (a diferencia de como se representa ahora mediante una gran cantidad de éstas a través de los diferenciales de voltaje en los componentes de la computadora), los dispositivos deberán de reconocer los fenómenos cuánticos, como por ejemplo: las partículas pueden tener varios estados atómicos a la vez (niveles de energía), pueden atravesar barreras aparentemente infranqueables, pueden seguir varias rutas a la vez, etc.

En relación con los algoritmos (procedimientos matemáticos para resolver problemas), la computación cuántica abre posibilidades antes no imaginadas: disminuciones exponenciales en el tiempo de procesamiento y realización de

operaciones en paralelo sin la necesidad de agregar procesadores a la máquina.

Antecedentes de la Criptografía:

La criptografía consiste básicamente en un sistema, llamado criptosistema, que encripta los mensajes antes de enviarlos y que los decripta al recibirlos. En el año 1976, y debido a la aparición de ordenadores digitales aparece el sistema, Data Encryption Standard (DES). Inspirado del sistema Lucifer cipher de IBM (1970). En 1977 es ratificado como Federal Information Processing Standard (FIPS) por el National Institute of Standards and Technology (NIST), el sistema DES fue el primero de los sistemas complejos que hoy conocemos. En 1981, se convierte en el estándar X3.92 de American National Standards Institute (ANSI). Los datos son encriptados en bloques de 64 bits usando una llave de 56 bits. El algoritmo transforma una entrada de 64 bits después de una serie de pasos, en una salida de 64 bits. Los mismos pasos, con la misma llave, son usados para descifrar y ese mismo año hacían su aparición Diffie y Hellman³ creadores del primer sistema basado en claves públicas. Finalmente es Phill Zimmermann quien crea el sistema Pretty Good Privacy (PGP)⁴ que es el sistema de encriptación más difundido y que puede ser descargado en forma gratuita de Internet. La aparición de la Red ha acelerado la expansión de la criptografía, sacándola de los centros de cálculo y llevándola a los ordenadores domésticos.

³ Diffie – Hellman : Creadores del algoritmo asimétrico. Solamente se puede utilizar para intercambiar claves simétricas. (Ver anexo 2).

⁴ PGP. Protocolo que permite cifrar y firmar mensajes de correo electrónico basándose en un sistema de claves públicas.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Determinar las consecuencias del desarrollo de la computación cuántica en los sistemas de seguridad que usan criptografía asimétrica en El Salvador, mediante un criptoanálisis, utilizando el algoritmo de Shor con la simulación de una computadora cuántica.

1.3.2 OBJETIVOS ESPECIFICOS

- Investigar los principios y fundamentos de la computación cuántica.
- Conocer el funcionamiento del algoritmo de Shor para ordenadores cuánticos.
- Investigar los principios y fundamentos de los algoritmos asimétricos de cifrado.
- Investigación de los métodos de encriptamiento utilizados por las empresas en El Salvador.
- Determinar las posibles consecuencias que provocaría el surgimiento de la computación cuántica y por ende el uso del algoritmo de Shor para ordenadores cuánticos en los sistemas criptográficos asimétricos utilizados en las empresas de El Salvador.
- Proporcionar mediante esta investigación, bases de referencia, estudio y aplicación a las empresas que utilizan métodos de encriptamiento asimétrico en El Salvador.

1.4 JUSTIFICACIÓN

Con la siguiente investigación se pretende informar a las empresas que utilizan sistemas criptográficos asimétricos las posibles consecuencias del surgimiento de la computación cuántica.

Dado que actualmente están emergiendo nuevas tendencias con relación a la tecnología informática, como lo es la computación cuántica, existe la necesidad de investigar; ya que sería de grandes beneficios saber cuales son las ventajas o desventajas que se tendrían al poner en práctica dicha tecnología aplicada a técnicas que se ven en problemas al no poder realizar operaciones con la tecnología actual o de operaciones que llegarían a ser obsoletas.

Tal es el caso del algoritmo de Shor para computadores cuánticos que resuelve el problema del Logaritmo Discreto y el Problema de Factorización, con lo cual la criptografía asimétrica actual quedaría obsoleta.

Ya que, las computadoras actuales son muy buenas para multiplicar grandes números; el computador cuántico no lo hará mucho mejor. Sin embargo aquellos procesos que requieran de operaciones repetitivas, pueden hacer uso del cómputo en paralelo.

La factorización de grandes números: Una computadora actual se estima que tardaría varios miles de millones de años para factorizar un número de 1000 dígitos, mientras que una computadora cuántica lo realizaría en 20 minutos.

Se considera enfocar la investigación en los algoritmos asimétricos de cifrado, porque presentan una gran ventaja con respecto a los algoritmos simétricos de cifrado, en los siguientes aspectos:

- Los algoritmos asimétricos emplean generalmente longitudes de clave mucho mayores que los simétricos.

- Los algoritmos asimétricos tienen claves diferentes para cifrado y descifrado, es decir, usan una clave pública para cifrar y una clave secreta para descifrar, de esa manera la intercepción de la clave pública es inútil para descifrar un mensaje.

1.5 DEFINICIÓN DE CONCEPTOS

1.5.1 CONCEPTOS BÁSICOS SOBRE CRIPTOGRAFÍA

CRIPTOGRAFÍA

La palabra criptografía (oculto + escritura) es definida por la Real Academia como: *"el arte de escribir mensajes con una clave secreta o de modo enigmático"*.⁵

Obviamente la criptografía hace años dejó de ser un arte para convertirse en una técnica, por lo que se le considera como: “La rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a diferentes tipos de criptosistemas que permiten asegurar cuatro aspectos fundamentales de la seguridad informática: confidencialidad, integridad, disponibilidad y no repudio de emisor y receptor”.⁶

Entre las disciplinas que engloba la criptografía cabe destacar la Teoría de la Información, la Complejidad Algorítmica y la Teoría de Números —o Matemática Discreta, que estudia las propiedades de los números enteros—.

⁵ LUCENA LOPEZ, Manuel José. Criptografía y seguridad en Computadores. Depto. Informática Universidad de Jaén. Edición virtual. España 2003

⁶ AGUIRRE, Jorge Ramiro. Curso Seguridad Informática y Criptografía. Universidad Politécnica de Madrid. 3ª Edición

CRIPTOSISTEMA

Un criptosistema, es un sistema que toma información, legible, intelegible para convertirlo en información no legible, inintelegible, o no entendible.

Definiremos un criptosistema como una quintupla (M; C; K; E; D), donde:

- **M** representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto plano, o plaintext) que pueden ser enviados.
- **C** representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- **K** representa el conjunto de claves que se pueden emplear en el criptosistema.
- **E** es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente
- **E_k** para cada valor posible de la clave k.
- **D** es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición:

$$D_k(E_k(m)) = m$$

es decir, que si tenemos un mensaje m, lo ciframos empleando la clave k y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original m.

Los criptosistemas se clasifican en dos tipos fundamentales:

Criptosistemas simétricos o de clave privada:

Existirá una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra por lo que la seguridad reside sólo en mantener dicha clave en secreto.

Criptosistemas asimétricos o de clave pública:

Cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública. Para ello usan funciones matemáticas de un solo sentido con trampa.

CRIPTOANÁLISIS

El criptoanálisis consiste en comprometer la seguridad de un criptosistema. Esto se puede hacer descifrando un mensaje sin conocer la llave, o bien obteniendo a partir de uno o más criptogramas la clave que ha sido empleada en su codificación. No se considera criptoanálisis el descubrimiento de un algoritmo secreto de cifrado; hemos de suponer por el contrario que los algoritmos siempre son conocidos.

Es evidente que cuando existe comunicación entre dos personas, ambos tienen la llave para cifrar y descifrar un texto, pero si ese texto es interceptado por una tercera persona, esta no conoce que tipo de encriptación se utilizó y menos la llave usada, por lo cual requiere realizar un análisis del criptosistema con el objeto de determinar la llave usada.

SEGURIDAD

El concepto de seguridad en la información es mucho más amplio que la simple protección de los datos a nivel lógico. Para proporcionar una seguridad real hemos de tener en cuenta múltiples factores, tanto internos como externos. En primer lugar habrá que caracterizar el sistema que va a albergar la información para poder identificar las amenazas, y en este sentido podemos hacer la siguiente subdivisión:

1. **Sistemas aislados.** Son los que no están conectados a ningún tipo de red. De unos años este arte se ha convertido en minoría, debido al auge que ha experimentado Internet.
2. **Sistemas interconectados.** Hoy por hoy casi cualquier ordenador pertenece a alguna red, enviando y recogiendo información del exterior casi constantemente. Esto hace que las redes sean cada día más complejas y supongan un peligro potencial que no puede en ningún momento ser ignorado.

En cuanto a las cuestiones de seguridad que hemos de fijar podemos clasificarlas de la siguiente forma:

1. Seguridad física. Englobaremos dentro de esta categoría a todos los asuntos relacionados con la salvaguarda de los soportes físicos de la información, más que de la información propiamente dicha. En este nivel están, entre otras, las medidas contra incendios y sobrecargas eléctricas, la prevención de ataques terroristas, las políticas de backup, etc. También se suelen tener en cuenta dentro de este punto aspectos relacionados con la restricción de acceso físico a las computadoras únicamente a personas autorizadas.

2. Seguridad de la información. En este apartado prestaremos atención a la preservación de la información frente a observadores no autorizados. Para ello podemos emplear tanto criptografía simétrica como asimétrica, estando la primera únicamente indicada en sistemas aislados, ya que si la empleáramos en redes, al tener que transmitir la clave por el canal de comunicación, estaríamos asumiendo un riesgo excesivo.
3. Seguridad del canal de comunicación. Los canales de comunicación rara vez se consideran seguros. Debido a que en la mayoría de los casos escapan a nuestro control, ya que pertenecen a terceros, resulta imposible asegurarse totalmente de que no están siendo escuchados o intervenidos.
4. Problemas de autenticación. Debido a los problemas del canal de comunicación, es necesario asegurarse de que la información que recibimos en la computadora viene de quien realmente creemos que viene. Para esto se suele emplear criptografía asimétrica en conjunción con funciones resumen. (ver Firmas Digitales. Función resumen)
5. Problemas de suplantación. En las redes tenemos el problema añadido de que cualquier usuario autorizado puede acceder al sistema desde fuera, por lo que hemos de confiar en sistemas fiables para garantizar que los usuarios no están siendo suplantados por intrusos. Normalmente se emplean mecanismos basados en password para conseguir esto.

1.5.2 CONCEPTOS BÁSICOS SOBRE COMPUTACIÓN CUÁNTICA

COMPUTACIÓN CUÁNTICA

Se refiere a los fenómenos que tendrá que enfrentar la tecnología de las computadoras cuando el tamaño de sus componentes (transistores, circuitos,

etc.) rebase un límite inferior determinado, para el que las leyes de la física son fundamentalmente diferentes a las que se aplican en el mundo macroscópico.

COMPUTACIÓN CUÁNTICA A NIVEL DE HARDWARE

A medida que la información pase a ser representada por unas cuantas partículas subatómicas, (a diferencia de como se representa ahora mediante una gran cantidad de éstas a través de los diferenciales de voltaje en los componentes de la computadora), los dispositivos deberán de reconocer los fenómenos cuánticos, como por ejemplo: las partículas pueden tener varios estados atómicos a la vez (niveles de energía), pueden atravesar barreras aparentemente infranqueables, pueden seguir varias rutas a la vez, etc..

COMPUTACIÓN CUÁNTICA A NIVEL DE ALGORITMOS

Con relación a los algoritmos (procedimientos matemáticos para resolver problemas), la computación cuántica abre posibilidades antes no imaginadas: disminuciones exponenciales en el tiempo de procesamiento y realización de operaciones en paralelo sin la necesidad de agregar procesadores a la máquina.⁷

MECANICA CUANTICA

Es la mecánica que describe el movimiento de los átomos, moléculas y los electrones, y permite explicar el comportamiento de los semiconductores, de los superfluidos, de los superconductores, y aún de todo lo que nos rodea: se puede decir que un automóvil, y una computadora son, a final de cuentas, sistemas cuánticos. No sólo es fundamental la teoría cuántica, sino la base de gran parte de nuestra tecnología; sus conceptos se emplean para formular la mayoría de las teorías actuales con la única excepción de la relatividad general.

⁷ Todos los conceptos escritos anteriormente están tomados de
<http://www.albanet.com.mx/articulos/cuantico.htm>

Debido a que la física cuántica es radicalmente diferente a la clásica, y a que la información es física, la teoría del procesamiento de la información debe cambiar drásticamente para adaptarse a una descripción cuántica.

ASPECTOS DE LA MECANICA CUANTICA RELEVANTES PARA LA COMPUTACIÓN

- a) La **cuantización**, significa que los valores que toman cantidades físicas no varían de manera continua, sino que lo hacen de un tamaño predeterminado a los que se conoce como cuantos. Así, cualquier sistema con dos (o más) estados parecerá diseñado para representar 0's y 1's, esto es, para representar información. Esta característica es la que hace posible a la computación, tanto la cuántica como la clásica, ya que, sino fuera por ella, los semiconductores y los circuitos integrados no funcionarían. Aquí hay casi una contradicción: las computadoras actuales (a las que llamaremos clásicas o binarias) requieren de fenómenos cuánticos que hagan funcionar sus circuitos integrados para realizar los cálculos clásicamente.

- b) La **superposición** de estados cuánticos, esto quiere decir que todo estado cuántico se puede describir como una suma o superposición de otros; también significa que dados un cierto número de estados, una suma cualquiera de ellos es otro estado admisible. Ésta y la cercanamente propiedad siguiente son las que hacen a las computadoras cuánticas muchísimo más poderosas que las clásicas.

- c) La **interferencia** entre estados cuánticos, significa que todo resultado de un proceso cuántico depende de todas las posibles historias que pudieran producir el proceso. Cuando un estado se forma sumando otros, es seguro

que ocurra interferencia entre éstos. El fenómeno puede usarse para aumentar o disminuir el efecto desde una propiedad preseleccionada. Esta propiedad y la anterior son las que hacen a las computadoras cuánticas muchísimo más poderosas que las clásicas.

- d) El **enredamiento** (*entanglement*, inglés), quiere decir que dos sistemas pueden contener información en común simplemente por haber interactuado en el pasado y a pesar de que ya no lo hagan más. Sin embargo la información en común no es accesible localmente a ninguno de los sistemas por separado. Esta propiedad es la que hace posible a la criptografía cuántica.

DE LOS BITS A LOS CUBITS

Sabemos que la información se representa en piezas discretas, al igual que los niveles energéticos de los átomos. La unidad básica de información es el bit. Desde un punto de vista físico, un bit es un sistema con dos estados, pudiendo ser separado en uno de estos estados, que representan dos valores lógicos: sí ó no, 1 ó 0.

Por ejemplo, en los computadores digitales, estaría representado por el valor del voltaje que adquieren las placas de un condensador. Así, 1 sería un valor de "a" volts, y 0 un valor de "b" volts. Pero un bit puede también ser representado por dos diferentes polarizaciones de la luz, o por dos estados electrónicos de un átomo.

Ahora la mecánica cuántica nos dice que si un bit puede estar en cualquiera dos estados distinguibles, también puede estar en cualquier superposición coherente de ellos, y claro, estos son más estados, que no tienen análogos

clásicos, y en los cuales un átomo representa ambos valores 0 y 1 simultáneamente (y este comportamiento es propio de los sistemas atómicos).

Es a esta representación, que puede tomar los dos valores 0 ó 1 en proporciones arbitrarias, pero simultáneamente, a lo que se llama cubit ó unidad de información cuántica.

CAPÍTULO II

METODOLOGÍA

CAPÍTULO II. METODOLOGÍA

2.1 OBJETIVO

Realizar una investigación de campo en las Empresas Salvadoreñas para cuantificar, analizar e interpretar los datos obtenidos de cada una de ellas con el fin de analizar el impacto que tendría el desarrollo de la computación cuántica con respecto a los mecanismos de seguridad que utilizan criptografía asimétrica.

Además se realiza una investigación de tipo deductivo, para hacer las suposiciones referentes a hechos investigados.

2.2 METODOLOGÍA DE INVESTIGACION

2.2.1 MÉTODO CIENTÍFICO

El método científico en esta investigación servirá para que de una forma práctica se pueda llevar a cabo una experimentación y poder corroborar sus resultados.

Los pasos o fases que la investigación debe de seguir son:

- a) **observación o análisis**,
- b) **hipótesis**,
- c) **síntesis o construcción**,
- d) **validación o resultados**, y
- e) **conclusión** en la cual se incluye la argumentación final.

- a) Observación o análisis. La observación o análisis es la parte del método experimental que nace del poder observar en forma repetitiva una serie de fenómenos o situaciones del universo estudiado. Así mismo nos situamos en las Empresas de El Salvador que utilizan en su seguridad algoritmos de

cifrado asimétrico, podemos ver una serie de manifiestos que giran sobre las empresas. El siguiente paso dentro de esta misma parte, es el hacernos una serie de preguntas de lo que estamos observando: y estas preguntas de alguna forma van a involucrar a ciertos elementos de las observaciones que hemos realizado tomando en cuenta una parte limitada de la población que constituye la muestra; en este caso se estudia una muestra representativa de las Empresas de tipo industrial, comercial, de comunicaciones, establecimientos financieros y aduanales, establecidas y registradas legalmente, de acuerdo a la “Dirección General de Estadísticas y Censos” (DIGESTYC), posteriormente se generalizan los resultados del análisis a todas las Empresas Salvadoreñas que pertenecen a los tipos mencionados.

- b) La segunda fase de la investigación científica se denomina hipótesis que viene de la raíz que significa la falta de una tesis completa. Solo tenemos la suposición de la misma. Esta suposición nos va a invitar a tratar de construir un modelo que valide nuestra suposición. La suposición está fundamentada en la regulación de los elementos que hemos observado de la fase anterior.
- c) Síntesis o construcción del experimento será nuestro tercer paso. Ya que tenemos una serie de suposiciones sobre una observación general, vamos a querer construir un modelo que nos permita sintetizar, (juntar) nuestra observación para poder enfocarnos a contestar si nuestra suposición (HIPOTESIS) es correcta o no. A esta fase se le llama síntesis que consiste solamente en la construcción del modelo o el experimento mismo. En este caso sería la preparación de una encuesta y/o un cuestionario. Otro, se refiere a la preparación de las fuentes de información de lo que vamos a investigar.
- d) La siguiente fase del método científico es la validación de la suposición planteada en la hipótesis, usando la construcción efectuada anteriormente

en la síntesis. En este caso procede a aplicar el instrumento o experimento desarrollado en la población que hemos observado durante nuestro análisis. Al final de esta fase se obtienen los resultados tanto cualitativamente, esto es en forma de conceptos y el análisis de estos.

- e) Finalmente tenemos la conclusión ya sea que la hipótesis haya quedado validada, con lo cual generaríamos una tesis, ya que la suposición ha sido corroborada. Ahora bien, puede suceder que la suposición que empleamos o desarrollamos sea falsa, por lo cual tendremos que utilizar una hipótesis alternativa y así regresar a la síntesis para poder buscar nuevos resultados y llegar a una tesis. Teniendo una tesis podremos plantear una serie de conclusiones que se fundamentan en los argumentos producto de los resultados de la investigación. Sin embargo, estas argumentaciones no son tesis sino simplemente argumentaciones que invitan a una nueva observación y la repetición del método científico para llegar a nuevas tesis.

2.2.2 MÉTODO DEDUCTIVO

Este método consiste en partir de los datos generales aceptados como válidos y que, por medio del razonamiento lógico pueden deducirse varias suposiciones. El método deductivo fue utilizado para realizar la investigación de los primeros tres objetivos específicos los cuales consisten en la investigación de los principios y fundamentos de la computación cuántica, el funcionamiento del algoritmo de Shor y los algoritmos asimétricos de cifrado.

2.2.3 TIPO DE ESTUDIO

El desarrollo de la Investigación se caracteriza de acuerdo a los siguientes criterios:

Exploratorio: Por la Necesidad esencial de familiarizarse con el tema. Este es novedoso y poco estudiado en nuestro medio. Además será el punto de partida para estudios posteriores de mayor profundidad.

Descriptivo: Debido que se analizará e interpretará el funcionamiento de los algoritmos de cifrado asimétrico y el algoritmo de Shor para ordenadores cuánticos, exponiendo sus características.

De Campo: Ya que este estudia el fenómeno en el escenario donde se manifiestan los hechos, se tendrá que visitar las Empresas legalmente establecidas y registradas en El Salvador de acuerdo a DIGESTYC, siendo esta una muestra representativa.

2.2.4 TÉCNICAS DE INVESTIGACIÓN

RECOPILACIÓN DE DATOS

Para el desarrollo del proyecto se realizó una investigación tanto documental como de campo.

Las fuentes de consulta fueron de dos tipos:

a. Bibliográfica

Que incluyó libros de texto sobre Criptografía y Seguridad de la Información, Manuales Técnicos sobre las herramientas utilizadas para el desarrollo de este tipo de proyectos, Tesis, revistas relacionados con el tema.

b. Internet

Fue una de las principales fuentes de información, ya que de ella se pudieron obtener información descriptiva sobre Criptografía y los avances de la Computación Cuántica.

En la investigación de campo se aplicaron las siguientes técnicas de recopilación de información:

a. Entrevistas

La entrevista consiste en una conversación entre dos o más personas, sobre un tema determinado de acuerdo a ciertos esquemas o pautas determinadas. Mediante las entrevistas se obtuvo información referente a la situación de las Empresas en cuanto a usos de Internet, tecnología informática y seguridad. Las entrevistas realizadas fueron dirigidas a

a.1 Expertos en el tema

Se entrevistó a personas que por su trabajo o experiencia, conocen sobre tecnologías o herramientas de desarrollo, así como detalles de implementación que contribuyan al desarrollo del proyecto.

a.2. Empresas

De la misma manera, se realizaron entrevistas con el personal de las Empresas para recolectar información sobre los servicios de Internet y uso de mecanismos de seguridad. La información obtenida de estas fue recopilada en las encuestas.

b. Observación

Consiste básicamente en utilizar los sentidos para observar los hechos, realidades sociales y a las personas en su contexto cotidiano con el objetivo de obtener información que es difícil obtener a través de una entrevista o encuesta. Se visitaron de forma presencial, Empresas salvadoreñas, de esta manera se conocieron los usos de Internet.

c. Encuestas

Es una metodología que satisface todas las exigencias de investigación, para su realización se necesita una planificación y su objetivo es investigar acontecimientos presentes ocurridos y de opinión; el instrumento utilizado fue el cuestionario, ya que es la traducción de los objetivos de la investigación a preguntas específicas y opera problemas de investigación. El cuestionario que se utilizó es de carácter genérico, conteniendo una diversidad de preguntas las cuales son de tipo abiertas, cerradas y categorizadas.

Se realizaron las encuestas con el objetivo de conocer de manera directa, los servicios de Internet y los mecanismos de seguridad que utilizan las Empresas, además saber los conocimientos que tienen sobre criptografía. Así mismo, las encuestas permitieron determinar la situación actual de dichas empresas en cuanto a tecnología se refiere. (Ver Anexo 3, se presenta el modelo propuesto para la Encuesta, dirigida a los Administradores de Informática).

2.2.5 MARCO MUESTRAL

El marco muestral estará determinado por toda la población de la cual se extrae la muestra en la que se realizara la investigación. Para el análisis de la muestra se utilizara el método estadístico inferencial.

POBLACIÓN

La población constituye la totalidad de un grupo de elementos u objetos que se quiere investigar, es el conjunto de todos los casos que concuerdan con lo que se pretende investigar. La población que forma el universo en la investigación lo constituyen las Empresas de tipo industrial, comercial, comunicaciones, financiero, tramitadoras aduaneras que están legalmente registradas en El Salvador; ya que se considera que una empresa que pertenece a uno de estos tipos esta en la capacidad de hacer una inversión, de acuerdo a los requerimientos mínimos planteados para el proyecto.

Para la obtención de estos datos se consultó a “La Dirección General de Estadísticas y Censos” (DIGESTYC) para la obtención de las Empresas Legalmente registradas. Es importante mencionar el hecho de que pueden existir muchas Empresas que no estén legalmente registradas y para efectos de la investigación no se tomaran en cuenta. A continuación se presenta una tabla con los datos recolectados.

El Salvador 2000	
Tipo	No. De establecimientos
Industrial	16
Comercial	67
Comunicaciones	50
Financieras	236
Aduaneras	14
TOTAL	383

El total de Empresas legalmente registradas es de 383. Este es el tamaño de la Población a utilizar. La referencia más reciente es del año 2000.

MUESTRA

La muestra es un subconjunto de la población o parte representativa de la misma. Se hará uso de la siguiente fórmula para obtener el tamaño de la muestra; siendo está una recomendación de los métodos estadísticos probabilísticos para población finita.

$$n = \frac{N (z^2 \cdot P \cdot Q)}{E^2 (N-1) + (z^2 \cdot P \cdot Q)}$$

donde:

N = Tamaño del universo

z = Nivel de Confianza

P x Q = Factores de Variabilidad de fenómeno

E = Error

n = Tamaño de la muestra

operando se tiene:

N = 383

Z = Se utilizará el nivel de confianza de 0.95% por lo tanto: $0.95/2=0.475$.

De acuerdo a la tabla de la curva normal se tiene que: Z = 1.96

P = 0.5 Es la probabilidad de éxito

Q = 0.5 Es la probabilidad de fracaso

E =10%

Utilizando la fórmula para calcular la muestra (n) se tiene:

$$n = \frac{(383 \times (1.96)^2 \times (0.5 \times 0.5))}{((0.1)^2 \times (383 - 1)) + ((1.96)^2 \times 0.5 \times 0.5)}$$

n = 77

2.3 INTERPRETACION DE LOS RESULTADOS

La interpretación de los resultados de las encuestas y su análisis serán mostrados en el capítulo IV como parte del Desarrollo de la investigación.

CAPÍTULO III

MARCO TEÓRICO

CAPÍTULO III. MARCO TEÓRICO

3. 1 FUNDAMENTOS TEÓRICOS DE LA CRIPTOGRAFÍA

3.1 .1 TEORÍA DE LA INFORMACIÓN

Cantidad de Información

Podemos fijarnos en la cantidad de información como una medida de la disminución de incertidumbre acerca de un suceso. Por ejemplo, si nos dicen que el número que ha salido en un dado es menor que dos, nos dan más información que si nos dicen que el número que ha salido es par.

Se puede decir que la cantidad de información que obtenemos al conocer un hecho es directamente proporcional al número posible de estados que éste tenga a priori. Si inicialmente teníamos diez posibilidades, conocer el hecho nos proporciona más información que si inicialmente tuviéramos dos. Por ejemplo, supone mayor información conocer la combinación ganadora del próximo sorteo de la Lotería Primitiva, que saber si una moneda lanzada al aire va a caer con la cara o la cruz hacia arriba. Claramente es más fácil acertar en el segundo caso.

Confusión y Difusión

Según la Teoría de Shannon, las dos técnicas básicas para ocultar la redundancia en un texto claro son la confusión y la difusión. Estos conceptos, a pesar de su antigüedad, poseen una importancia clave en Criptografía moderna.

- *Confusión.* Trata de ocultar la relación entre el texto claro y el texto cifrado. Recordemos que esa relación existe y se da a partir de la clave k empleada, puesto que si no existiera jamás podríamos descifrar los mensajes. El mecanismo más simple de confusión es la sustitución, que consiste en cambiar cada ocurrencia de un símbolo en el texto claro por otro. La sustitución puede ser tan simple o tan compleja como queramos.

- *Difusión.* Diluye la redundancia del texto claro repartiéndola a lo largo de todo el texto cifrado. El mecanismo más elemental para llevar a cabo una difusión es la transposición, que consiste en cambiar de sitio elementos individuales del texto claro.

3.1.2 INTRODUCCIÓN A LA COMPLEJIDAD ALGORÍTMICA

Concepto de Algoritmo

En la actualidad, prácticamente todas las aplicaciones criptográficas emplean computadoras en sus cálculos, y las computadoras convencionales están diseñadas para ejecutar algoritmos. Definiremos algoritmo como una secuencia finita y ordenada de instrucciones elementales que, dados los valores de entrada de un problema, en algún momento finaliza y devuelve la solución.

En efecto, las computadoras actuales poseen una memoria, que les sirve para almacenar datos, unos dispositivos de entrada y salida que les permiten comunicarse con el exterior, una unidad capaz de hacer operaciones aritméticas y lógicas, y una unidad de control, capaz de leer, interpretar y ejecutar un programa o secuencia de instrucciones. Habitualmente, las unidades aritmético-lógica y de control se suelen encapsular en un único circuito integrado, que se conoce por microprocesador o CPU.

Cuando nosotros diseñamos un algoritmo de cifrado, estamos expresando, de un modo más o menos formal, la estructura que ha de tener la secuencia de instrucciones concreta que permita implementar dicho algoritmo en cada computadora particular. Habrá computadoras con más o menos memoria, velocidad o incluso número de microprocesadores —capaces de ejecutar varios programas al mismo tiempo—, pero en esencia todas obedecerán al concepto de algoritmo.

La Teoría de Algoritmos es una ciencia que estudia cómo construir algoritmos para resolver diferentes problemas. En muchas ocasiones no basta con encontrar una forma de solucionar el problema: la solución ha de ser óptima. En este sentido la Teoría de Algoritmos también proporciona herramientas formales que nos van a permitir decidir qué algoritmo es mejor en cada caso, independientemente de las características particulares de la computadora concreta en la que queramos implantarlo.

La Criptografía depende en gran medida de la Teoría de Algoritmos, ya que por un lado hemos de asegurar que el usuario legítimo, que posee la clave, puede cifrar y descifrar la información de forma rápida y cómoda, mientras que por otro hemos de garantizar que un atacante no dispondrá de ningún algoritmo eficiente capaz de comprometer el sistema.

Cabría plantearnos ahora la siguiente cuestión: si un mismo algoritmo puede resultar más rápido en una computadora que en otra, ¿podría existir una computadora capaz de ejecutar de forma eficiente algoritmos que sabemos que no lo son?. Existe un principio fundamental en Teoría de Algoritmos, llamado principio de invarianza, que dice que si dos implementaciones del mismo algoritmo consumen $t_1(n)$ y $t_2(n)$ segundos respectivamente, siendo n el tamaño de los datos de entrada, entonces existe una constante positiva c tal que $t_1(n) \leq c \cdot t_2(n)$, siempre que n sea lo suficientemente grande. En otras palabras, que aunque podamos encontrar una computadora más rápida, o una implementación mejor, la evolución del tiempo de ejecución del algoritmo en función del tamaño del problema permanecerá constante, por lo tanto la respuesta a la pregunta anterior es, afortunadamente, negativa. Eso nos permite centrarnos por completo en el algoritmo en sí y olvidarnos de la implementación concreta a la hora de hacer nuestro estudio.

En muchas ocasiones, el tiempo de ejecución de un algoritmo viene dado por las entradas concretas que le introduzcamos. Por ejemplo, se necesitan menos operaciones elementales para ordenar de menor a mayor la secuencia {1, 2, 3, 4, 6, 5} que {6, 5, 3, 2, 1, 4}. Eso nos llevará a distinguir entre tres alternativas:

- *Mejor caso*: Es el número de operaciones necesario cuando los datos se encuentran distribuidos de la mejor forma posible para el algoritmo. Evidentemente este caso no es muy práctico, puesto que un algoritmo puede tener un mejor caso muy bueno y comportarse muy mal en el resto.
- *Peor caso*: Es el número de operaciones necesario para la distribución más pesimista de los datos de entrada. Nos permitirá obtener una cota superior del tiempo de ejecución necesario. Un algoritmo que se comporte bien en el peor caso, será siempre un buen algoritmo.
- *Caso promedio*: Muchas veces, hay algoritmos que en el peor caso no funcionan bien, pero en la mayoría de los casos que se presentan habitualmente tienen un comportamiento razonablemente eficiente. De hecho, algunos algoritmos típicos de ordenación necesitan el mismo número de operaciones en el peor caso, pero se diferencian considerablemente en el caso promedio.

Complejidad Algorítmica

En la mayoría de los casos carece de interés calcular el tiempo de ejecución concreto de un algoritmo en una computadora, e incluso algunas veces simplemente resulta imposible. En su lugar emplearemos una notación de tipo asintótico, que nos permitirá acotar dicha magnitud. Normalmente consideraremos el tiempo de ejecución del algoritmo como una función $f(n)$ del tamaño n de la entrada. Por lo tanto f debe estar definida para los números naturales y devolver valores en \mathbb{R}^+ .

Dada la función $f(n)$, haremos las siguientes definiciones:

Límite superior asintótico: $f(n) = O(g(n))$ si existe una constante positiva c y un número entero positivo n_0 tales que $0 \leq f(n) \leq cg(n) \forall n \geq n_0$

Límite inferior asintótico: $f(n) = \Omega(g(n))$ si existe una constante positiva c y un número entero positivo n_0 tales que $0 \leq cg(n) \leq f(n) \forall n \geq n_0$

Límite exacto asintótico: $f(n) = \theta(g(n))$ si existen dos constantes positivas c_1, c_2 y un número entero positivo n_0 tales que $c_1g(n) \leq f(n) \leq c_2g(n) \forall n \geq n_0$

Notación o : $f(n) = o(g(n))$ si para cualquier constante positiva c existe un número entero positivo $n_0 > 0$ tal que $0 \leq f(n) < cg(n) \forall n \geq n_0$

Intuitivamente, $f(n) = O(g(n))$ significa que $f(n)$ crece asintóticamente no más rápido que $g(n)$ multiplicada por una constante. Análogamente $f(n) = \Omega(g(n))$ quiere decir que $f(n)$ crece asintóticamente al menos tan rápido como $g(n)$ multiplicada por una constante.

Definiremos ahora algunas propiedades sobre la notación que acabamos de introducir:

- a) $f(n) = O(g(n)) \Leftrightarrow g(n) = \Omega(f(n))$.
- b) $f(n) = \theta(g(n)) \Leftrightarrow f(n) = O(g(n)) \wedge f(n) = \Omega(g(n))$.
- c) Si $f(n) = O(h(n)) \wedge g(n) = O(h(n))$, entonces $(f + g)(n) = O(h(n))$.
- d) Si $f(n) = O(h(n)) \wedge g(n) = O(l(n))$, entonces $(f \cdot g)(n) = O(h(n)l(n))$.
- e) $f(n) = O(f(n))$.
- f) Si $f(n) = O(g(n)) \wedge g(n) = O(h(n))$, entonces $f(n) = O(h(n))$.

Para algunas funciones de uso común, podemos definir directamente su orden de complejidad:

3.1.3 ALGORITMOS POLINOMIALES, EXPONENCIALES Y SUBEXPONENCIALES

Diremos que un algoritmo es polinomial si su peor caso de ejecución es de orden $O(n^k)$, donde n es el tamaño de la entrada y k es una constante. Adicionalmente, cualquier algoritmo que no pueda ser acotado por una función polinomial, se conoce como exponencial. En general, los algoritmos polinomiales se consideran eficientes, mientras que los exponenciales se consideran ineficientes.

Un algoritmo se denomina subexponencial si en el peor de los casos, la función de ejecución es de la forma $e^{o(n)}$, donde n es el tamaño de la entrada. Son asintóticamente más rápidos que los exponenciales puros, pero más lentos que los polinomiales.

Clases de Complejidad

Para simplificar la notación, en muchas ocasiones se suele reducir el problema de la complejidad algorítmica a un simple problema de decisión, de forma que se considera un algoritmo como un mecanismo que permite obtener una respuesta sí o no a un problema concreto.

La clase de **complejidad P** es el conjunto de todos los problemas de decisión que pueden ser resueltos en tiempo polinomial.

La clase de **complejidad NP** es el conjunto de todos los problemas para los cuales una respuesta afirmativa puede ser verificada en tiempo polinomial, empleando alguna información extra, denominada certificado.

La clase de **complejidad co-NP** es el conjunto de todos los problemas para los cuales una respuesta negativa puede ser verificada en tiempo polinomial, usando un certificado apropiado.

Nótese que el hecho de que un problema sea NP, no quiere decir necesariamente que el certificado correspondiente sea fácil de obtener, sino que, dado éste último, puede verificarse la respuesta afirmativa en tiempo polinomial. Una observación análoga puede llevarse a cabo sobre los problemas co-NP.

Sabemos que $P \subseteq NP$ y que $P \subseteq co-NP$. Sin embargo, aún no se sabe si $P = NP$, si $NP = co-NP$, o si $P = NP \cap co-NP$. Si bien muchos expertos consideran que ninguna de estas tres igualdades se cumple, este punto no ha podido ser demostrado matemáticamente.

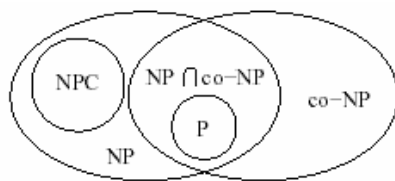


Figura: Relación entre las clases de complejidad P, NP, co-NP y NPC.

Dentro de la clase NP, existe un subconjunto de problemas que se llaman NP-completos, y cuya clase se nota como NPC. Estos problemas tienen la peculiaridad de que todos ellos son equivalentes, es decir, se pueden reducir unos en otros, y si lográramos resolver alguno de ellos en tiempo polinomial, los habríamos resuelto todos. También se puede decir que cualquier problema NP-completo es al menos tan difícil de resolver como cualquier otro problema NP, lo cual hace a la clase NPC la de los problemas más difíciles de resolver computacionalmente.

Sea $A = \{a_1, a_2, \dots, a_n\}$ un conjunto de números enteros positivos, y s otro número entero positivo. El problema de determinar si existe un subconjunto de A cuyos elementos sumen s es un problema NP-completo, y, como ya se ha

dicho, todos los problemas de esta clase pueden ser reducidos a una instancia de este. Nótese que dado un subconjunto de A , es muy fácil verificar si suma s , y que dado un subconjunto de A que suma s que desempeñaría el papel de certificado, se puede verificar fácilmente que la respuesta al problema es afirmativa.

En la figura anterior puede observarse gráficamente la relación existente entre las distintas clases de complejidad que acabamos de definir.

Finalmente, apuntaremos que existe una clase de problemas, los denominados NP duros esta clase se define sobre los problemas en general, no sólo sobre los de decisión, y que contiene la versión computacional del problema definido anteriormente, que consistiría en encontrar el subconjunto de A cuyos elementos suman s .

Algoritmos Probabilísticos

Este tipo de algoritmos maneja algún tipo de parámetro aleatorio, lo cual hace que dos ejecuciones diferentes con los mismos datos de entrada no tengan por qué ser idénticas. En algunos casos, métodos de este tipo permiten obtener soluciones en una cantidad de tiempo considerablemente inferior a los determinísticos.

Podemos clasificar los algoritmos no determinísticos según la probabilidad con la que devuelvan la solución correcta. Sea A un algoritmo aleatorizado para el problema de decisión L , y sea I una instancia arbitraria de L . Sea P_1 la probabilidad de que A devuelva cierto cuando I es cierto, y P_2 la probabilidad de que A devuelva cierto cuando I es falso.

- A es de tipo error nulo si $P_1 = 1$ y $P_2 = 0$.
- A es de tipo error simple si $P_1 \geq c$, siendo c una constante positiva, y $P_2 = 0$
- A es de tipo error doble si $P_1 \geq 1/2 + \epsilon$, y $P_2 \leq 1/2 - \epsilon$

Definiremos también el tiempo esperado de ejecución de un algoritmo aleatorizado como el límite superior del tiempo de ejecución esperado para cada entrada, expresado en función del tamaño de la entrada. El tiempo de ejecución esperado para cada entrada será la media de los tiempos obtenidos para esa entrada y todas las posibles salidas del generador aleatorio.

Las clases de complejidad probabilística son las siguientes:

- **Clase ZPP:** conjunto de todos los problemas de decisión para los cuales existe un algoritmo de tipo error nulo que se ejecuta en un tiempo esperado de ejecución polinomial.
- **Clase RP:** conjunto de los problemas de decisión para los cuales existe un algoritmo de tipo error simple que se ejecuta en el peor caso en tiempo polinomial.
- **Clase BPP:** conjunto de los problemas de decisión para los cuales existe un algoritmo de tipo error doble que se ejecuta en el peor caso en tiempo polinomial.

Finalmente, diremos que $P \subseteq ZPP \subseteq RP \subseteq BPP$ y $RP \subseteq NP$.

3.1.4 FUNDAMENTOS DE ARITMÉTICA MODULAR

Aritmética Modular. Propiedades

La aritmética modular es una parte de las Matemáticas extremadamente útil en Criptografía, ya que permite realizar cálculos complejos y plantear problemas interesantes, manteniendo siempre una representación numérica compacta y definida, puesto que sólo maneja un conjunto finito de números enteros. Mucha

gente la conoce como la aritmética del reloj, debido a su parecido con la forma que tenemos de contar el tiempo. Por ejemplo, si son las 19:13:59 y pasa un segundo, decimos que son las 19:14:00, y no las 19:13:60. Como vemos, los segundos al igual que los minutos, se expresan empleando sesenta valores cíclicamente, de forma que tras el 59 viene de nuevo el 0. Desde el punto de vista matemático diríamos que los segundos se expresan módulo 60.

Dados tres números $a, b, n \in \mathbb{N}$, decimos que a es congruente con b módulo n , y se escribe: $a \equiv b \pmod{n}$ si se cumple: $a = b + kn$, para algún $k \in \mathbb{Z}$

Por ejemplo, $37 \equiv 5 \pmod{8}$, ya que $37 = 5 + 4 \cdot 8$. De hecho, los números 5, -3, 13, -11, 21, -19, 29. . . son todos equivalentes en la aritmética módulo 8, es decir, forman una clase de equivalencia. Como se puede apreciar, cualquier número entero pertenecerá necesariamente a alguna de esas clases, y en general, tendremos n clases de equivalencia módulo n (números congruentes con 0, números congruentes con 1, . . . , números congruentes con $n-1$). Por razones de simplicidad, representaremos cada clase de equivalencia por un número comprendido entre 0 y $n - 1$. De esta forma, en nuestro ejemplo (módulo 8) tendremos el conjunto de clases de equivalencia $\{0, 1, 2, 3, 4, 5, 6, 7\}$, al que denominaremos \mathbb{Z}_8 . Podemos definir ahora las operaciones suma y producto en este tipo de conjuntos:

- $a + b \equiv c \pmod{n} \Leftrightarrow a + b = c + kn \quad k \in \mathbb{Z}$
- $ab \equiv c \pmod{n} \Leftrightarrow ab = c + kn \quad k \in \mathbb{Z}$

Propiedades de la suma:

- *Asociativa*: $\forall a, b, c \in \mathbb{Z}_n \quad (a + b) + c \equiv a + (b + c) \pmod{n}$
- *Conmutativa*: $\forall a, b \in \mathbb{Z}_n \quad a + b \equiv b + a \pmod{n}$
- *Elemento Neutro*: $\forall a \in \mathbb{Z}_n \quad \exists 0 \text{ tal que } a + 0 \equiv a \pmod{n}$
- *Elemento Simétrico (opuesto)*: $\forall a \in \mathbb{Z}_n \quad \exists b \text{ tal que } a + b \equiv 0 \pmod{n}$

Propiedades del producto:

- *Asociativa*: $\forall a, b, c \in \mathbb{Z}_n \quad (a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod{n}$
- *Conmutativa*: $\forall a, b \in \mathbb{Z}_n \quad a \cdot b \equiv b \cdot a \pmod{n}$
- *Elemento Neutro*: $\forall a \in \mathbb{Z}_n \quad \exists 1 \text{ tal que } a \cdot 1 \equiv a \pmod{n}$

Propiedades del producto con respecto de la suma:

- *Distributiva*: $\forall a, b, c \in \mathbb{Z}_n \quad (a + b) \cdot c \equiv (a \cdot c) + (b \cdot c) \pmod{n}$

La operación suma en este conjunto cumple las propiedades asociativa y conmutativa y posee elementos neutro y simétrico, por lo que el conjunto tendría estructura de grupo conmutativo. A partir de ahora llamaremos grupo finito inducido por n a dicho conjunto.

Con la operación producto se cumplen las propiedades asociativa y conmutativa, y tiene elemento neutro, pero no necesariamente simétrico recordemos que al elemento simétrico para el producto se le suele denominar inverso. La estructura del conjunto con las operaciones suma y producto es, pues, de anillo conmutativo.

Algoritmo de Euclides

Quizá sea el algoritmo más antiguo que se conoce, y a la vez es uno de los más útiles.

Permite obtener de forma eficiente el máximo común divisor de dos números.

Sean a y b dos números enteros de los que queremos calcular su máximo común divisor m .

El Algoritmo de Euclides explota la siguiente propiedad:

$$m/a \wedge m/b \Rightarrow m/(a - kb) \text{ con } k \in \mathbb{Z} \Rightarrow m/(a \bmod b)$$

a/b quiere decir que a divide a b , o en otras palabras, que b es múltiplo de a , mientras que $(a \bmod b)$ representa el resto de dividir a entre b . En esencia estamos diciendo, que, puesto que m divide tanto a " a " como a " b ", debe dividir a su diferencia. Entonces si restamos k veces b de a , llegará un momento en el que obtengamos el resto de dividir a por b , o sea $a \bmod b$.

Si llamamos c a $(a \bmod b)$, podemos aplicar de nuevo la propiedad anterior y tenemos:

$$m/(b \bmod c)$$

Sabemos, pues, que m tiene que dividir a todos los restos que vayamos obteniendo. Es evidente que el último de ellos será cero, puesto que los restos siempre son inferiores al divisor.

El penúltimo valor obtenido es el mayor número que divide tanto a " a " como a " b ", o sea, el máximo común divisor de ambos. El algoritmo queda entonces como sigue:

```
int euclides(int a, int b)
{ int i;
  int g[];
  g[0]=a;
  g[1]=b;
  i=1;
  while (g[i]!=0)
  { g[i+1]=g[i-1]%g[i];
    i++;
  }
  return(g[i-1]);
}
```

El invariante -condición que se mantiene en cada iteración- del Algoritmo de Euclides es el siguiente:

$$g_{i+1} = g_{i-1} \pmod{g_i}$$

y su orden de complejidad será de $O((\log_2(n))^2)$ operaciones a nivel de bit, siendo n una cota superior de a y b .

Complejidad de las Operaciones Aritméticas en \mathbb{Z}_n

La complejidad algorítmica de las operaciones aritméticas modulares es la misma que la de las no modulares:

- Suma modular $((a + b) \bmod n)$: $O(\log_2(a) + \log_2(b)) = O(\log_2(n))$
- Resta modular $((a - b) \bmod n)$: $O(\log_2(a) + \log_2(b)) = O(\log_2(n))$
- Multiplicación modular $((a \cdot b) \bmod n)$: $O(\log_2(a) \cdot \log_2(b)) = O((\log_2(n))^2)$

3.1.5 IMPORTANCIA DE LOS NÚMEROS PRIMOS

Para explotar la dificultad de cálculo de logaritmos discretos, muchos algoritmos criptográficos de llave pública se basan en operaciones de exponenciación en grupos finitos. Dichos conjuntos deben cumplir la propiedad de que su *módulo* n sea un número muy grande con pocos factores usualmente dos. Estos algoritmos funcionan si se conoce n y sus factores se mantienen en secreto. Habitualmente para obtener n se calculan primero dos números primos muy grandes, que posteriormente se multiplican. Necesitaremos pues mecanismos para poder calcular esos números primos grandes.

La factorización es el problema inverso a la multiplicación: dado n , se trata de buscar un conjunto de números tales que su producto valga n . Normalmente, y para que la solución sea única, se impone la condición de que los factores de n que obtengamos sean todos primos elevados a alguna potencia. Al igual que para el problema de los logaritmos discretos, no existen algoritmos eficientes para efectuar este tipo de cálculos. Esto nos permite confiar en que, en la

práctica, será imposible calcular los factores de n , incluso disponiendo de elevados recursos computacionales.

En cuanto al cálculo de primos grandes, bastaría con aplicar un algoritmo de factorización para saber si un número es primo o no. Este mecanismo es inviable, puesto que acabamos de decir que no hay algoritmos eficientes de factorización. Por suerte, sí que existen algoritmos probabilísticos que permiten decir con un grado de certeza bastante elevado si un número cualquiera es primo o compuesto.

Cabría preguntarse, dado que para los algoritmos asimétricos de cifrado necesitaremos generar muchos números primos, si realmente hay suficientes. De hecho se puede pensar que, a fuerza de generar números, llegará un momento en el que repitamos un primo generado con anterioridad. Podemos estar tranquilos, porque si a cada átomo del universo le asignáramos mil millones de números primos cada microsegundo desde su origen hasta hoy, harían falta un total de 10^{109} números primos diferentes, mientras que el total estimado de números primos de 512 bits o menos es aproximadamente de 10^{151} .

También podríamos pensar en calcular indiscriminadamente números primos para luego emplearlos en algún algoritmo de factorización rápida. Por desgracia, si quisiéramos construir un disco duro que albergara diez mil GBytes por cada gramo de masa y milímetro cúbico para almacenar todos los primos de 512 bits o menos, el artilugio pesaría más de 10^{135} Kg y ocuparía casi 10^{130} metros cúbicos, es decir, sería miles de billones de veces más grande y pesado que la Vía Láctea.

3.1.6 ALGORITMOS DE FACTORIZACIÓN

Como bien es sabido, la descomposición de un número entero $n = P_1^{e_1} \cdot P_2^{e_2} \dots P_k^{e_k}$ siendo p_i números primos y e_i números enteros mayores que 1, es única. Cuando tratamos de obtener la factorización de n , normalmente nos conformamos con alcanzar una descomposición $n = a \cdot b$ no trivial (la descomposición trivial es aquella en la que $a = n$ y $b = 1$). En tal caso, y puesto que tanto a como b son menores que n , podemos aplicar el mismo algoritmo de forma recursiva hasta que recuperemos todos los factores primos. Esta es la razón por la que los algoritmos de factorización suelen limitarse a dividir n en dos factores.

También conviene apuntar el hecho de que, es mucho más eficiente comprobar si un número es primo que tratar de factorizarlo, por lo que normalmente se recomienda aplicar primero un *test de primalidad* para asegurarse de que el número puede descomponerse realmente de alguna manera no trivial.

Finalmente, queda la posibilidad de que n tenga un único factor, elevado a una potencia superior a 1. Afortunadamente, existen métodos capaces de verificar si n es una potencia perfecta x^k , con $k > 1$, por lo que todos los algoritmos que comentaremos en esta sección partirán de la suposición de que n tiene al menos dos factores primos diferentes.

El algoritmo más sencillo e intuitivo para tratar de factorizar un número n es probar a dividirlo por todos los números enteros positivos comprendidos entre 2 y \sqrt{n} . Evidentemente, este método es del todo inaceptable en cuanto n alcanza valores elevados, y ha sido ampliamente mejorado por otras técnicas que, sin llegar a ser realmente eficientes, son mucho más rápidas que la fuerza bruta. Algunos de los métodos más interesantes aparecidos hasta la fecha.

Método de Fermat

Para factorizar n , el método de Fermat intenta representarlo mediante la expresión

$$n = x^2 - y^2$$

con $x, y \in \mathbb{Z}$, $x, y \geq 1$. Es fácil ver que

$$n = (x + y)(x - y) = a \cdot b$$

donde a y b serán dos factores de n . El método de Fermat empieza tomando x_0 como el primer entero mayor que \sqrt{n} . Se comprueba entonces que $y_0 = x_0^2 - n$ es un cuadrado perfecto, y en caso contrario se calcula $x_{i+1} = x_i + 1$. Usando la siguiente expresión:

$$y_{i+1} = x_{i+1}^2 - n = (x_i + 1)^2 - n = x_i^2 - n + 2x_i + 1 = y_i + 2x_i + 1$$

se puede obtener el siguiente y_i haciendo uso únicamente de operaciones sencillas. En cuanto encontremos un y_i que sea un cuadrado perfecto, habremos dado con una factorización de n .

Por ejemplo, vamos a intentar factorizar el número 481:

$$x_0 = 22 \quad y_0 = 3 \quad 2x_0 + 1 = 45$$

$$x_1 = 23 \quad y_1 = 48 \quad 2x_1 + 1 = 47$$

$$x_2 = 24 \quad y_2 = 95 \quad 2x_2 + 1 = 49$$

$$x_3 = 25 \quad y_3 = 144$$

Como puede verse, y_3 es el cuadrado de 12, luego podemos poner:

$$481 = (25 + 12)(25 - 12) = 13 \cdot 37$$

Este método permite aún varios refinamientos, pero en cualquier caso resulta inviable cuando el número n a factorizar es lo suficientemente grande, ya que presenta un orden de complejidad para el peor caso de $O(\sqrt{n})$ nótese que al ser lineal en \sqrt{n} , resulta exponencial en el tamaño de n .

Método $p - 1$ de Pollard

Este método se basa en poseer un múltiplo cualquiera m de $p - 1$, siendo p un factor primo de n . Todo ello, por supuesto, sin conocer el valor de p . Para ello

necesitaremos definir el concepto de uniformidad. Diremos que n es B -uniforme si todos sus factores primos son menores o iguales a B .

Llegados a este punto, suponemos que p es un factor de n y $p - 1$ es $B1$ -uniforme, con $B1$ suficientemente pequeño. Calcularemos m como el producto de todos los números primos inferiores a $B1$, elevados a la máxima potencia que los deje por debajo de n . De esta forma, garantizamos que m es un múltiplo de $p - 1$, aunque no conozcamos el valor de p . Una vez obtenido el valor de m , el algoritmo de factorización queda como sigue:

1. Escoger un número a aleatorio dentro del conjunto $\{2, \dots, n - 1\}$.
2. Calcular $d = \text{mcd}(a, n)$. Si $d > 1$, d es un factor de n . Fin.
3. Calcular $x = (a^m \bmod n)$.
4. Calcular $d = \text{mcd}(x - 1, n)$. Si $d > 1$, d es un factor de n . Fin.
5. Devolver fallo en la búsqueda de factores de n . Fin.

Nótese que, en el paso 3, puesto que m es múltiplo de $p - 1$, x debería ser congruente con 1 módulo p , luego $x - 1$ debería ser múltiplo de p , por lo que el paso 4 debería devolver p .

Está demostrado que este algoritmo tiene un 50% de probabilidades de encontrar un valor de a que permita obtener un factor de n . Ejecutándolo, pues, varias veces, es bastante probable que podamos hallar algún factor de n .

Como ejemplo, vamos a tratar de factorizar el número 187, suponiendo que alguno de sus factores es 3-uniforme. En tal caso $m = 2^7 \cdot 3^4 = 10368$. Sea $a = 2$, entonces $x = (2^{10368} \bmod 187) = 69$. Calculando $\text{mcd}(69, 187)$ nos queda 17, que divide a 187, por lo que $187 = 17 \cdot 13$.

El orden de eficiencia de este algoritmo es de $O(B \log_B(n))$ operaciones de multiplicación modular, suponiendo que n tiene un factor p tal que $p - 1$ es B -uniforme.

Métodos Cuadráticos de Factorización

Los métodos cuadráticos de factorización se basan en la ecuación $x^2 \equiv y^2 \pmod{n}$

Siempre y cuando $x \not\equiv \pm y \pmod{n}$, tenemos que $(x^2 - y^2)$ es múltiplo de n , y por lo tanto

$$n \mid (x - y)(x + y)$$

Adicionalmente, puesto que tanto x como y son menores que n , n no puede ser divisor de $(x+y)$ ni de $(x-y)$. En consecuencia, n ha de tener factores comunes tanto con $(x+y)$ como con $(x-y)$, por lo que el valor $d = \text{mcd}(n, x-y)$ debe ser un divisor de n . Se puede demostrar que si n es impar, no potencia de primo y compuesto, entonces siempre se pueden encontrar

x e y .

Para localizar un par de números satisfactorio, en primer lugar elegiremos un conjunto

$$F = \{p_0, p_1, \dots, p_{t-1}\}$$

formado por t números primos diferentes, con la salvedad de que p_0 puede ser igual a -1 . Buscaremos ahora ecuaciones en congruencias con la forma

$$x_i^2 \equiv z_i \pmod{n}$$

tales que z_i se pueda factorizar completamente a partir de los elementos de F . El siguiente paso consiste en buscar un subconjunto de los z_i tal que el producto de todos sus elementos, al que llamaremos z , sea un cuadrado perfecto. Puesto que tenemos la factorización de los z_i , basta con escoger estos de forma que la multiplicidad de sus factores sea par. Este problema equivale a resolver un sistema de ecuaciones lineales con coeficientes en \mathbb{Z}_2 . Multiplicando los x_i^2 correspondientes a los factores de z escogidos, tendremos una ecuación del tipo que necesitamos, y por lo tanto una factorización de n .

Criba Cuadrática

Este método se basa en emplear un polinomio de la forma $q(x) = (x + m)^2 - n$ siendo $m = [\sqrt{n}]$, donde $[x]$ representa la parte entera de x . Puede comprobarse que

$$q(x) = x^2 + 2mx + m^2 - n \approx x^2 + 2mx$$

es un valor pequeño en relación con n , siempre y cuando x en valor absoluto sea pequeño. Si escogemos $x_i = a_i + m$ y $z_i = q(a_i)$, tendremos que se cumple la relación.

Lo único que nos queda es comprobar si z_i puede descomponerse totalmente con los elementos de F . Esto se consigue con la fase de criba, pero antes nos fijaremos en que si $p_i \in F$ divide a $q(x)$, también dividiría a $q(x + kp)$. Calcularemos la solución de la ecuación

$$q(x) \equiv 0 \pmod{p}$$

obteniendo una o dos series dependiendo del número de soluciones que tenga la ecuación de valores y tales que p divide a $q(y)$.

La criba propiamente dicha se lleva a cabo definiendo un vector $Q[x]$, con $-M \leq x \leq M$,

que se inicializa según la expresión $Q[x] = [\log |q(x)|]$. Sean x_1, x_2 las soluciones a $q(x) \equiv 0 \pmod{p}$.

Entonces restamos el valor $[\log(p)]$ a aquellas entradas $Q[x]$ tales que x sea igual a algún valor de las series de soluciones obtenidas en el paso anterior. Finalmente, los valores de $Q[x]$ que se aproximen a cero son los más susceptibles de ser descompuestos con los elementos de F , propiedad que se puede verificar de forma directa tratando de dividirlos.

Criba del Cuerpo de Números

Hoy por hoy es el algoritmo de factorización más rápido que se conoce, y fue empleado con éxito en 1996 para factorizar un número de 130 dígitos

decimales. Es una extensión de la criba cuadrática, que emplea una segunda base de factores, esta vez formada por polinomios irreducibles.

3.1.7 TESTS DE PRIMALIDAD

Como ya hemos dicho, no es viable tratar de factorizar un número para saber si es o no primo, pero existen métodos probabilísticos que nos pueden decir con un alto grado de certeza si un número es o no compuesto.

Método de Lehmann

Es uno de los tests más sencillos para saber si un número p es o no primo:

1. Escoger un número aleatorio $a < p$.
2. Calcular $b = a^{(p-1)/2} \pmod{p}$.
3. Si $b \not\equiv 1 \pmod{p}$ y $b \not\equiv -1 \pmod{p}$, p no es primo.
4. Si $b \equiv 1 \pmod{p}$ ó $b \equiv -1 \pmod{p}$, la probabilidad de que p sea primo es igual o superior al 50 %.

Repitiendo el algoritmo n veces, la probabilidad de que p supere el test y sea compuesto es decir, no primo será de 1 contra 2^n .

Método de Rabin-Miller

Es el algoritmo más empleado, debido a su facilidad de implementación. Sea p el número se quiere saber si es primo. Se calcula b , siendo b el número de veces que 2 divide a $(p-1)$, es decir, 2^b es la mayor potencia de 2 que divide a $(p-1)$. Calculamos entonces m , tal que $p-1 = 2^b * m$.

1. Escoger un número aleatorio $a < p$.
2. Sea $j = 0$ y $z = a^m \pmod{p}$.
3. Si $z = 1$, o $z = p-1$, entonces p pasa el test y puede ser primo.
4. Si $j > 0$ y $z = 1$, p no es primo.
5. Sea $j = j + 1$. Si $j = b$ y $z \neq p-1$, p no es primo.
6. Si $j < b$ y $z \neq p-1$, $z = z^2 \pmod{p}$. Volver al paso (4).
7. Si $j < b$ y $z = p-1$, entonces p pasa el test y puede ser primo.

8. p no es primo.

La probabilidad de que un número compuesto pase este algoritmo para un número a es del 25 %. Esto quiere decir que necesitaremos menos pasos para llegar al mismo nivel de confianza que el obtenido con el algoritmo de Lehmann.

Consideraciones Prácticas

A efectos prácticos, el algoritmo que se suele emplear para generar aleatoriamente un

número primo p es el siguiente:

1. Generar un número aleatorio p de n bits.
2. Poner a uno el bit más significativo garantizamos que el número es de n bits y el menos significativo debe ser impar para poder ser primo.
3. Intentar dividir p por una tabla de primos precalculados (usualmente aquellos que sean menores que 2000). Esto elimina gran cantidad de números no primos de una forma muy rápida. Baste decir a título informativo que más del 99.8% de los números impares no primos es divisible por algún número primo menor que 2000.
4. Ejecutar el test de Rabin-Miller sobre p como mínimo cinco veces.
5. Si el test falla, incrementar p en dos unidades y volver al paso 3.

Primos fuertes

Debido a que muchos algoritmos de tipo asimétrico basan su potencia en la dificultad para factorizar números enteros grandes, a lo largo de los años se propusieron diversas condiciones que debían cumplir los números empleados en aplicaciones criptográficas para que no fueran fáciles de factorizar. Se empezó entonces a hablar de números primos fuertes.

Sin embargo, en diciembre de 1998, Ronald Rivest y Robert Silverman publicaron un trabajo en el que quedaba demostrado que no era necesario emplear primos fuertes para los algoritmos asimétricos. En él se argumentaba

que la supuesta necesidad de números de este tipo surgió para dificultar la factorización mediante ciertos métodos como por ejemplo, el método “p-1”—, pero la aparición de técnicas más modernas como la de Lenstra, basada en curvas elípticas, o la criba cuadrática, hacía que se ganase poco o nada con el empleo de este tipo de números primos.

3.1.8 ANILLOS DE POLINOMIOS

Definición: Si tenemos un anillo conmutativo R , entonces un polinomio con variable x sobre el anillo R tiene la siguiente forma

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

donde cada $a_i \in R$ y $n \geq 0$. El elemento a_i se denomina coeficiente i -ésimo de $f(x)$, y el mayor m para el cual $a_m \neq 0$ se denomina grado de $f(x)$. Si $f(x) = a_0$ con $a_0 \neq 0$, entonces se dice que $f(x)$ tiene grado 0. Si todos los coeficientes de $f(x)$ valen 0, se dice que el grado de $f(x)$ es $-\infty$. Finalmente, un polinomio se dice mónico si su coeficiente de mayor grado vale 1.

Podemos definir las operaciones suma y producto de polinomios de la siguiente forma,

siendo $f(x) = a_n x^n + \cdots + a_0$ y $g(x) = b_m x^m + \cdots + b_0$:

Suma: $f(x) + g(x) = \sum c_i x^i$, donde $c_i = a_i + b_i$.

Producto: $f(x) \cdot g(x) = \sum c_i x^i$, donde $c_i = \sum a_j b_k$, tal que $j + k = i$.

La suma de polinomios cumple las propiedades asociativa, conmutativa, elemento neutro y elemento simétrico, mientras que el producto cumple la asociativa, conmutativa y elemento neutro. El conjunto de polinomios definidos en un anillo R , que notaremos $R[x]$, con las operaciones suma y producto, tiene en consecuencia estructura de anillo conmutativo.

Dados $f(x), g(x) \in R[x]$, existen dos polinomios únicos $c(x)$ y $r(x)$, tales que $f(x) = g(x)c(x) + r(x)$. Esta operación es la división de polinomios, donde $c(x)$ desempeña el papel de cociente, y $r(x)$ el de resto, y tiene propiedades

análogas a la de enteros. Eso nos permite definir una aritmética modular sobre polinomios, igual que la que ya hemos definido para enteros.

Definición: Se dice que $g(x)$ es congruente con $h(x)$ módulo $f(x)$, y se nota

$$g(x) \equiv h(x) \pmod{f(x)}$$

sí

$$g(x) = h(x) + k(x)f(x), \text{ para algún } k(x) \in R[x]$$

Definición: Un polinomio $f(x)$ en $R[x]$ induce un conjunto de clases de equivalencia de polinomios en $R[x]$, donde cada clase posee al menos un representante de grado menor que el de $f(x)$. La suma y multiplicación pueden llevarse a cabo, por tanto, módulo $f(x)$, y tienen estructura de anillo conmutativo.

Definición: Decimos que un polinomio $f(x) \in R[x]$ de grado mayor o igual a 1 es irreducible si no puede ser puesto como el producto de otros dos polinomios de grado positivo en $R[x]$.

Aunque no lo demostraremos aquí, se puede deducir que si un polinomio es irreducible, el conjunto de clases de equivalencia que genera tiene estructura de cuerpo. Nótese que en este caso, el papel que desempeñaba un número primo es ahora ocupado por los polinomios irreducibles.

Polinomios en \mathbb{Z}_n

Puesto que, como ya sabemos, \mathbb{Z}_n es un anillo conmutativo, podemos definir el conjunto $\mathbb{Z}_n[x]$ de polinomios con coeficientes en \mathbb{Z}_n .

Vamos a centrarnos ahora en el conjunto $\mathbb{Z}_2[x]$. En este caso, todos los coeficientes de los polinomios pueden valer únicamente 0 ó 1, por lo que un polinomio puede ser representado mediante una secuencia de bits. Por ejemplo, $f(x) = x^3 + x + 1$ podría representarse mediante el número binario 1011, y $g(x) = x^2 + 1$ vendría dado por el número 101.

Podemos ver que $f(x) + g(x) = x^3 + x^2 + x$, que viene dado por el número 1110. Puesto que las operaciones se realizan en Z_2 , esta suma podría haber sido realizada mediante una simple operación or-exclusivo entre los números binarios que representan a $f(x)$ y $g(x)$. Como vemos, sería muy fácil implementar estas operaciones mediante hardware, y ésta es una de las principales ventajas de trabajar en $Z_2[x]$.

Si escogemos un polinomio irreducible en Z_2 , podemos generar un cuerpo finito, o sea, un cuerpo de Galois. Dicho conjunto se representa como $GF(2^n)$, siendo n el grado del polinomio irreducible que lo genera, y tiene gran importancia en Criptografía, ya que algunos algoritmos de cifrado simétrico, como el estándar de cifrado AES, se basan en operaciones en $GF(2^n)$.

A modo de ejemplo, veamos cómo funciona la operación producto dentro de estos conjuntos.

Tomemos el polinomio $f(x) = x^8 + x^4 + x^3 + x + 1$, que es irreducible en $Z_2[x]$, y genera un cuerpo de Galois $GF(2^8)$. Vamos a multiplicar dos polinomios:

$$(x^5 + x) \cdot (x^4 + x^3 + x^2 + 1) = x^9 + x^8 + x^7 + x^5 + x^5 + x^4 + x^3 + x = x^9 + x^8 + x^7 + x^4 + x^3 + x$$

Nótese que $x^5 + x^5 = 0$, dado que los coeficientes están en Z_2 . Ahora hemos de tomar el resto módulo $f(x)$. Para ello emplearemos el siguiente truco:

$$x^8 + x^4 + x^3 + x + 1 \equiv 0 \pmod{f(x)} \Rightarrow x^8 \equiv x^4 + x^3 + x + 1 \pmod{f(x)}$$

luego

$$\begin{aligned} x^9 + x^8 + x^7 + x^4 + x^3 + x &= x(x^8) + x^8 + x^7 + x^4 + x^3 + x = \\ &= x(x^4 + x^3 + x + 1) + (x^4 + x^3 + x + 1) + x^7 + x^4 + x^3 + x = \\ &= x^5 + x^4 + x^2 + x + x^4 + x^3 + x + 1 + x^7 + x^4 + x^3 + x = \\ &= x^7 + x^5 + x^4 + x^4 + x^4 + x^3 + x^3 + x^2 + x + x + x + 1 = \\ &= x^7 + x^5 + x^4 + x^2 + x + 1 \end{aligned}$$

La ventaja esencial que posee este tipo de conjuntos es que permite llevar a cabo implementaciones muy sencillas y paralelizables de los algoritmos aritméticos. En realidad, aunque el orden de complejidad sea el mismo, se logra multiplicar la velocidad por una constante y simplificar el diseño de los circuitos, por lo que se obtienen sistemas con mayores prestaciones, y a la vez más baratos.

3.2 ALGORITMOS DE CIFRADO ASIMÉTRICO

3.2.1 INTRODUCCIÓN

Los algoritmos de llave pública, o algoritmos asimétricos, han demostrado su interés para ser empleados en redes de comunicación inseguras (Internet). Introducidos por Whitfield Diffie y Martin Hellman a mediados de los años 70, su novedad fundamental con respecto a la criptografía simétrica es que las claves no son únicas, sino que forman pares. Hasta la fecha han aparecido multitud de algoritmos asimétricos, la mayoría de los cuales son inseguros; otros son poco prácticos, bien sea porque el criptograma es considerablemente mayor que el mensaje original, bien sea porque la longitud de la clave es enorme. Se basan en general en plantear al atacante problemas matemáticos difíciles de resolver. En la práctica muy pocos algoritmos son realmente útiles. El más popular por su sencillez es RSA, que ha sobrevivido a multitud de ataques, si bien necesita una longitud de clave considerable.

3.2.2 APLICACIONES DE LOS ALGORITMOS ASIMÉTRICOS

Los algoritmos asimétricos poseen dos claves diferentes en lugar de una, K_p y K_P , denominadas clave privada y clave pública. Una de ellas se emplea para codificar, mientras que la otra se usa para decodificar. Dependiendo de la aplicación que se le dé al algoritmo, la clave pública será la de cifrado o viceversa. Para que estos criptosistemas sean seguros también ha de cumplirse que a partir de una de las claves resulte extremadamente difícil calcular la otra.

Protección de la información

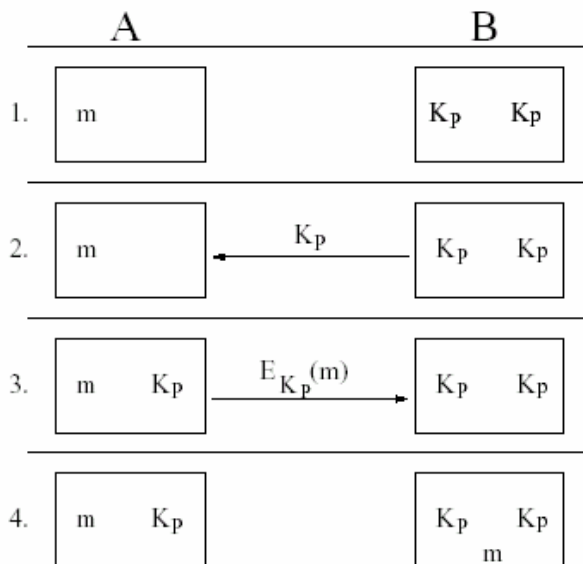


Figura 1.

Una de las aplicaciones inmediatas de los algoritmos asimétricos es el cifrado de la información sin tener que transmitir la clave de decodificación, lo cual permite su uso en canales inseguros. Supongamos que A quiere enviar un mensaje a B (figura 1). Para ello solicita a B su clave pública K_p . A genera entonces el mensaje cifrado $E_{K_p}(m)$. Una vez hecho esto únicamente quien posea la clave K_p —en el ejemplo, B— podrá recuperar el mensaje original m .

Para este tipo de aplicación, la llave que se hace pública es aquella que permite codificar los mensajes, mientras que la llave privada es aquella que permite descifrarlos.

Autenticación

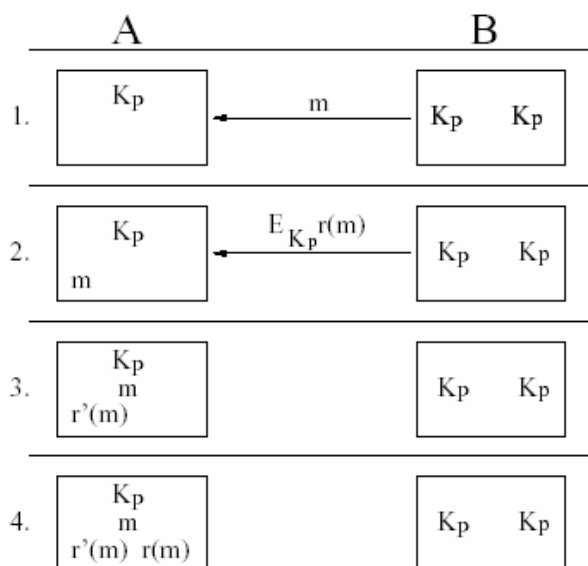


Figura 2.

La segunda aplicación de los algoritmos asimétricos es la autenticación de mensajes, que nos permiten obtener una firma digital a partir de un mensaje. Dicha firma es mucho más pequeña que el mensaje original, y es muy difícil encontrar otro mensaje de lugar a la misma. Supongamos que A recibe un mensaje m de B y quiere comprobar su autenticidad. Para ello B genera un resumen del mensaje $r(m)$ (ver figura 2) y lo codifica empleando la clave de cifrado, que en este caso será privada.

En este caso la clave que se emplea para cifrar es la clave privada, justo al revés que para la simple codificación de mensajes.

En muchos de los algoritmos asimétricos ambas claves sirven tanto para cifrar como para descifrar, de manera que si se emplea una para codificar, la otra

permitirá decodificar y viceversa. Esto ocurre con el algoritmo RSA, en el que un único par de claves es suficiente para codificar y autenticar.

3.2.3 ALGORITMO RSA

Sus claves sirven indistintamente tanto para codificar como para autenticar. Debe su nombre a sus tres inventores: Ronald Rivest, Adi Shamir y Leonard Adleman, y estuvo bajo patente de los Laboratorios RSA hasta el 20 de septiembre de 2000, por lo que su uso comercial estuvo restringido hasta esa fecha.

El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número.

Ahora bien, si el número considerado es un número primo (el que sólo es divisible por 1 y por él mismo), tendremos que para factorizarlo habría que empezar por 1, 2, 3,... hasta llegar a él mismo, ya que por ser primo ninguno de los números anteriores es divisor suyo. Y si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo. (*ver sección 3.1.5 algoritmos de factorización*).

Basado en la exponenciación modular de exponente y módulo fijos, el sistema RSA crea sus claves de la siguiente forma:

Algoritmo para generar un par de llaves (KP ,Kp),

1. Se eligen aleatoriamente dos números primos grandes, (**p** y **q** de entre 100 y 300 dígitos). Después se calcula el producto $n = pq$.
2. Los valores **p** y **q** no se hacen públicos.

3. Se escoge un número e primo relativo con $(p - 1)(q - 1)$. (e, n) será la clave pública. Nótese que e debe tener inversa módulo $(p-1)(q-1)$,
4. Existirá un número d tal que

$$de \equiv 1 \pmod{(p - 1)(q - 1)}$$

es decir, que d es la inversa de e módulo $(p - 1)(q - 1)$. (d, n) será la clave privada. Esta inversa puede calcularse fácilmente empleando el Algoritmo Extendido de Euclides. Nótese que si desconocemos los factores de n , este cálculo resulta prácticamente imposible.

La codificación se lleva a cabo según la expresión:

$$c = m^e \pmod{n}$$

mientras que la decodificación se hará de la siguiente forma:

$$m = c^d \pmod{n}$$

ya que

$$c^d = (m^e)^d = m^{ed} = m^{k(p-1)(q-1)+1} = (m^k)^{(p-1)(q-1)} m$$

Recordemos que $\phi(n) = (p-1)(q-1)$, por lo que, según la ecuación (Teorema Función de Euler),

$$(m^k)^{(p-1)(q-1)} = 1,$$

lo cual nos lleva de nuevo a m , siempre y cuando m y n sean primos relativos.

Ya que en nuestro caso n es compuesto, puede ocurrir que no sea primo relativo con m .

Para ver lo que ocurre, podemos llevar a cabo el siguiente razonamiento: buscamos un número a tal que

$$m^a \equiv 1 \pmod{n}$$

Tiene que cumplirse que $m^a \equiv 1 \pmod{p}$ y $m^a \equiv 1 \pmod{q}$, ya que p y q dividen a n .

Aplicando el Teorema de Fermat (3.1.5 Algoritmos de Factorización), tenemos que a debe ser múltiplo de $(p - 1)$ y de $(q - 1)$, por lo que $a = \text{mcm}(p - 1, q - 1)$. Ya que el mínimo común múltiplo de $(p - 1)$ y $(q - 1)$ divide a $(p - 1)(q - 1)$, el razonamiento dado inicialmente para demostrar el buen funcionamiento del algoritmo sigue siendo válido. Por esta razón, en muchos lugares se propone obtener d de forma que:

$$de \equiv 1 \pmod{\text{mcm}(p - 1, q - 1)}$$

con lo que obtendremos valores más pequeños, y por lo tanto más manejables, para la clave de descifrado.

En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo).

RSA basa su seguridad en ser una función computacionalmente segura, ya que si bien realizar la exponenciación modular es fácil, su operación inversa, la extracción de raíces de módulo \emptyset no es factible a menos que se conozca la factorización de e , clave privada del sistema.

3.3 OTROS ALGORITMOS ASIMÉTRICOS

3.3.1 ALGORITMO DE DIFFIE-HELLMAN

Es un algoritmo asimétrico, basado en el problema de Diffie-Hellman⁸, que se emplea fundamentalmente para acordar una clave común entre dos interlocutores, a través de un canal de comunicación inseguro. La ventaja de este sistema es que no son necesarias llaves públicas en el sentido estricto, sino una información compartida por los dos comunicantes.

Sean A y B los interlocutores en cuestión. En primer lugar, se calcula un número primo p y un generador α de \mathbb{Z}^*_p , con $2 \leq \alpha \leq p - 2$. Esta información es pública y conocida por ambos.

El algoritmo queda como sigue:

1. A escoge un número aleatorio x , comprendido entre 1 y $p - 2$ y envía a B el valor $\alpha^x \pmod{p}$
2. B escoge un número aleatorio y , análogamente al paso anterior, y envía a A el valor $\alpha^y \pmod{p}$.
3. B recoge α^x y calcula $K = (\alpha^x)^y \pmod{p}$.
4. A recoge α^y y calcula $K = (\alpha^y)^x \pmod{p}$.

Puesto que x e y no viajan por la red, al final A y B acaban compartiendo el valor de K , sin que nadie que capture los mensajes transmitidos pueda repetir el cálculo.

El algoritmo Diffie-Hellman fue el primer algoritmo asimétrico. Solamente se puede utilizar para intercambiar claves simétricas, pero esto es una de las

⁸ Ver Anexo 1

principales funciones de los algoritmos asimétricos, así está muy extendido en sistemas de Internet con confidencialidad de clave simétrica (VPNs, SSL, etc.).

La seguridad del algoritmo depende de la dificultad del cálculo de un logaritmo discreto. Esta función es la inversa de la potencia discreta, o sea, de calcular una potencia y aplicar una función mod.

- Potencia discreta: $Y = X^a \bmod q$
- Logaritmo discreto: $X = L_{a,q}(Y)$

La generación de claves públicas es la siguiente:

- Se busca un número grande y primo llamado q .
- Se busca a raíz primitiva de q . Para ser raíz primitiva debe cumplir que: $a \bmod q, a^2 \bmod q, a^3 \bmod q, \dots, a^{q-1} \bmod q$ son números diferentes.
- a y q son claves públicas.

Para compartir una clave simétrica se realiza el proceso siguiente:

Las K calculadas por los dos usuarios son iguales por la propiedad distributiva de la multiplicación.

Para romper el sistema solo se dispone de las Y_i , q y a . Por lo tanto es necesario conocer alguna de las dos X_i , para esto se debe realizar el logaritmo discreto $L_{a,q}(Y_i)$ y esta operación no tiene solución analítica para números grandes.

En un sistema con múltiples usuarios que quieren compartir claves simétricas uno a uno se publican todas las Y_i en un directorio accesible. Cuando se quiere enviar un mensaje cifrado con otro usuario se realiza el proceso siguiente:

- El emisor coge del directorio la Y_R del receptor.

- El emisor calcula la clave K con su número secreto X_E .
- Se envía el mensaje cifrado con K .
- El receptor, para calcular K , utiliza su número secreto X_R y coge del directorio la Y_E del emisor.

3.3.2 ALGORITMO DE ELGAMAL

Fue diseñado en un principio para producir firmas digitales, pero posteriormente se extendió también para codificar mensajes. Se basa en el problema de los logaritmos discretos, que está íntimamente relacionado con el de la factorización, y en el de Diffie-Hellman.

Para generar un par de llaves, se escoge un número primo n y dos números aleatorios p y x menores que n . Se calcula entonces

$$y = p^x \pmod{n}$$

La llave pública es (p, y, n) , mientras que la llave privada es x .

Escogiendo n primo, garantizamos que sea cual sea el valor de p , el conjunto $\{p, p^2, p^3, \dots\}$ es una permutación del conjunto $\{1, 2, \dots, n-1\}$. Nótese que esto no es necesario para que el algoritmo funcione, por lo que podemos emplear realmente un n no primo, siempre que el conjunto generado por las potencias de p sea lo suficientemente grande.

3.3.3 ALGORITMO DE RABIN

El sistema de llave asimétrica de Rabin se basa en el problema de calcular raíces cuadradas módulo un número compuesto. Este problema se ha demostrado que es equivalente al de la factorización de dicho número.

En primer lugar escogemos dos números primos, p y q , ambos congruentes con 3 módulo 4 (los dos últimos bits a 1). Estos primos son la clave privada. La clave pública es su producto, $n = pq$.

Para codificar un mensaje m , simplemente se calcula

$$c = m_2 \pmod{n}$$

La decodificación del mensaje se hace calculando lo siguiente:

$$m_1 = c(p+1)/4 \pmod{p}$$

$$m_2 = (p - c(p+1)/4) \pmod{p}$$

$$m_3 = c(q+1)/4 \pmod{q}$$

$$m_4 = (q - c(q+1)/4) \pmod{q}$$

Luego se escogen a y b tales que $a = q(q-1 \pmod{p})$ y $b = p(p-1 \pmod{q})$. Los cuatro

posibles mensajes originales son

$$m_a = (am_1 + bm_3) \pmod{n}$$

$$m_b = (am_1 + bm_4) \pmod{n}$$

$$m_c = (am_2 + bm_3) \pmod{n}$$

$$m_d = (am_2 + bm_4) \pmod{n}$$

Desgraciadamente, no existe ningún mecanismo para decidir cuál de los cuatro es el auténtico, por lo que el mensaje deberá incluir algún tipo de información para que el receptor pueda distinguirlo de los otros.

3.3.4 ALGORITMO DSA

El algoritmo DSA (Digital Signature Algorithm) es una parte del estándar de firma digital DSS (Digital Signature Standard). Este algoritmo, propuesto por el NIST, data de 1991, es una variante del método asimétrico de ElGamal.

Creación del par llave pública-llave privada

El algoritmo de generación de claves es el siguiente:

1. Seleccionar un número primo q tal que $2^{159} < q < 2^{160}$.
3. Escoger t tal que $0 \leq t \leq 8$, y seleccionar un número primo p tal que $2^{511+64t} < p < 2^{512+64t}$, y que además q sea divisor de $(p - 1)$.
4. Seleccionar un elemento $g \in \mathbb{Z}_p^*$
5. $\alpha = g^{(p-1)/q} \pmod{p}$ y calcular α .
4. Si $\alpha = 1$ volver al paso 3.
5. Seleccionar un número entero aleatorio a , tal que $1 \leq a \leq q - 1$
6. Calcular $y = \alpha^a \pmod{p}$.
7. La clave pública es (p, q, α, y) . La clave privada es a .

Siendo h la salida de una función resumen sobre el mensaje m , la generación de una firma se hace mediante el siguiente algoritmo:

1. Seleccionar un número aleatorio k tal que $0 < k < q$.
2. Calcular $r = (\alpha^k \pmod{p}) \pmod{q}$.
3. Calcular $k^{-1} \pmod{q}$.
4. Calcular $s = k^{-1}(h + ar) \pmod{q}$.
5. La firma del mensaje m es el par (r, s) .

El destinatario efectuará las siguientes operaciones, suponiendo que conoce la clave pública (p, q, α, y) , para verificar la autenticidad de la firma:

1. Verificar que $0 < r < q$ y $0 < s < q$. En caso contrario, rechazar la firma.
2. Calcular el valor de h a partir de m .
3. Calcular $w = s^{-1} \pmod{q}$.
4. Calcular $u_1 = w \cdot h \pmod{q}$ y $u_2 = w \cdot r \pmod{q}$.
5. Calcular $v = (\alpha^{u_1} y^{u_2} \pmod{p}) \pmod{q}$.
6. Aceptar la firma si y sólo si $v = r$.

3.4 LOS PROTOCOLOS SSL Y TLS

SSL

SSL (Secure Layer Socket) es una tecnología desarrollada por **Netscape** en 1994 junto con su primer navegador, para asegurar la privacidad y fiabilidad de las comunicaciones entre dos aplicaciones. Utiliza un sistema de encriptación asimétrico basado en claves publica/privada para negociar una clave que luego se utilizará para establecer una comunicación basada en encriptación simétrica. **SSL** es el protocolo de encriptación más utilizado en Internet en estos momentos y es el más usado en servidores web donde se solicita información confidencial, además es abierto y de dominio público, trabaja cliente / servidor y su implementación es sencilla.

TLS (Transport Layer Security) es un nuevo protocolo muy similar a SSL, ya que de hecho se basa en la versión 3.0 de este último, mejorándolo en algunos aspectos. Si bien su nivel de implantación aún no es muy elevado, todo parece indicar que está llamado a ser su sustituto.



La seguridad de SSL actualmente proporciona servicios de encriptación de datos, servidor de autenticación, integridad de mensaje y autenticación de cliente para una conexión de TCP/IP.

- Cifrado de datos: la información transferida se cifra utilizando un algoritmo de clave secreta, capaz de cifrar grandes volúmenes de información en muy poco tiempo, por lo que resultará ininteligible en manos de un atacante, garantizando así la confidencialidad.
- Autenticación de servidores: el usuario puede asegurarse de la identidad del servidor al que se conecta y al que posiblemente envíe información personal confidencial. De esta forma se evita que un usuario se conecte a un servidor impostor que haya copiado las páginas del banco o comercio al que

suplanta. Estos ataques se conocen como Web spoofing, y se utilizan para hacerse con las contraseñas y números de tarjeta de crédito de los usuarios.

- Integridad de mensajes: se impide que pasen inadvertidas modificaciones intencionadas o accidentales en la información mientras viaja por Internet.
- Además opcionalmente, autenticación de cliente: permite al servidor conocer la identidad del usuario, con el fin de decidir si puede acceder a ciertas áreas protegidas. En este caso, el cliente debe tener instalado un certificado en su ordenador o en una tarjeta inteligente, que le permitirá autenticarse ante el servidor web. Se evitan así ataques comunes de captación de contraseñas mediante el uso de analizadores de protocolos (sniffers) o la ejecución de reventadores de contraseñas. De todas formas, son muy pocos los servidores web que autentican a los usuarios de esta manera.

SSL puede tener una clave de sesión de 40 bits o de 128 bits, dicha clave es generada en cada transacción. La longitud de la clave hará más difícil romper la envoltura de encriptación. La mayoría de los navegadores soportan una clave de 40 bits para sesiones SSL, mientras que las últimas versiones de Internet Explorer y Netscape soportan claves de sesión de 128 bits, ésta última es un trillón de veces más segura que una de 40 bits.

Un sitio puede identificarse como seguro si su dirección URL en vez de comenzar con **http://** comienza con **https://** o si en el navegador aparece algún indicador de sitio certificado (Netscape muestra una llave , mientras que Internet Explorer muestra un candado , en la parte inferior izquierda de la ventana).

Alguien mal intencionado podría producir ataques sobre el protocolo en la comunicación a través de la red, sobre los mensajes intercambiados entre el cliente y el servidor. Entre las diversas operaciones ilícitas que se prevenirían sobre los mensajes están:

- Sustitución.
- Eliminación.
- Interceptación.
- Descripción

Funcionamiento de SSL

Técnicamente SSL usa una capa (layer) ubicada entre el protocolo de hipertexto (HTTP) y el protocolo de transporte (TCP). SSL está incluido como parte de Internet Explorer y en Netscape (y la mayoría de productos para el web), y se incluye en el modelo de TCP en medio de las capas de transporte y aplicaciones como se muestra en la figura 3

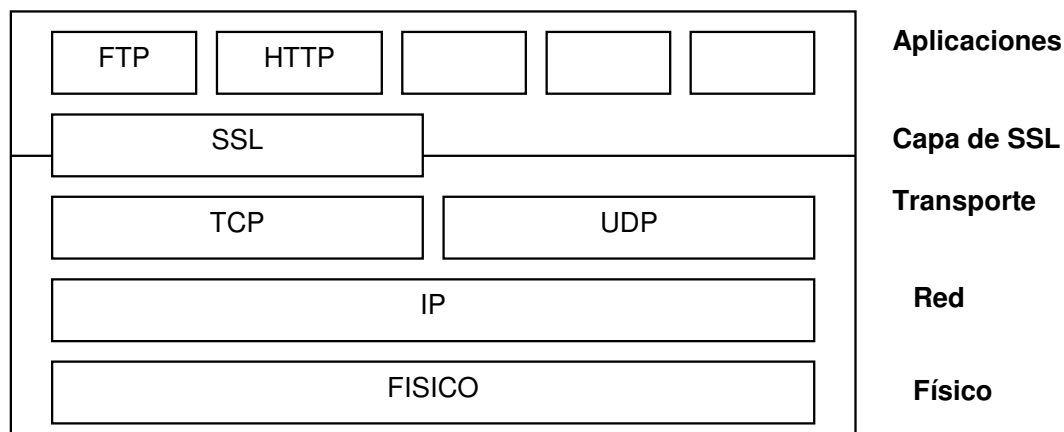


Figura 3. MODELO TCP/IP

SSL tiene dos fases en su proceso de comunicación. En la primera fase se establece una comunicación basada en encriptación asimétrica donde el cliente y el servidor intercambian los primeros mensajes y realizan la negociación de los parámetros de la sesión. Esta fase esta soportada por un protocolo conocido como HandShake⁹ (estrechamiento de manos), para la cual se emplean habitualmente los certificados X.509,(sección Métodos de Autenticación). En la segunda fase se establece la verdadera sesión de comunicación donde las aplicaciones intercambian información.

Implementación de SSL

Para implementar SSL se necesita mucho mas que marcar las opciones de seguridad del navegador que se esté usando, requiere de una entidad certificadora. A continuación se describirán muchos de los aspectos importantes para implementar SSL.

Servidor SSL

Los usuarios no realizarán negocios en un sitio web, a menos que tengan la certeza de que sea seguro. Necesitan saber que su negocio es real y que sus comunicaciones son privadas. Al mismo tiempo, usted necesita proteger su comercio electrónico de las ventas que se encuentran en controversia o de las personas que "husmean" su sitio y le quitan los clientes.

Un Servidor SSL es aquel que sirve como administrador de certificados digitales, y que generalmente esta instalado en las instalaciones de la misma compañía que ofrece sus servicios en la web (ya sea de Intranet, Extranet o Internet), o es perteneciente a una CA (Certified Authority).

⁹ Durante el protocolo SSL Handshake, el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad.

Sus funciones son:

- **Verificación de la Identidad:** Emitir al servidor del cliente un Certificado Digital único, asegurándole la autenticidad a las personas que visitan su sitio web y permitiendo que las comunicaciones se encripten para obtener mayor privacidad, y confiabilidad en las transacciones de comercio o de comunicación.
- **Mantener la seguridad:** Un servidor SSL debe mantener la seguridad e integridad de la información a través del método de clave pública/privada.
- **Facilidad de Utilización:** A pesar de la gran seguridad que debe tener, el servicio debe ser de fácil uso para los clientes sin grandes traumatismos que ocasionen confusiones.

Certificado Digital

Un certificado digital es un bloque de caracteres que acompaña a un documento o archivo acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema criptográfico asimétrico), a la que sólo el tiene acceso, lo que impide que pueda después negar su autoría (no revocación o no repudio). De esta forma, el autor queda vinculado al documento de la firma. La validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

¿ Cómo se realiza certificado digital ?

El software del firmante aplica un algoritmo *hash* ¹⁰sobre el texto a firmar, obteniendo un extracto de longitud fija, y absolutamente específico para ese mensaje. Un mínimo cambio en el mensaje produciría un extracto completamente diferente, y por tanto no correspondería con el que originalmente firmó el autor. Los algoritmos *hash* más utilizados son el MD5 ó SHA-1¹¹. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits (según el algoritmo utilizado), se somete a continuación a cifrado mediante la clave secreta del autor. El algoritmo más utilizado en este procedimiento de encriptación asimétrica es el RSA(ya que este utiliza llaves públicas). De esta forma obtenemos un extracto final cifrado con la clave privada del autor, el cual se añadirá al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por aquella persona interesada que disponga de la clave pública del autor.

¿ Cómo se comprueba la validez del certificado digital ?

Para poder verificar la validez del documento o archivo, es necesario la clave pública del autor. El procedimiento sería el siguiente: el software del receptor, previa introducción en el mismo de la clave pública de remitente (obtenida a través de una Autoridad de Certificación), descifraría el extracto cifrado del autor y a continuación calcularía el extracto hash que le correspondería al texto del mensaje y, si el resultado coincide con el extracto anteriormente descifrado, se considera válida; en caso contrario significaría que el documento ha sufrido una modificación posterior y por lo tanto no es válido.

¹⁰ Ver sección 3.2.5 Métodos de Autenticación

¹¹

¿ Cómo es la encriptación de un certificado digital?

Hay dos tipos de encriptación, la encriptación simétrica que obliga a los dos interlocutores (emisor y receptor) del mensaje a utilizar la misma clave para cifrar y descifrar el mismo (como por ejemplo el criptosistema DES¹², Data Encryption Standard, desarrollado por IBM), y la encriptación asimétrica o criptográfica de claves públicas que está basada en el concepto de pares de claves, de forma que cada uno de los elementos del par (una clave) puede cifrar información que solo la otra componente del par (la otra clave) puede descifrar. El par de claves se asocia con un solo interlocutor, así un componente del par (la clave privada) solamente es conocida por su propietario mientras que la otra parte del par (la clave pública) se publica ampliamente para que todos la conozcan (en este caso destaca el famoso criptosistema).

Clases de Certificados. Utilidad.

Certificados de Servidor.

El Certificado de Servidor aporta a un WEB SITE la característica de seguridad y confianza necesaria para poder entablar cualquier tipo de relación con los potenciales usuarios. Es el elemento necesario para poder aprovechar la gran vía de negocio que supone el comercio a través de Internet con la máxima rentabilidad y seguridad.

Los Certificados de Servidor permiten incorporar el protocolo SSL (Secure Socket Layer) en un servidor Web. Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando la información que se envía a ambos puntos protegiendo los datos personales, datos de tarjetas de crédito, números de cuenta, contraseñas, etcétera. Cobra especial importancia

¹² Algoritmo simétrico de cifrado

dentro del área del comercio electrónico, donde la seguridad de los datos es la principal barrera para el desarrollo de este sistema.

Certificados para WAP

Los Certificados WAP permiten a las WEB comerciales existentes y de nueva creación la realización de transacciones seguras con los consumidores móviles. Los nuevos portales basados en transacciones móviles seguras expandirán el comercio electrónico entre los usuarios móviles y los WEB SITES dedicados al comercio. Los servidores WAP necesitan proporcionar seguridad y confianza a los usuarios potenciales, realmente esta es la base para que se establezca una contraprestación que satisfaga a ambas partes.

Los Certificados WAP permiten mantener conexiones seguras basadas en encriptación y autenticación con dispositivos de telefonía móvil. Actualmente por ejemplo una de las compañías más interesadas en el tema de seguridad móvil es Microsoft puesto que dentro de su estrategia .net, la seguridad es clave para el éxito del “Anytime – Anywhere”.

Certificados Personales

Otorgan seguridad a los correos electrónicos basados en un standard S/MIME¹³. Un usuario puede firmar o cifrar los mensajes de correo para asegurarse de que sólo el receptor designado sea el lector de su mensaje.

¹³ Protocolo que soporta Codificación de Mensajes

CA's Corporativas

Es la solución óptima para las empresas que quieran disponer de un sistema de generación de cualquier tipo de Certificado para sus usuarios (trabajadores, proveedores, clientes, etc.) y servidores.

Una CA Corporativa puede generar cualquier tipo de certificado, ya sean Certificados Personales, de Servidor, para WAP, para firmar Código e incluso para IPSec-VPN (Windows 2000 es un ejemplo de ésta labor de certificación).

En función del tipo de funcionalidad que se le quiera dar a la CA deberá escogerse un diferente tipo de CA Corporativa.

Certificados para firmar Código

El Certificado para la Firma de Código, permitirá a un Administrador, Desarrollador o Empresa de Software firmar su Software (ActiveX, Applets Java, Plug-ins, etc.) y Macros, y distribuirlo de una forma segura entre sus clientes.

Certificados para IPSec-VPN

Los Certificados para VPN son los elementos necesarios para que la empresa aproveche las cualidades y ventajas de la utilización de las VPNs de un modo plenamente seguro.

Las VPNs surgen como consecuencia de la creciente demanda de Seguridad en las comunicaciones ya sea entre Router-Router o Cliente-Servidor. La apertura de las redes corporativas a empleados remotos (con gran importancia en el caso del Teletrabajo), sucursales, business partners o clientes (Apache de Linux, ISA Server de Microsoft y Border Manager de Novell emplean estos mecanismos en sus proxy server).

Información del certificado

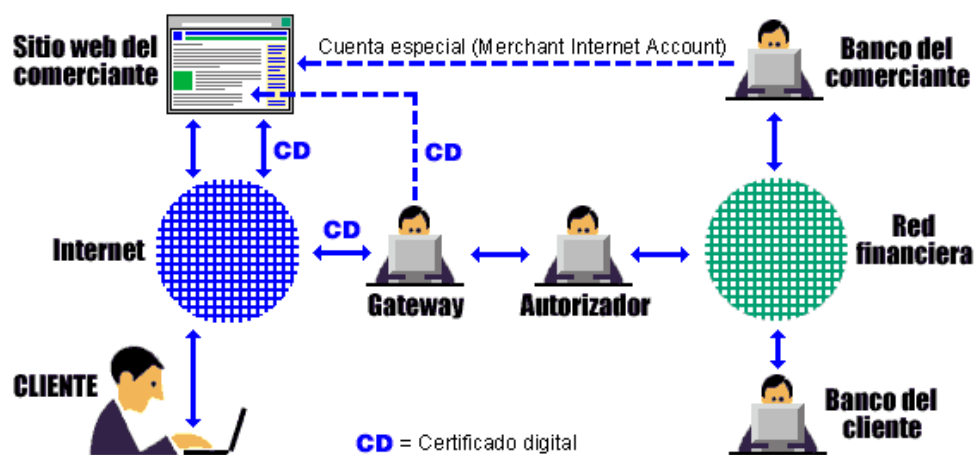
El proceso de certificación requiere que el propietario del certificado suministre cierta información de identificación:

- El nombre común o de sistema completo del servidor (como por ejemplo: `hostname.netscape.com`)
- Nombre de departamento, opcional
- Nombre legal y registrado de la organización
- Localidad o ciudad donde la organización reside o está registrada
- Nombre de la provincia o estado
- Nombre del país
- También se suministra información similar acerca de la autoridad emisora del certificado. El certificado está identificado por:
- Número de serie
- Fecha de inicio y caducidad de la validación
- Huella digital del certificado (en números hexadecimales)

Usos actuales de SSL

Compras por Internet

SISTEMA DE PAGO TIPICO EN INTERNET



1. El comerciante pone su sitio en Internet, y, si quiere habilitarlo para pagos en línea, pide a su banco una **cuenta corriente especial** ("Merchant Internet Account").
2. El comerciante contrata un servicio de "**Gateway**" para que conecte su sitio web con el sistema de autorizaciones del sector financiero. Este trámite lo hace por cuenta propia, o se lo hace su ISP.
3. El Gateway le expide un **certificado digital** para instalar en su sitio web, a fin de validar siempre su autenticidad.

4. El cliente entra al sitio web del comerciante y hace sus compras comunicándose en forma encriptada de acuerdo con el **protocolo "SSL"**, sin necesidad de poseer certificado digital.
5. El sitio web del comerciante transmite **en línea y en tiempo real** la información al Gateway por protocolo SSL, y el Gateway hace lo propio ante el sistema de autorizaciones. El sistema financiero responde en línea y en tiempo real. El Gateway transmite esta respuesta al sitio web del comerciante.
6. El sitio web del comerciante informa al cliente de inmediato, **en línea y en tiempo real**, si la operación no ha sido exitosa.
7. El comerciante conserva la información de la operación, la cual **incluye** el número de tarjeta de crédito del cliente, y asume esa responsabilidad.
8. Si el cliente rechaza el cargo, al comerciante se le debita el importe. Si le sustraen los números de las tarjetas de crédito y ocurren fraudes, **el comerciante responde**.

VPN's

SSL permite asegurar el túnel de VPN haciéndolo un canal blindado en contra de ataques de hackers y permitiendo intercambio de información segura.

Adicionalmente es perfecto para:

- Comunicaciones Business-to-business, B2C, C2C, etcétera.
- Transacciones bancarias.

- Tiendas Online.
- Proveedores de servicios
- Correo certificado
- Administración y mercadeo
- Administración y seguridad frente a usuarios móviles

Las VPN's con SSL brindan niveles de seguridad excelentes que permiten el establecimiento de Intranets con confianza y tranquilidad.

3.5 METODOS DE AUTENTIFICACIÓN

Se considera autenticación a cualquier método que permita comprobar de manera segura alguna característica sobre un objeto. Dicha característica puede ser su origen, su integridad, su identidad, etc. Se consideran tres grandes tipos dentro de los métodos de autenticación:

- *Autenticación de mensaje.* Garantiza la procedencia de un mensaje conocido, de forma que podamos asegurarnos de que no es una falsificación. Este mecanismo se conoce habitualmente como *firma digital*.
- *Autenticación de usuario mediante contraseña.* En este caso se trata de garantizar la presencia de un usuario legal en el sistema. El usuario deberá poseer una contraseña secreta que le permita identificarse.
- *Autenticación de dispositivo.* Se trata de garantizar la presencia de un dispositivo válido. Este dispositivo puede estar solo o tratarse de una llave electrónica que sustituye a la contraseña para identificar a un usuario.

Firmas digitales. Función Resumen

La criptografía asimétrica permite autenticar información, es decir, asegura que un mensaje m provenga de un emisor A y no de cualquier otro. La

autenticación debe hacerse empleando una función resumen y no codificando el mensaje completo. Las funciones resumen también se conocen como MCD (modificación de detección de código), que va a permitir crear firmas digitales.

Un mensaje m puede ser autenticado codificando con la llave privada K_p el resultado de aplicarle una función resumen, $EK_p(r(m))$. Esa información adicional (que denominaremos firma o signatura del mensaje m) sólo puede ser generada por el poseedor de la clave privada K_p . Cualquiera que tenga la llave pública correspondiente estará en condiciones de decodificar y verificar la firma. Para que sea segura, la función resumen $r(x)$ debe cumplir además ciertas características:

$r(m)$ es de longitud fija, independientemente de la longitud de m .

Dado m , es fácil calcular $r(m)$.

Dado $r(m)$, es computacionalmente intratable recuperar m .

Dado m , es computacionalmente intratable obtener un m' tal que $r(m) = r(m')$.

Algoritmo MD5

Se trata de uno de los más populares algoritmos de generación de signaturas(firmas digitales), debido en gran parte a su inclusión en las primeras versiones de PGP. Resultado de una serie de mejoras sobre el algoritmo MD4, diseñado por Ron Rivest, procesa los mensajes de entrada en bloques de 512 bits, y produce una salida de 128 bits.

Siendo m un mensaje de b bits de longitud, en primer lugar se alarga m hasta que su longitud sea exactamente 64 bits inferior a un múltiplo de 512. El alargamiento se lleva a cabo añadiendo un 1 seguido de tantos ceros como sea necesario. En segundo lugar, se añaden 64 bits con el valor de b , empezando por el byte menos significativo. De esta forma tenemos el mensaje como un

número entero de bloques de 512 bits, y además le hemos añadido información sobre su longitud.

Seguidamente, se inicializan cuatro registros de 32 bits con los siguientes valores hexadecimales

A = 67452301

B = EFCDAB89

C = 98BADCFE

D = 10325476

Posteriormente comienza el lazo principal del algoritmo, que se repetirá para cada bloque de 512 bits del mensaje. En primer lugar copiaremos los valores de A, B, C y D en otras cuatro variables, a, b, c y d. Luego definiremos las siguientes cuatro funciones:

$$F(X, Y, Z) = (X \wedge Y) \vee ((\neg X) \wedge Z)$$

$$G(X, Y, Z) = (X \wedge Z) \vee ((Y \wedge (\neg Z)))$$

$$H(X, Y, Z) = X \oplus Y \oplus Z$$

$$I(X, Y, Z) = Y \oplus (X \vee (\neg Z))$$

Ahora representaremos por m_j el j -ésimo bloque de 32 bits del mensaje m (de 0 a 15), y

definiremos otras cuatro funciones:

$$FF(a, b, c, d, m_j, s, t_i) \text{ representa } a = b + ((a + F(b, c, d) + m_j + t_i) \ll s)$$

$$GG(a, b, c, d, m_j, s, t_i) \text{ representa } a = b + ((a + G(b, c, d) + m_j + t_i) \ll s)$$

$$HH(a, b, c, d, m_j, s, t_i) \text{ representa } a = b + ((a + H(b, c, d) + m_j + t_i) \ll s)$$

$$II(a, b, c, d, m_j, s, t_i) \text{ representa } a = b + ((a + I(b, c, d) + m_j + t_i) \ll s)$$

donde la función $a \ll s$ representa desplazar circularmente el valor a s bits a la izquierda.

Las 64 operaciones que se realizan en total quedan agrupadas en cuatro rondas.

Primera Ronda:

$$FF(a, b, c, d, m_0, 7, D76AA478)$$

$$FF(d, a, b, c, m_1, 12, E8C7B756)$$

FF(c, d, a, b,m2, 17, 242070DB)
FF(b, c, d, a,m3, 22,C1BDCEEE)
FF(a, b, c, d,m4, 7, F57C0FAF)
FF(d, a, b, c,m5, 12, 4787C62A)
FF(c, d, a, b,m6, 17,A8304613)
FF(b, c, d, a,m7, 22, FD469501)
FF(a, b, c, d,m8, 7, 698098D8)
FF(d, a, b, c,m9, 12, 8B44F7AF)
FF(c, d, a, b,m10, 17, FFFF5BB1)
FF(b, c, d, a,m11, 22, 895CD7BE)
FF(a, b, c, d,m12, 7, 6B901122)
FF(d, a, b, c,m13, 12, FD987193)
FF(c, d, a, b,m14, 17,A679438E)
FF(b, c, d, a,m15, 22, 49B40821)

Segunda Ronda:

GG(a, b, c, d,m1, 5, F61E2562)
GG(d, a, b, c,m6, 9,C040B340)
GG(c, d, a, b,m11, 14, 265E5A51)
GG(b, c, d, a,m0, 20,E9B6C7AA)
GG(a, b, c, d,m5, 5,D62F105D)
GG(d, a, b, c,m10, 9, 02441453)
GG(c, d, a, b,m15, 14,D8A1E681)
GG(b, c, d, a,m4, 20,E7D3FBC8)
GG(a, b, c, d,m9, 5, 21E1CDE6)
GG(d, a, b, c,m14, 9,C33707D6)
GG(c, d, a, b,m3, 14, F4D50D87)
GG(b, c, d, a,m8, 20, 455A14ED)
GG(a, b, c, d,m13, 5,A9E3E905)
GG(d, a, b, c,m2, 9, FCEFA3F8)
GG(c, d, a, b,m7, 14, 676F02D9)

GG(b, c, d, a,m12, 20, 8D2A4C8A)

Tercera Ronda:

HH(a, b, c, d,m5, 4, FFFA3942)

HH(d, a, b, c,m8, 11, 8771F681)

HH(c, d, a, b,m11, 16, 6D9D6122)

HH(b, c, d, a,m14, 23, FDE5380C)

HH(a, b, c, d,m1, 4,A4BEEA44)

HH(d, a, b, c,m4, 11, 4BDECFA9)

HH(c, d, a, b,m7, 16, F6BB4B60)

HH(b, c, d, a,m10, 23,BEBFBC70)

HH(a, b, c, d,m13, 4, 289B7EC6)

HH(d, a, b, c,m0, 11,EAA127FA)

HH(c, d, a, b,m3, 16,D4EF3085)

HH(b, c, d, a,m6, 23, 04881D05)

HH(a, b, c, d,m9, 4,D9D4D039)

HH(d, a, b, c,m12, 11,E6DB99E5)

HH(c, d, a, b,m15, 16, 1FA27CF8)

HH(b, c, d, a,m2, 23,C4AC5665)

Cuarta Ronda:

II(a, b, c, d,m0, 6, F4292244)

II(d, a, b, c,m7, 10, 432AFF97)

II(c, d, a, b,m14, 15,AB9423A7)

II(b, c, d, a,m5, 21, FC93A039)

II(a, b, c, d,m12, 6, 655B59C3)

II(d, a, b, c,m3, 10, 8F0CCC92)

II(c, d, a, b,m10, 15, FFEFF47D)

II(b, c, d, a,m1, 21, 85845DD1)

II(a, b, c, d,m8, 6, 6FA87E4F)

II(d, a, b, c,m15, 10, FE2CE6E0)

II(c, d, a, b,m6, 15,A3014314)

II(b, c, d, a,m13, 21, 4E0811A1)

II(a, b, c, d,m4, 6, F7537E82)

II(d, a, b, c,m11, 10,BD3AF235)

II(c, d, a, b,m2, 15, 2AD7D2BB)

II(b, c, d, a,m9, 21,EB86D391)

Finalmente, los valores resultantes de a,b,c y d son sumados con A,B,C y D, se procesa el siguiente bloque de datos. El resultado final del algoritmo es la concatenación de A,B,C y D.

A modo de curiosidad, diremos que las constantes ti empleadas en cada paso son la parte entera del resultado de la operación $2^{32} \cdot \text{abs}(\sin(i))$, estando i representado en radianes.

En los últimos tiempos el algoritmo MD5 ha mostrado ciertas debilidades, aunque sin implicaciones prácticas reales, por lo que se sigue considerando en la actualidad un algoritmo seguro, si bien su uso tiende a disminuir.

DSS (Digital Signature Standard)

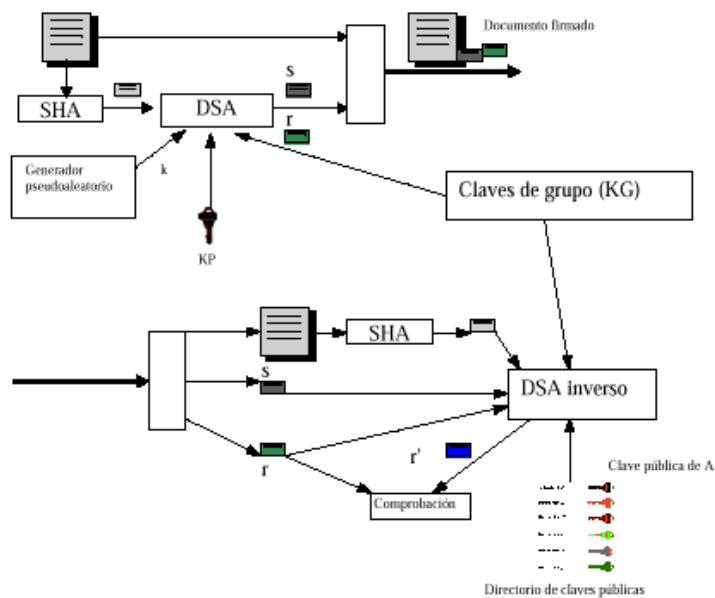
El DSS (Digital Signature Standard) es un sistema de firma digital adoptado como estándar por la organización de estándares de los EE.UU. (NIST). Utiliza la función Hash SHA y el algoritmo asimétrico DSA (Digital Signature Algorithm).

El DSA es un algoritmo asimétrico que únicamente se puede utilizar con firma digital. Utiliza más parámetros que el RSA y así se consigue un grado de mayor seguridad. Los parámetros son los siguientes:

- KG claves públicas de grupo. Son comunes y públicas para un grupo de usuarios.
- KU clave pública. Se genera una por usuario a partir de las KG y es pública.

- KP clave privada. Es privada de cada usuario, se genera a partir de las anteriores.
- k número aleatorio. Se genera uno para cada firma.
- s y r. Son dos palabras de 160 bits que forman la firma de un texto.

El número k permite que el mismo texto del mismo usuario no genere siempre la misma firma. El siguiente esquema resume el funcionamiento de este algoritmo:



Certificados X.509

Un certificado es esencialmente una clave pública y un identificador, firmados digitalmente por una autoridad de certificación, y su utilidad es demostrar que una clave pública pertenece a un usuario concreto. El formato de certificados

X.509 (Recomendación X.509 de CCITT: "The Directory - Authentication Framework". 1988) es el más común y extendido en la actualidad.

El estándar X.509 sólo define la sintaxis de los certificados, por lo que no está atado a ningún algoritmo en particular, y contempla los siguientes campos:

Versión.

Número de serie.

Identificador del algoritmo empleado para la firma digital.

Nombre del certificador.

Periodo de validez.

Nombre del sujeto.

Clave pública del sujeto.

Identificador único de certificador.

Identificador único de sujeto.

Extensiones.

Firma digital de todo lo anterior generada por el certificador.

3.6 FUNDAMENTOS TEÓRICOS DEL ALGORITMO DE SHOR

3.6.1 ALGORITMO CUÁNTICO DE FACTORIZACIÓN DE SHOR

Los sistemas criptográficos más utilizados actualmente (como el RSA) se encuentran basados en la siguiente conjetura:

La factorización de números enteros es computacionalmente mucho más difícil que la multiplicación de enteros. En otras palabras, cuando hay obviamente muchos algoritmos de tiempo polinomial para la multiplicación de enteros, no hay algoritmos de tiempo polinomial para la factorización de enteros. Computacionalmente la factorización de enteros requiere tiempo super-polinomial.

Esta conjetura es basada en el hecho que, a pesar de los intensos esfuerzos de las mejores mentes por muchos años para encontrar un algoritmo de factorización de tiempo polinomial, aun no ha sido encontrado hasta ahora. Asintóticamente el algoritmo clásico más eficiente es la teoría del filtrado de números, el cual factoriza un entero N en tiempo $O(\exp[(\lg N)^{1/3} (\lg \lg N)^{2/3}])$. De esta manera, este es un algoritmo de tiempo super-polinomial en los $O(\lg N)$ numero de dígitos en N .

Oculto sobre esta conjetura se encuentra fluctuantemente, pero implícitamente sobresaliente, asumiendo que todos estos algoritmos corren en computadoras basadas en los principios de la mecánica clásica, es decir en computadoras clásicas. ¿Pero qué pasaría si una computadora puede ser construida de tal forma que no solo esté basada en mecanismos clásicos sino en mecanismos cuánticos?

Peter Shor creó un algoritmo para ser ejecutado en una computadora cuántica, un algoritmo cuántico, que factoriza enteros en tiempo polinomial. Asintóticamente el algoritmo de Shor toma $O((\lg N)^2 (\lg \lg N) (\lg \lg \lg N))$ pasos en una computadora cuántica, lo cual es tiempo polinomial en los $O(\lg N)$ números de dígitos de N .

Problema de factorización de primos. Determinado un entero positivo impar compuesto N , encontrar sus factores primos.

Es conocido que la factorización de N puede ser reducido a la tarea de seleccionar aleatoriamente un entero m relativamente primo de N , y luego determinar su módulo con N multiplicador orden P , es decir, encontrar el entero positivo menor P tal que

$$m^P = 1 \bmod N$$

Fue precisamente este método para factorar el que le permitió a Shor construir su algoritmo de factorización.

¿Pero qué es el algoritmo cuántico de factorización de Shor?

El algoritmo de Shor provee una solución para el problema de factorización de números primos. Este algoritmo consiste en cinco pasos, dentro de los cuales únicamente el paso 2 requiere del uso de una computadora cuántica.

CAPÍTULO IV

DESARROLLO DE LA INVESTIGACIÓN

CAPÍTULO IV. DESARROLLO DE LA INVESTIGACIÓN

4.1 FORMULACION DE HIPÓTESIS

Para el desarrollo de esta investigación se formula una hipótesis de trabajo, ya que se propone para llevar a cabo la investigación.

HIPÓTESIS DE TRABAJO: El análisis de los avances del desarrollo de la computación cuántica permite conocer las posibles consecuencias que traerá a los mecanismos de seguridad que utilizan criptografía asimétrica en las empresas de El Salvador.

VARIABLE DEPENDIENTE: Los sistemas de seguridad que utilizan criptografía asimétrica.

VARIABLE INDEPENDIENTE: El análisis de los avances del desarrollo de la computación cuántica.

RELACION ENTRE VARIABLES:

Conocer las consecuencias que traería el desarrollo de la computación cuántica analizando los diferentes mecanismos de seguridad que utilizan criptografía asimétrica.

4.2 FUNCIONAMIENTO DE SISTEMA CRIPTOGRAFICO ASIMÉTRICO

Resumen

Para ver el funcionamiento de un sistema criptográfico asimétrico, tenemos que ver donde es implementado; como ya se había explicado antes el algoritmo RSA es usado por el SSL en la generación de los Certificados Digitales y la Firma Electrónica. Por tal motivo se presenta la configuración del Servidor Apache HTTP con Red Hat Linux, mostrando los tipos de Certificado que pueden ser utilizados por el servidor, la generación de las llaves y por ende la generación de un Certificado Autofirmado y la generación de la solicitud de un Certificado Digital firmado por una Autoridad Certificadora.

Además presentamos la configuración del servidor Apache para win32, mostrando todos los requerimientos necesarios para que funcione en un ambiente Windows y por lo tanto mostrar lo necesario para que sea un servidor seguro y poder generar las llaves para un certificado autofirmado o para la generación de la solicitud de un certificado digital.

También se presentan las diferentes entidades certificadoras más conocidas y comerciales, y la única entidad certificadora de El Salvador; se muestra el proceso para la obtención del certificado digital, la verificación de éstos y también los precios que incurren para adquirir dichos certificados

4.2.1 CONFIGURACIÓN DEL SERVIDOR SEGURO APACHE HTTP CON RED HAT LINUX

4.2.1.1 Introducción

En este apartado se proporciona información básica sobre el Servidor Apache HTTP con el módulo de seguridad mod_ssl activado para usar la librería y el conjunto de herramientas OpenSSL. La combinación de estos tres

componentes, proporcionados con Red Hat Linux, se conocen como el servidor seguro Web o simplemente como el servidor seguro.

El software *OpenSSL* es un proyecto de software desarrollado por los miembros de la comunidad Open Source. Es un robusto juego de herramientas que le ayudan a su sistema a implementar el *Secure Sockets Layer* (SSL), así como otros protocolos relacionados con la seguridad, tales como el *Transport Layer Security* (TLS). También incluye una librería de criptografía. Este paquete de software es importante para cualquiera que esté planeando usar cierto nivel de seguridad en su máquina.

El módulo `mod_ssl` es un módulo de seguridad para el Servidor Apache HTTP. El módulo `mod_ssl` usa las herramientas proporcionadas por el Proyecto OpenSSL para añadir una característica muy importante al Servidor Apache HTTP — la habilidad de tener comunicaciones encriptadas. En contraste, usando HTTP normal, las comunicaciones entre el navegador y el servidor Web son enviadas en texto plano, lo cual puede ser interceptado y leído por alguna persona no autorizada.

Este apartado le mostrará como instalar estos programas. También los pasos necesarios para generar una clave privada y una petición de certificado, cómo generar su propio certificado firmado, y cómo instalar un certificado para usarlo con su servidor web seguro.

El archivo de configuración `mod_ssl` está ubicado en `/etc/httpd/conf.d/ssl.conf`. Para que este archivo sea cargado, y por ende para que `mod_ssl` funcione, debe tener la sentencia `Include conf.d/*.conf` en `/etc/httpd/conf/httpd.conf`.

4.2.1.2 Certificados y seguridad

Su servidor proporciona seguridad usando una combinación del protocolo SSL Secure Sockets Layer y (en la mayoría de los casos) un certificado digital de una Autoridad de Certificación (CA). SSL maneja las comunicaciones encriptadas y la mutua autenticación entre navegadores y su servidor seguro. El certificado digital aprobado por una CA proporciona autenticación para su servidor seguro (el CA pone su reputación detrás de la certificación de la identidad de su organización). Cuando su navegador se esté comunicando usando la encriptación SSL, verá el prefijo `https://` al principio de la URL (Localizador de Recursos Uniforme - la dirección de Internet) en la barra de navegación.

La encriptación depende del uso de claves (imagínelas como anillos codificador/decodificador en formato de datos). En criptografía convencional o simétrica, ambas partes de la transacción tienen la misma clave, la cual usan para decodificar la transmisión del otro. En criptografía pública o asimétrica, coexisten dos claves: una pública y una privada. Una persona o una organización guarda su clave privada en secreto, y publica su clave pública. Los datos codificados con la llave pública sólo pueden ser decodificados con la clave privada; y los datos codificados con la clave privada sólo pueden ser decodificados con la llave pública.

Para configurar su servidor seguro, usará criptografía pública para crear un par de claves pública y privada. En muchos casos, enviará su petición de certificado (incluyendo su clave pública), demostrando la identidad de su compañía y pago a la CA. La CA verificará la petición del certificado y su identidad, y entonces mandará un certificado para su servidor seguro.

Un servidor seguro usa un certificado para identificarse a sí mismo a los navegadores web. Puede generar su propio certificado (llamado certificado

autofirmado) o puede conseguirlo de una CA. Un certificado de una CA con buena reputación garantiza que un sitio web está asociado a una compañía u organización particular.

Comentario [CL1]: Ya se había definido antes que una CA es una entidad certificadora.

Alternativamente, puede crear su propio certificado autofirmado. Note, sin embargo, que estos certificados autofirmados no deben ser usados en muchos entornos de producción. Dichos certificados pueden no ser aceptados automáticamente por el navegador de un usuario — el usuario será preguntado por el navegador si quiere aceptar el certificado y crear la conexión segura.

Una vez que tenga un certificado autofirmado o firmado por la CA de su elección, necesitará instalarlo en su servidor seguro.

4.2.1.3 Tipos de certificados

Si ha instalado su servidor seguro desde el paquete RPM proporcionado en Red Hat Linux, una clave aleatoria y un certificado de prueba son generados y puestos en sus directorios apropiados. Antes de que empiece a usar su servidor seguro, sin embargo, necesitará generar su propia clave y obtener un certificado que identifique correctamente su servidor.

Necesita una clave y un certificado para operar su servidor seguro — lo cual significa que puede generar un certificado autofirmado o adquirir uno firmado por una CA. ¿Cuáles son las diferencias entre los dos?

Un certificado firmado por una CA proporciona dos importantes capacidades para su servidor:

- Los navegadores (normalmente) reconocen automáticamente el certificado y permiten establecer la conexión segura sin preguntar al usuario.

- Cuando una CA emite un certificado firmado, ellos garantizan la identidad de la organización que está proporcionando las páginas web al navegador.

Si su servidor seguro está siendo accedido por todo el mundo, necesitará un certificado firmado por una CA, así la gente que acceda a su sitio web sabrá que dicho sitio es propiedad de la organización que proclama ser la dueña. Antes de firmar un certificado, una CA verifica que la organización peticionaria de dicho certificado es realmente quien proclama ser.

Muchos navegadores web que soportan SSL tienen una lista de CA's cuyos certificados admiten automáticamente. Si el navegador encuentra un certificado autorizado por una CA que no está en la lista, el navegador preguntará al usuario si desea aceptar o rechazar la conexión.

Puede generar un certificado autofirmado para su servidor seguro, pero tenga claro que dicho certificado no proporciona la misma funcionalidad que uno firmado por una CA. Un certificado autofirmado no será reconocido automáticamente por los navegadores de los usuarios, además de no proporcionar ninguna garantía concerniente a la identidad de la organización que provee el sitio web. Un certificado firmado por una CA proporciona ambas importantes características a un servidor seguro. Si su servidor seguro será usado en un ambiente de producción, probablemente necesite un certificado firmado por una CA.

El proceso para conseguir un certificado de una CA es bastante sencillo. A continuación un vistazo rápido a dicho proceso:

1. Crear un par de claves encriptadas, pública y privada.

2. Crear una petición de certificado basada en la clave pública. La petición contiene información sobre su servidor y la compañía que lo hospeda.
3. Mande la petición de certificado, junto con los documentos que prueben su identidad, a una CA. No le diremos qué Autoridad de Certificación elegir. Su elección puede basarse en experiencias previas, experiencias de sus amigos o conocidos o simplemente en factores monetarios.

Una vez que haya decidido sobre el CA, necesitará seguir las instrucciones que se le indiquen para obtener un certificado.

4. Cuando la CA esté satisfecha de que usted es en realidad quién dice ser, le enviarán su certificado digital.
5. Instale este certificado en su servidor seguro y comience a manejar transacciones seguras.

Si está consiguiendo un certificado de una CA o generando su propio certificado autofirmado, el primer paso es generar una clave.

4.2.1.4 Generación de clave privada.

Tiene que ser root para generar una clave.

Primero, cámbiese al directorio /etc/httpd/conf. Elimine la clave y el certificado simulados que se generaron durante la instalación con los siguientes comandos:

```
rm ssl.key/server.key
rm ssl.crt/server.crt
```

A continuación, necesita crear su propia clave aleatoria. Cambie al directorio /usr/share/ssl/certs y escriba el comando siguiente:

```
make genkey
```

Su sistema mostrará un mensaje similar al siguiente:

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
```

Necesita teclear una palabra de paso. Para mayor seguridad, su palabra de paso debe incluir, al menos, ocho caracteres, incluyendo números y símbolos de puntuación, y no ser una palabra que esté incluida en un diccionario. También, recuerde que su palabra de paso es sensible a las mayúsculas.

Nota: *Necesitará acordarse de su palabra de paso para poder introducirla cada vez que inicie su servidor Web seguro; así que no la olvide.*

Le será requerido que reintroduzca su contraseña, para verificar que es correcta. Una vez que la haya tecleado correctamente, será creado un archivo llamado /etc/httpd/conf/ssl.key/server.key, que contendrá dicha clave.

Observe que si no quiere teclear la palabra de paso cada vez que comience su servidor seguro, necesitará usar los dos comandos siguientes en vez de `make genkey` para crear su clave.

Utilice el siguiente comando para crear su clave:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

Luego, utilice el comando siguiente para asegurarse que los permisos de su clave están correctamente asignados:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

Después de usar los comandos anteriores para crear su clave, no necesitará utilizar una contraseña para comenzar su servidor Web seguro.

Atención *El desactivar la contraseña para su servidor web seguro es un riesgo de seguridad. NO es recomendable que lo haga.*

Los problemas asociados con no usar la contraseña están directamente relacionados al mantenimiento de la seguridad en el sistema de la máquina. Si por ejemplo, un individuo sin escrúpulos compromete la seguridad UNIX estándar de la máquina, ésta persona podrá obtener su clave privada (el contenido de su archivo `server.key`). La clave podría ser usada para servir páginas web que aparenten estar en su servidor web.

Si las labores de seguridad de UNIX son rigurosamente mantenidas en el sistema (todos los parches y actualizaciones del sistema operativo son instalados tan pronto como están disponibles, no se ejecutan servicios innecesarios o peligrosos, etc.), la contraseña del servidor seguro puede parecer innecesaria. Sin embargo, desde que su servidor Web seguro no necesita ser reiniciado muy a menudo, la seguridad extra proporcionada por la introducción de la contraseña es un pequeño esfuerzo que vale la pena en muchos casos.

El archivo `server.key` debe ser propiedad del usuario `root` de su sistema y no debe ser accesible por nadie más. Haga una copia de seguridad de dicho archivo y guárdela en un lugar seguro. Necesitará la copia de seguridad por que si pierde el archivo `server.key` después de haberlo usado para crear su certificado, el susodicho certificado no funcionará más y la CA no podrá ayudarlo. Su única solución será pedir (y volver a pagar por ello) un nuevo certificado.

4.2.1.5 Generar una petición de certificado para enviarla a un CA.

Una vez creada la clave, el siguiente paso es generar la petición de certificado que necesitaremos enviar al CA de nuestra elección. Asegúrese de estar en el directorio `/usr/share/ssl/certs` y teclee el siguiente comando:

```
make certreq
```

Su sistema mostrará la siguiente salida y le preguntará por su contraseña (a menos que desactivara dicha opción):

```
umask 77 ; \  
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key  
-out /etc/httpd/conf/ssl.csr/server.csr  
Using configuration from /usr/share/ssl/openssl.cnf  
Enter PEM pass phrase:
```

Teclee la palabra de paso que eligió cuando generó su clave. Su sistema mostrará algunas instrucciones y le requerirá una serie de respuestas. Dichas respuestas serán incorporadas a la petición del certificado. La pantalla, con respuestas de ejemplo, será similar a esta:

```
You are about to be asked to enter information that will be incorporated  
into your certificate request.
```

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:**SV**

State or Province Name (full name) [Berkshire]:**San Salvador**

Locality Name (eg, city) [Newbury]:**San Salvador**

Organization Name (eg, company) [My Company Ltd]:**Empresa Prueba**

Organizational Unit Name (eg, section) []:**Pruebas**

Common Name (your name or server's hostname) []:**prueba.ejemplo.com**

Email Address []:**admon@ejemplo.com**

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

Las respuestas por defecto aparecerán entre corchetes [] inmediatamente después de cada petición de entrada. Por ejemplo, la primera información requerida es el nombre del país dónde el certificado será usado, parecido a:

Country Name (2 letter code) [GB]:

La entrada por defecto, entre corchetes, es GB. Para aceptarla, pulse [Intro], o rellene con el código de dos letras de su país.

Tendrá que introducir el resto de las entradas. Todas estas entradas son autoexplicativas, pero necesitará seguir estas directrices:

- No abrevie la localidad o el estado. Escríbalas enteras (por ejemplo, Sta. Ana debe escribirse como Santa Ana).
- Si está mandando esta información de un CSR a un CA, sea cuidadoso en proporcionar la información correcta en todos los campos, pero

Comentario [CL2]: No sería mejor hacer aquí un ejemplo con una empresa salvadoreña?

especialmente en el Nombre de la Organización y el Nombre común. Las CA's verifican los datos para determinar si su organización es responsable de quién proporcionó como Nombre común. Las CA's rechazarán las peticiones que incluyan información que ellos perciban como inválida.

- Para Nombre común, asegúrese que teclea el *verdadero* nombre de su servidor Web seguro (un nombre de DNS válido) y no un alias que el servidor tenga.
- La Dirección email debe ser la del webmaster o administrador del sistema.
- Evite caracteres especiales como @, #, &, !, etc. Algunas CA's rechazarán una petición de certificado que contenga un carácter especial. Así, si el nombre de su compañía contiene una "y" comercial (&), escríbalo como "y" en vez de "&".
- No use los atributos extra (Otra Contraseña y Nombre opcional de la compañía). Para continuar sin introducir estos campos, simplemente pulse [Intro] para aceptar los valores en blanco por defecto.

El archivo `/etc/httpd/conf/ssl.csr/server.csr` es creado cuando termine de introducir su información. Este archivo es su petición de certificado, listo para enviar a su CA.

Después de haber decidido una CA, siga las instrucciones que ellos proporcionen en su sitio web. Estas instrucciones le dirán como mandar su petición de certificado, cualquier otra documentación que ellos requieran, y como pagarles.

Después de haber satisfecho los requisitos de la CA, ellos le mandarán un certificado para usted (normalmente por email). Guarde (o copie y pegue) el certificado que le manden como `/etc/httpd/conf/ssl.crt/server.crt`. Asegúrese de hacer una copia de respaldo.

4.2.1.6 Creación de un certificado autofirmado.

Usted puede crear su propio certificado autofirmado. Por favor, tenga en cuenta que un certificado autofirmado no proporciona las garantías de seguridad que un certificado firmado por una CA sí proporciona.

Si quiere crear su propio certificado autofirmado, necesitará primero crear una clave aleatoria usando las instrucciones proporcionadas anteriormente. Una vez que tenga la clave y que se asegure de estar en el directorio /usr/share/ssl/certs, utilice el siguiente comando:

```
make testcert
```

Verá la siguiente salida, se le pedirá que introduzca su palabra de paso (a menos que haya generado una clave sin contraseña):

```
umask 77 ; \  
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key  
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt  
Using configuration from /usr/share/ssl/openssl.cnf  
Enter PEM pass phrase:
```

Después de que introduzca su contraseña (o sin la petición, si ha creado una clave sin ella), se le pedirá más información. La salida del ordenador y el conjunto de peticiones será parecido al siguiente (necesitará dar la información correcta de su organización y de su máquina):

```
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a  
DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [GB]:SV
```

Comentario [CL3]: Igual que el anterior

State or Province Name (full name) [Berkshire]:**San Salvador**
Locality Name (eg, city) [Newbury]:**San Salvador**
Organization Name (eg, company) [My Company Ltd]: **Empresa Prueba**
Organizational Unit Name (eg, section) []: **Pruebas**
Common Name (your name or server's hostname) []:**prueba.ejemplo.com**
Email Address []:**admon@ejemplo.com**

Después que proporcione la información correcta, un certificado autofirmado será creado y colocado en `/etc/httpd/conf/ssl.crt/server.crt`. Necesitará reiniciar su servidor seguro, después de generar el certificado, con el comando:

```
/sbin/service httpd restart
```

4.2.1.7 Probar su certificado

Para probar el certificado instalado por defecto, un certificado de una CA o un certificado autofirmado, apunte su navegador Web a la siguiente página web (reemplazando *prueba.ejemplo.com* con el nombre de su dominio):

<https://prueba.ejemplo.com>

Nota: Observe la *s* después de *http*. el prefijo *https*: es usado para las transacciones *HTTP seguras*.

Si ha comprado un certificado de una CA bien conocida, su navegador probablemente aceptará el certificado automáticamente (sin pedirle información adicional) y creará una conexión segura. Su navegador no reconocerá automáticamente un certificado de prueba o un certificado autofirmado, porque el certificado no es firmado por una CA. Si no está usando un certificado de una CA, siga las instrucciones proporcionadas por su navegador para aceptar el certificado.

Una vez que su navegador acepte el certificado, su servidor seguro mostrará una página de inicio predeterminada.

4.2.2 CONFIGURACIÓN DEL SSL EN EL APACHE WEB SERVER PARA WIN32

4.2.2.1 Información general

Antes que nada, se tiene que tener instalado el servidor web de Apache, se puede ser la versión 1.3.19. También se tiene que obtener el mod_ssl y el OpenSSL (ambos vienen en conjunto), bajarlos de aquí:

<http://www.modssl.org/contrib/> la versión de mod_ssl puede ser la 2.8.2 y la del OpenSSL la 0.9.6a.

Ahora bien, en este apartado se describe la instalación de la versión para Win32 de Apache con la extensión mod_ssl. El proceso funcionó para Windows98 y NT.

Apache con mod_ssl parece ser la única solución gratis para Win32. Se debe saber que el Apache en Win32 es considerado calidad beta, por lo tanto, no alcanza la estabilidad y rendimiento de Apache sobre plataformas UNIX/Linux.

4.2.2.2 Instalando Apache

El archivo que contiene la instalación del Apache 1.3.19 se llama **apache_1.3.19-win32-no_src-r2.msi** (si no se tiene el Instalador de archivos MSI, bajarlo de aquí:

<http://www.microsoft.com/msdownload/platformsdk/instdmsi.htm>, lo hay para las versiones Win9x y NT). Este archivo contiene la base del sistema Apache y ejemplos de archivos de configuración.

Instalar Apache como se indica en <http://www.apache.org/docs/windows.html>

Cambiar los siguientes parámetros del archivo

[APACHE_HOME]\conf\httpd.conf:

[Reemplazar todas las ocurrencias de www.mi-servidor.com con su nombre de dominio real!!!]

(Si lo está instalando en una intranet entonces solo utilice el nombre que tiene su computadora en lugar de www.mi-servidor.com d;)

- Port 443
- Listen 80
- Listen 443
- ServerName www.mi-servidor.com
- DocumentRoot [WWW_HOME] y el correspondiente <Directory [WWW_HOME]> con el directorio en donde deseas hospedar tu homepage(p.e. "c:/www")

Instalar el servicio Apache (solo en NT) e iniciar el servidor. Verificar que todo trabaje bien antes de proceder a la instalación del SSL.

Probar <http://mi-servidor.com:443/>. No será encriptada todavía pero si funciona significa que la configuración del puerto 443 funciona bien.

4.2.2.3 Obteniendo el OpenSSL y mod_ssl

El archivo que contiene la instalación del OpenSSL y mod_ssl se llama **Apache_1.3.19_modssl_2.8.2_Win32_Diff.zip** descomprimirlo en un nuevo directorio.

Copiar los archivos `ssleay32.dll` and `libeay32.dll` del directorio `Apache\openssl\bin` al directorio `Windows\System` en caso de Win9x o `WINNT\System32` en caso de WinNT.

4.2.2.4 Creación del certificado de prueba

Las siguientes instrucciones vienen de <http://www.apache-ssl.org/#FAQ>

```
openssl req -config openssl.cnf -new -out mi-servidor.csr
```

Esto crea un certificado de requisición de firma y una llave privada. Cuando pregunte por "Common name (p.e. su nombre de dominio)" dar exactamente su nombre de dominio (p.e. www.mi-servidor.com). El certificado pertenece al nombre del servidor y los navegadores emiten un aviso de inconformidad si el nombre no coincide.

```
openssl rsa -in privkey.pem -out mi-servidor.key
```

Esto remueve la contraseña de la llave privada. DEBE entender lo que significa esto; mi-servidor.key debe ser solamente legible por el servidor Apache y el administrador. Debe borrar el archivo .rnd porque contiene información entrópica para la creación de la llave y podría usarse para ataques criptográficos contra tu clave privada.

```
openssl x509 -in mi-servidor.csr -out mi-servidor.cert -req -signkey mi-servidor.key -days 365
```

Esto crea un certificado con firma propia (llamémoslo un certificado casero) que puede usar en tanto obtiene uno de validez oficial proveniente de una autoridad certificada. (El cual es opcional, si conoce a sus usuarios, decirles que instalen su certificado en sus navegadores.) Vea que el certificado expira después de un año, puede incrementar -days 365 si lo desea.

Si tiene usuarios con Microsoft Internet Explorer 4.x y quieres que tengan la posibilidad de almacenar su certificado (Al transferirlo y abrirlo), necesita crear una versión DER-cifrada del certificado.

```
openssl x509 -in mi-servidor.cert -out mi-servidor.der.crt -outform DER
```

Crear el directorio [APACHE_HOME]\conf\ssl y mover los archivos mi-servidor.key y mi-servidor.cert en el.

4.2.2.5 Configurando Apache y mod_ssl

Copiar los archivos que bajo de la distribución del Apache-mod_ssl en su directorio de instalación original de Apache (¡Recordar detener primero el Apache!).

Localizar las directivas LoadModule en su archivo http.conf y añadir lo siguiente al final de los existentes:

```
LoadModule ssl_module modules/mod_ssl.so  
ó LoadModule ssl_module modules/ApacheModuleSSL.so  
ó LoadModule ssl_module modules/mod_ssl.so  
en nuevas versiones.
```

Añade lo siguiente al final del archivo http.conf:

Para tener una mejor información ver:

http://www.modssl.org/docs/2.8/ssl_reference.html

```
SSLMutex sem  
SSLRandomSeed startup builtin  
SSLSessionCache none  
SSLLog logs/SSL.log  
SSLLogLevel info
```

Posteriormente puede cambiar "info" a "warn" si todo sale bien

```
SSLEngine On  
SSLCertificateFile conf/ssl/mi-servidor.cert
```

SSLCertificateKeyFile conf/ssl/mi-servidor.key

No olvidar cargar Apache si la directiva `Ifdefine` está activa en el archivo de configuración.

Quizá se necesite usar el `regedit` para cambiar la clave

`HKEY_LOCAL_MACHINE\SOFTWARE\Apache Group\Apache\X.Y.Z` a la versión correcta si el `apache.exe` de `modssl.org/contrib` no es la misma versión a la que previamente instaló.

Iniciar el servidor, en esta ocasión desde la línea de comandos (no como servicio) con el propósito de ver los mensajes de error que impiden iniciar el Apache. Si todo funciona bien, (de manera opcional) presionar `CTRL+C` para detener el servidor e iniciarlo como servicio si así lo prefiere.

Si esto no funciona, Apache escribe mensajes significativos en la pantalla y/o en los archivos `error.log` y `SSL.log` en el directorio `Apache\logs`.

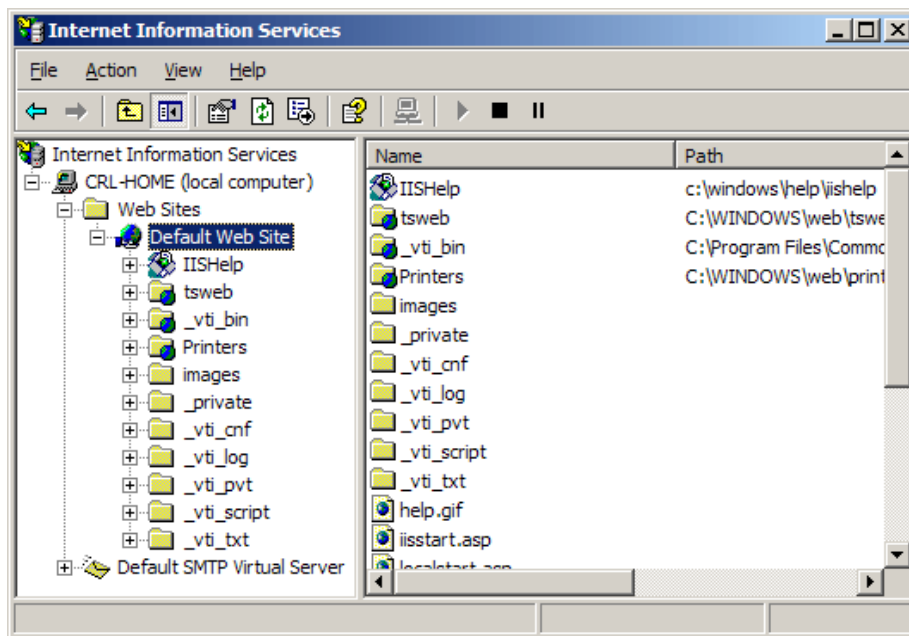
Si algo no trabaja, ajuste todos los `LogLevel`s al máximo y *vea en los archivos log*. Estos son muy útiles.

4.2.3 GENERAR UNA PETICIÓN DE CERTIFICADO (CSR) EN UN SERVIDOR MICROSOFT IIS 5.X / 6.X

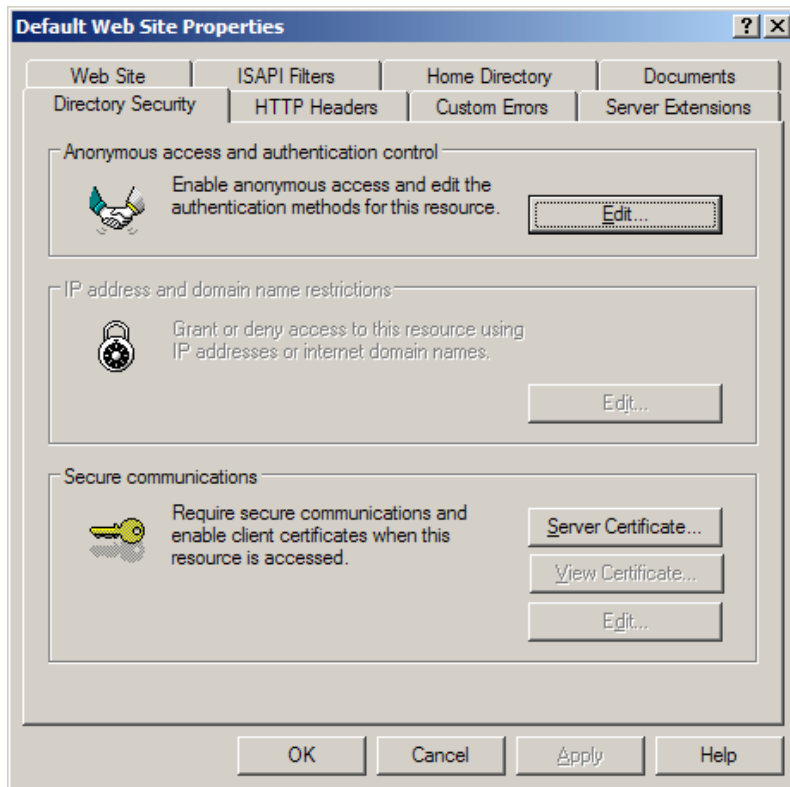
Un CRS es un archivo que incluye la información necesaria para solicitar un certificado de seguridad, incluyendo en él una llave pública. Al terminar este proceso deberá adjuntar el CSR en el formulario de compra de certificados, que proporciona la CA:

Generar las llaves y el CSR:

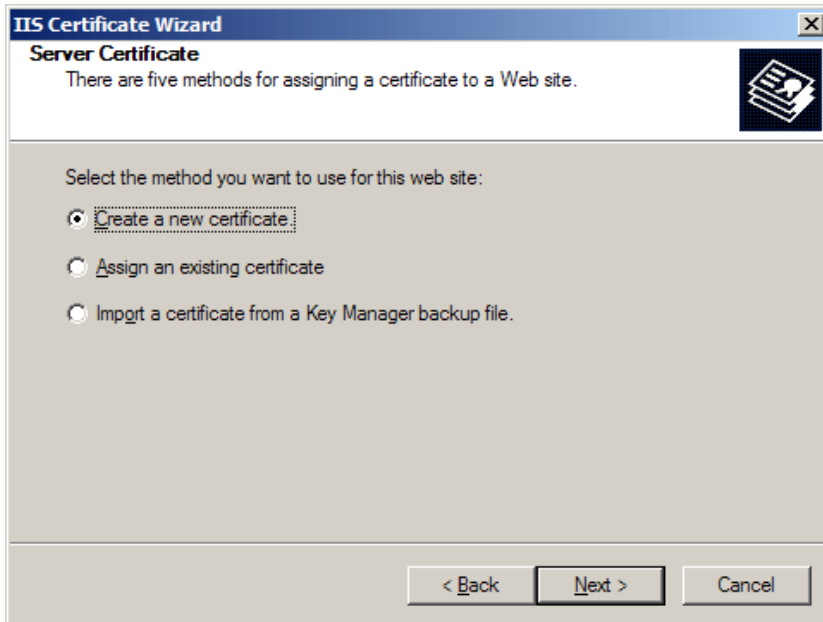
- Seleccione Herramientas de administración (**Administrative Tools**)
- Inicie **Internet Services Manager**



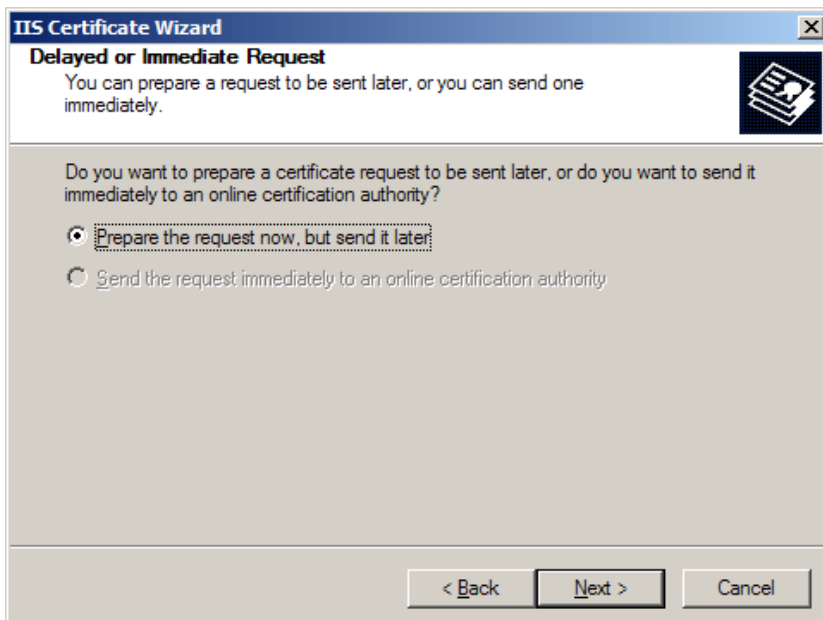
- Abra la ventana de propiedades de la web para la que se va a solicitar el CRS. (click derecho>propiedades)
- Sitúese en la pestaña referente a los directorios seguros (**Directory Security**)



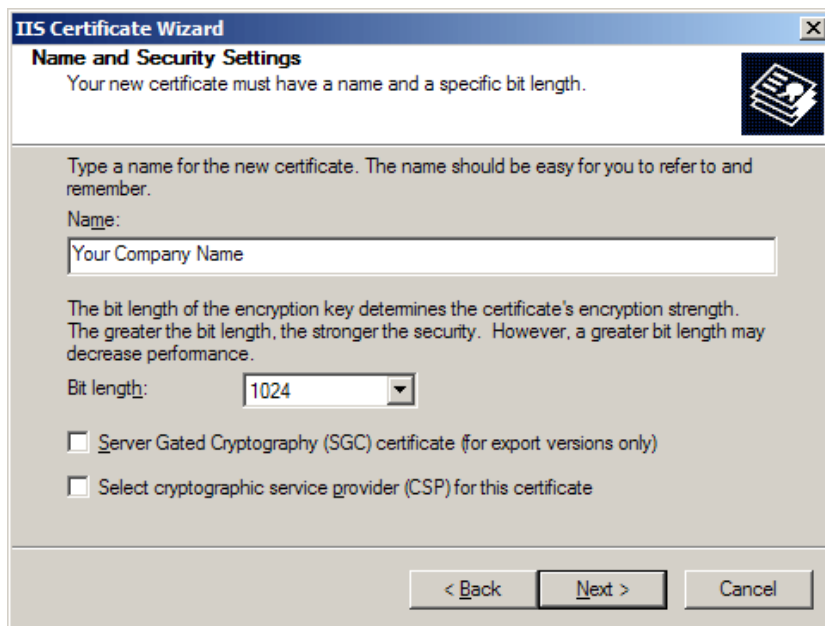
- Click en el botón referente al certificado del servidor (**Server Certificate**), y siga los siguientes pasos:



- Click en crear nuevo certificado (**Create a new certificate**) y en después en siguiente.



- Seleccione preparar la petición y enviar mas tarde (**Prepare the request**) y click en siguiente.



IIS Certificate Wizard

Name and Security Settings

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Name:

The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length:

☐ Server Gated Cryptography (SGC) certificate (for export versions only)

☐ Select cryptographic service provider (CSP) for this certificate

< Back Next > Cancel

- Nombre el certificado para que sea fácilmente identificable (esto no afecta al certificado, es solo para su información personal).
- Seleccione 1024 bit key al tratarse de un certificado SSL de 128bits. Click en Siguiente

The screenshot shows the 'IIS Certificate Wizard' window with the 'Organization Information' tab selected. The window has a title bar with 'IIS Certificate Wizard' and a close button. Below the title bar, the tab name 'Organization Information' is displayed. The main content area contains the following text: 'Your certificate must include information about your organization that distinguishes it from other organizations.' followed by a small icon of a certificate. Below this, instructions state: 'Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.' and 'For further information, consult certification authority's Web site.' There are two dropdown menus: 'Organization:' with 'Your Company Name' selected, and 'Organizational unit:' with 'Web' selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

IIS Certificate Wizard

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization:

Your Company Name

Organizational unit:

Web

< Back Next > Cancel

- Introducir Nombre de organización y departamento de la compañía y click en siguiente.

The screenshot shows the 'IIS Certificate Wizard' window with the 'Your Site's Common Name' tab selected. The window has a title bar with 'IIS Certificate Wizard' and a close button. Below the title bar, the tab name 'Your Site's Common Name' is displayed. The main content area contains the following text: 'Your Web site's common name is its fully qualified domain name.' followed by a small icon of a certificate. Below this, instructions state: 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.' and 'If the common name changes, you will need to obtain a new certificate.' There is a text input field labeled 'Common name:' containing the text 'www.mydomainname.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

IIS Certificate Wizard

Your Site's Common Name

Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

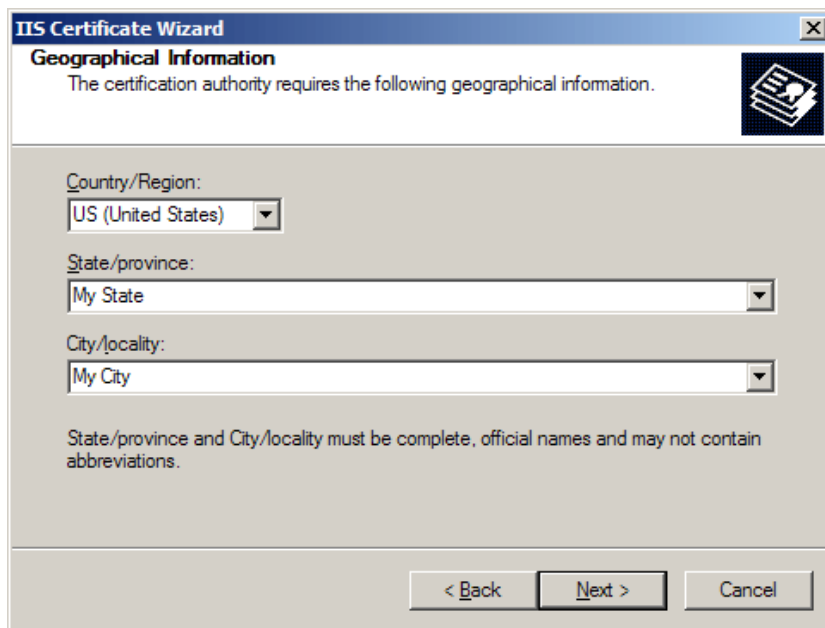
If the common name changes, you will need to obtain a new certificate.

Common name:

www.mydomainname.com

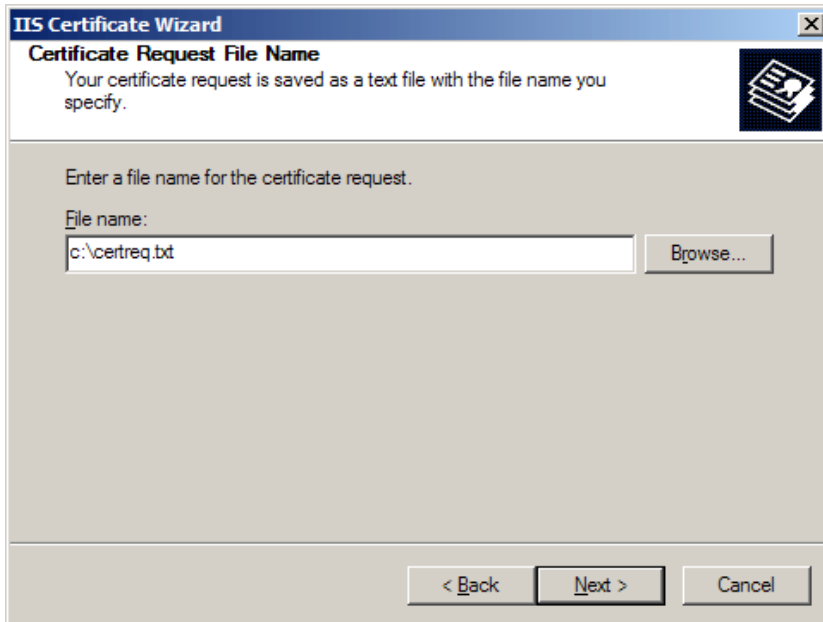
< Back Next > Cancel

- Nombre de dominio para el que se va a solicitar el certificado. Asegúrese de que todo es correcto y que contiene un dominio principal o subdominio (e.g. seguridad.ejemplo.com, www.ejemplo.com, ...). Click en siguiente.

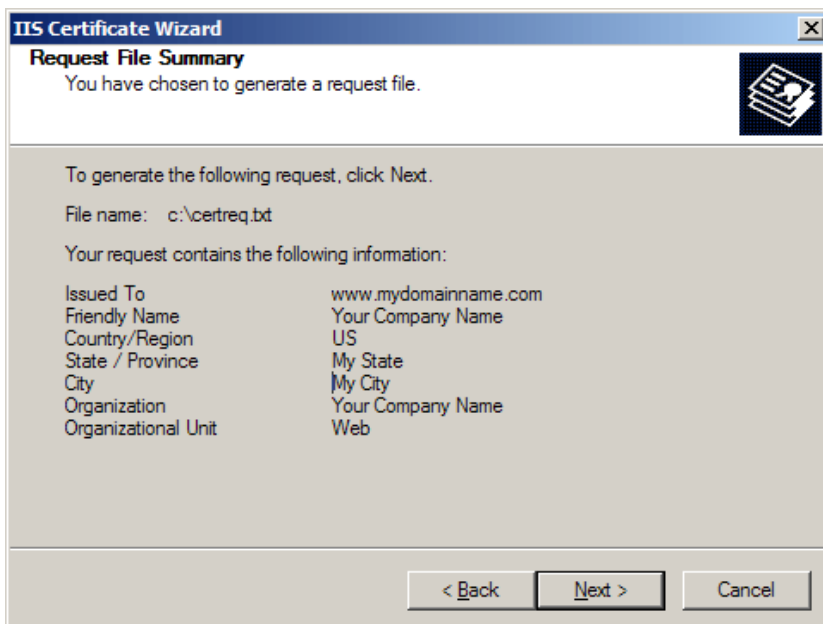


The screenshot shows a Windows-style dialog box titled "IIS Certificate Wizard". The main heading is "Geographical Information" in bold. Below it, a message states: "The certification authority requires the following geographical information." To the right of this text is a small icon of a document with a keyhole. The form contains three dropdown menus: "Country/Region:" with "US (United States)" selected, "State/province:" with "My State" selected, and "City/locality:" with "My City" selected. Below these fields, a note reads: "State/province and City/locality must be complete, official names and may not contain abbreviations." At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

- Introduzca País, provincia y ciudad. Click siguiente.



- Introduzca un nombre y ruta para guardar el CSR.



- Comprueba que los detalles introducidos son totalmente correctos. En el caso de haber cometido algún error tiene la opción de volver hacia atrás para subsanarlo. Si todo es correcto haga click en siguiente.
- Copie todo el contenido del CSR, comprendido desde:

-----BEGIN CERTIFICATE REQUEST-----

hasta

-----END CERTIFICATE REQUEST-----

Necesitará utilizarlo durante el proceso de compra de su certificado.

Grabar su llave privada:

- Click en el botón "Certificados" dentro de la consola de mantenimiento (**Microsoft Management Console**)
- Seleccionar "Peticiones" (**Requests**)
- Seleccione "Todas las tareas" (**All tasks**)
- Seleccione "Exportar" (**Export**)

Le recomendamos anotar su contraseña y realizar una copia de seguridad de su llave privada, ya que al ser una llave única, otorgada al administrador de sistema, en caso de perdida no es posible recuperarla. Esta copia de datos se puede hacer un disco floppy.

4.2.4 ¿ CÓMO OBTENER UN CERTIFICADO DIGITAL ?

La obtención de un certificado puede hacerse de dos formas: petición on-line y petición postal.

Dependiendo del tipo de certificado debe procederse de una u otra forma.

Por ejemplo, en el caso de la petición de certificados personales, la lógica y la operativa apuntan a que la petición sea on-line. Es decir, a la hora de pedir un certificado personal se debe rellenar un cuestionario con nuestros datos personales directamente en la web a una CA y, dependiendo de la clase de certificado, remitir una fotocopia de la documentación a la Autoridad de Certificación o personarnos físicamente en la Autoridad de Registro al efecto.

Comentario [CL4]: lo mismo que el primer comentario

Una vez superados estos trámites la CA firmará el certificado y se lo entregará a su titular.

El caso de la petición postal resulta indicado, por ejemplo, para la petición de Certificados para Servidor. De hecho resulta un sistema mixto, pues como contacto inicial debe enviarse una copia de la CSR por e-mail y después, a través de correo postal, la documentación necesaria (contrato, documentación acreditativa, etc.)

4.2.5 AUTORIDADES DE CERTIFICACIÓN (AC).

Es la tercera parte fiable que acredita la correspondencia entre una determinada clave y su propietario real. Actúa como una especie de notario electrónico que extiende un certificado de claves el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información.

La ley de firma electrónica las define como "prestadores de servicios de certificación" y, según la legislación de cada país, "son aquellas personas físicas o jurídicas que expiden certificados, pudiendo prestar, además otros servicios en relación con la firma electrónica".¹⁴

Son aquellos órganos encargados de otorgar confianza en la infraestructura de clave pública. Desde el punto de vista de una infraestructura de clave pública es necesario confiar en una tercera parte solvente que pueda garantizar u otorgue la confianza necesaria para poder identificar a una persona física o jurídica con una determinada clave pública.

Para aumentar la seguridad de las transacciones en la red, se recurre al servicio de las "Autoridades Certificadoras", que son las que certifican la identidad de las partes emitiendo un "certificado".

"Un certificado es un documento electrónico que se utiliza para identificar a un individuo o a una compañía. Las Autoridades Certificadoras son entidades que validan identidades y proporcionan certificados. Los métodos empleados para la validación de identidades dependen de las políticas de cada CA.

Un certificado es como el pasaporte de una persona. Incluye una clave pública (que sirve para la encriptación), el nombre de la entidad a quien identifica, una fecha de expiración, el nombre de la CA que ha proporcionado el certificado y un número de serie.

Lo más importante de todo, es que el certificado viene firmado digitalmente por la CA, de esta manera es como si la Autoridad Certificadora presentase a la entidad a la que identifica, asegurándonos que confía en la identidad del propietario del certificado."

¹⁴ Esta ley es conocida a nivel mundial, pero en nuestro país no existe una ley propia que regule el uso de Firma Electrónica y Certificado Digital.

Sin embargo, las CA sólo aseguran la corrección -en función de sus normas- de los datos entregados por quien pidió el certificado, pero ninguna está en condiciones de asegurar que la identidad registrada no es falsa: no tienen la posibilidad de chequear físicamente la identidad de los postulantes. Sin embargo la documentación que solicitan antes de otorgar un certificado es bastante exhaustiva y los antecedentes obtenidos son verificados de diferentes maneras (verificación de domicilio, control de antecedentes comerciales, etc.).

Las Autoridades Certificadoras más conocidas son:

1- VERISIGN	2- IPSCA	3- ENTRUST
		
http://www.verisign.com	http://www.ipsc.com	http://www.entrust.com

1- VERISIGN

Proporciona firmas para cualquier servidor SSL (servidor seguro) y efectúa estrictas comprobaciones de identidad (Es la más conocida y comercial).

- Certificados SSL. Servicio de Sitio Seguro

Los certificados SSL son ideales para asegurar sitios, intranets y extranets del Web. Cada una de estas soluciones seguras del sitio entrega el cifrado de gran alcance de SSL y viene con el servicio de la autenticación de la identidad de VeriSign. Elegir el sitio seguro favorable para garantizar que cada sesión del

SSL recibirá el cifrado de gran alcance del SSL 128-bit, el cifrado más fuerte disponible, sin importar la versión del browser.

- Administrador de PKI (Infraestructura de llave publica)

El administrador PKI para certificados SSL es la solución más eficiente y rentable para las compañías que necesitan 5 o más certificados SSL para intranets, extranets, servidor de sitio web, operación interna del ISP, o todos los nombres de dominio de su compañía. Con una compra simple el administrador de servicios le deja fácilmente publicar y administrar todos los certificados SSL que necesita para asegurar todos los dominios de la empresa.

2- IPSCA

Internet Publishing Services Certification Authority. Autoridad Certificadora española que entrega certificados basados en SSL.

Tipos de Certificados que ofrece ipsca:

- Certificados de servidor.

Emite dos tipos de certificados de servidor:

Tipo A1. No existe una comprobación documental, sólo se comprueba la propiedad del dominio y la autorización por parte de sus contactos, mediante email.

Tipo A2. Existe una comprobación documental, se compra mediante transferencia bancaria y existe una gestión manual. Para emitir estos certificados se comprueba la identidad de la organización propietaria del servidor en cuestión.

- **Certificados personales.**

Tipos de certificados personales:

- B1. Certificado de Correo con validez mensual/anual.
- B2. Certificado Personal con verificación documental.
- B3. Certificado Personal Presencial.

- **Certificados de servidor WAP.**

- ***Certificados para firma de código.***

- ***Certificados para IPSEC VPN.***

Los Certificados de Servidor de ipsCA permiten incorporar el protocolo SSL (Secure Socket Layer) en un servidor Web. Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando la información que se envía entre ambos puntos, con una longitud de hasta 128 bits, protegiendo los datos personales, datos de tarjetas de crédito, números de cuenta, passwords, etc. Cobra especial importancia dentro del área del comercio electrónico, donde la seguridad es un elemento esencial para garantizar el desarrollo de este sistema.

3- ENTRUST

Entrust Secured, Autoridad Certificadora que ofrece Certificados para servidor Web y WAP que provee el primer paso de seguridad en Internet y ayuda a habilitar el comercio electrónico.

4.2.6 AUTORIDAD CERTIFICADORA EN EL SALVADOR

DIESCO EAN El Salvador es una organización empresarial, privada, sin fines de lucro, parte de la Cámara de Comercio e Industria, cuya misión es la de velar

por la mayor integración de las diferentes cadenas de abastecimiento (supply chains) del país, mediante la promoción y el desarrollo de estándares abiertos e internacionales de identificación y comunicación, el comercio electrónico y prácticas de logística, que ayuden a optimizar el intercambio comercial de bienes y servicios.

TELEDESPACHO:

Trámites de Importación por Internet.

Teledespacho es un proyecto de Comercio Electrónico implementado hasta la fecha por DIESCO EAN El Salvador.

El intercambio de información, particularmente de la Declaración de Mercancía y la respectiva respuesta por parte de la Dirección de Aduanas, se hace bajo estándares EDIFACT, con un modelo de seguridad altamente confiable, que contempla el uso de Certificados Digitales (estándar X509), Firma Digital, y Criptografía (infraestructura estándar de llave pública/privada – PKCS).

Para dicho Proyecto, el rol de **DIESCO EAN El Salvador** ha sido de gran envergadura, tanto por el Desarrollo de la Plataforma Tecnológica y Operativa de TELEDESPACHO, como por los Servicios Cerrados de emisión de Certificados Digitales **(a través de su Autoridad Certificadora, CERTIC@MARA- www.diescoean.com.sv)** Software de Firma Digital, y su Centro de Soporte.

CertiC@mara. La Primera Autoridad Certificadora Cerrada del País¹⁵:

Para el sistema de **TELEDESPACHO POR INTERNET**, se ha implementado el uso de la **Firma Electrónica Y Certificados Digitales** con el objetivo de asegurar las transacciones electrónicas de dicho proyecto. Estos mecanismos

¹⁵ (En anexos 4). Para más información ver Requisitos para solicitar Certificados Digitales y Firma Electrónica, y Certic@mara. Prácticas de Certificación Digital.

de seguridad permiten asegurar el envío y la recepción de la información, ya que el emisor, al firmar el documento electrónico y validarlo con su Certificado Digital, está dotando a dicho documento con las siguientes características de seguridad: **No repudio, autenticación e integridad del emisor del mensaje.** Esto le da la certeza al receptor de que quien firma y envía, es quien dice ser, por lo tanto no se puede hacer a nombre de un tercero. Adicionalmente este mensaje firmado se codifica (cifra) para que viaje por Internet en un lenguaje en que solo las partes involucradas podrán entenderlo.

Aclaración Importante: Los Certificados Digitales emitidos por CertiC@mara **solo certifican al Usuario**, no la Información y su uso es únicamente para Teledespacho por Internet (Tramites de Importación por Internet con la Dirección General de la Renta de Aduanas).



4.2.7 COSTOS PARA LA OBTENCIÓN DE CERTIFICADOS DIGITALES

VERISIGN

Certificados SSL. Servicio de Sitio Seguro

Características	Sitio Seguro	Sitio Seguro Pro
Un año	\$349	\$895
Dos años(recomendado)	\$598	\$1,595
Características de Base:		
Cifrado SSL	40-bit	128-bit
Autenticación de Servicios		
Sello de Sitio Seguro		
Protección seguridad de redes		

Administrador de PKI (Infraestructura de llave publica)

Certificados SSL	Administrador PKI para SSL Certificado: 40-bits	Administrador PKI para SSL Certificado: 128-bits
10	\$2,490	\$6,950
25	\$5,900	\$16,500
50	\$11,450	\$32,000
100	\$20,450	\$57,000
250	Contactar a los representantes de ventas verisales@verisign.com	

IPSCA

Tipo de Certificado	Precio(para 2 años)
Certificados de servidor:	
Tipo A1	\$69
Tipo A3	120 Euros
Certificados personales:	
Clase B1	10 Euros
Clase B2	20 Euros
Clase B3	50 Euros
Certificados WAP	195 Euros
Certificados para firma de código	195 Euros
Certificados para IPSEC - VPN	20 Euros

ENTRUST

Tipo de Certificado	Precio	
	1 Año	2 Años
Certificados para servidor Web	\$299	%549
Certificados para WAP	\$749	\$1,295

DIESCO EAN El Salvador.Certic@mar El Salvador

INVERSIÓN POR SERVICIOS:

Características	Precio
1. Sistema de teledespacho por Internet – pago inicial(único):	
1.1 Modulo de seguridad para SIDUNEA++ ¹⁶ : Mas la configuración, generación de llaves privadas y públicas, publicación en sitio web de la clave pública del usuario.	\$300.00
2. Servicios anuales:	
2.1 Soporte y mantenimiento de software:	\$250.00
2.2 Certificado digital	\$100.00
3. Servicio opcional:	
3.1 Visita adicional técnico	\$35.00

¹⁶ SIDUNEA es un sistema computerizado para la administración de aduanas que cubre la mayor parte de procedimientos de comercio exterior. El sistema maneja manifiestos y declaraciones de aduana, procedimientos de contabilidad, procedimientos de tránsito y regímenes suspensivos.

4.3 CRIPTOANÁLISIS

4.3.1 CRIPTOANÁLISIS UTILIZANDO EL ALGORITMO DE SHOR

Se parte del punto de la generación de llaves llevada a cabo por el algoritmo RSA como sigue:

Algoritmo para generar un par de llaves (**e** ,**d**)

1. Se eligen aleatoriamente dos números primos grandes, (**p** y **q** de entre 100 y 300 dígitos). Después se calcula el producto $n = pq$.

NOTA: Para motivos de demostración se tomará p y q de 2 dígitos ya que no se trabajará con una computadora cuántica, sino que, solo se simulará como trabajaría está mediante la librería Quantum::entanglement de Perl en una computadora clásica. Y como se menciona más adelante es prácticamente imposible determinar los factores primos de n sin conocer p y q.

2. Los valores p y q no se hacen públicos.
3. Se escoge un número e primo relativo con $(p - 1)(q - 1)$. (e, n) será la clave pública. Nótese que e debe tener inversa módulo $(p-1)(q-1)$,
4. Existirá un número d tal que

$$de \equiv 1 \pmod{(p - 1)(q - 1)}$$

es decir, que d es la inversa de e módulo $(p - 1)(q - 1)$. (d, n) será la clave privada. Esta inversa puede calcularse fácilmente empleando el Algoritmo Extendido de Euclides. Nótese que si desconocemos los factores de n, este cálculo resulta prácticamente imposible.

La codificación se lleva a cabo según la expresión:

$$c = m^e \pmod{n}$$

mientras que la decodificación se hará de la siguiente forma:

$$m = c^d \pmod{n}$$

De esta forma tenemos conocimiento que existe un mensaje codificado c y que para decodificarlo únicamente necesitamos conocer d para llegar al tener el mensaje original m .

Para nuestro caso de criptoanalistas partimos de que solamente conocemos n y llegaremos a d .

4.3.2 FUNCIONAMIENTO DE ALGORITMO CUANTICO DE SHOR

A continuación se describen de una forma resumida los cinco pasos. Y luego nos enfocaremos en la parte cuántica del algoritmo (paso 2).

Paso 1

Elegir aleatoriamente un entero positivo m . Utilizar el algoritmo de Euclides de tiempo polinomial para computar el máximo común divisor $\text{mdc}(m, N) \neq 1$, entonces habremos encontrado un factor no trivial de N , y regresaremos al inicio. En cambio si $\text{mcd}(m, N) = 1$, entonces pasamos al PASO 2.

PASO 2

Haciendo uso de la función QFT del modulo `Quantum::entanglement`¹⁷ determinar el periodo desconocido de P de la función

$$\begin{array}{ccc} \mathbb{N} & \rightarrow & \mathbb{N} \\ a & \mapsto & m^a \bmod N \end{array} \longrightarrow f_N$$

¹⁷ `Quantum::entanglement`, modulo del lenguaje de programación Perl que permite simular el modo de programación cuántico que incluye la función QFT.

Paso 3

Si P es un entero impar, entonces regresar al **Paso 1**. [La probabilidad de que P sea impar es $(1/2)^k$, donde k es el número de los distintos factores primos de N .] Si P es impar entonces procedemos al **Paso 4**.

Paso 4

Partiendo de que P es par

$$(m^{P/2} - 1)(m^{P/2} + 1) = m^P - 1 = 0 \pmod{N}$$

Si $m^{P/2} + 1 = 0 \pmod{N}$, entonces regresaremos al **Paso 1**. Si $m^{P/2} + 1 \neq 0 \pmod{N}$, se procede al **Paso 5**. Lo cual muestra que la probabilidad que $m^{P/2} + 1 = 0 \pmod{N}$ es menor que $(1/2)^{k-1}$, donde k denota el número de los distintos factores primos de N .

Paso 5

Usar el algoritmo de Euclides para computar $d = \text{mcd}(m^{P/2} - 1, N)$. Partiendo de que $m^{P/2} + 1 \neq 0 \pmod{N}$, puede mostrarse fácilmente que d es un factor no trivial de N . Fin del algoritmo devolviendo como respuesta d .

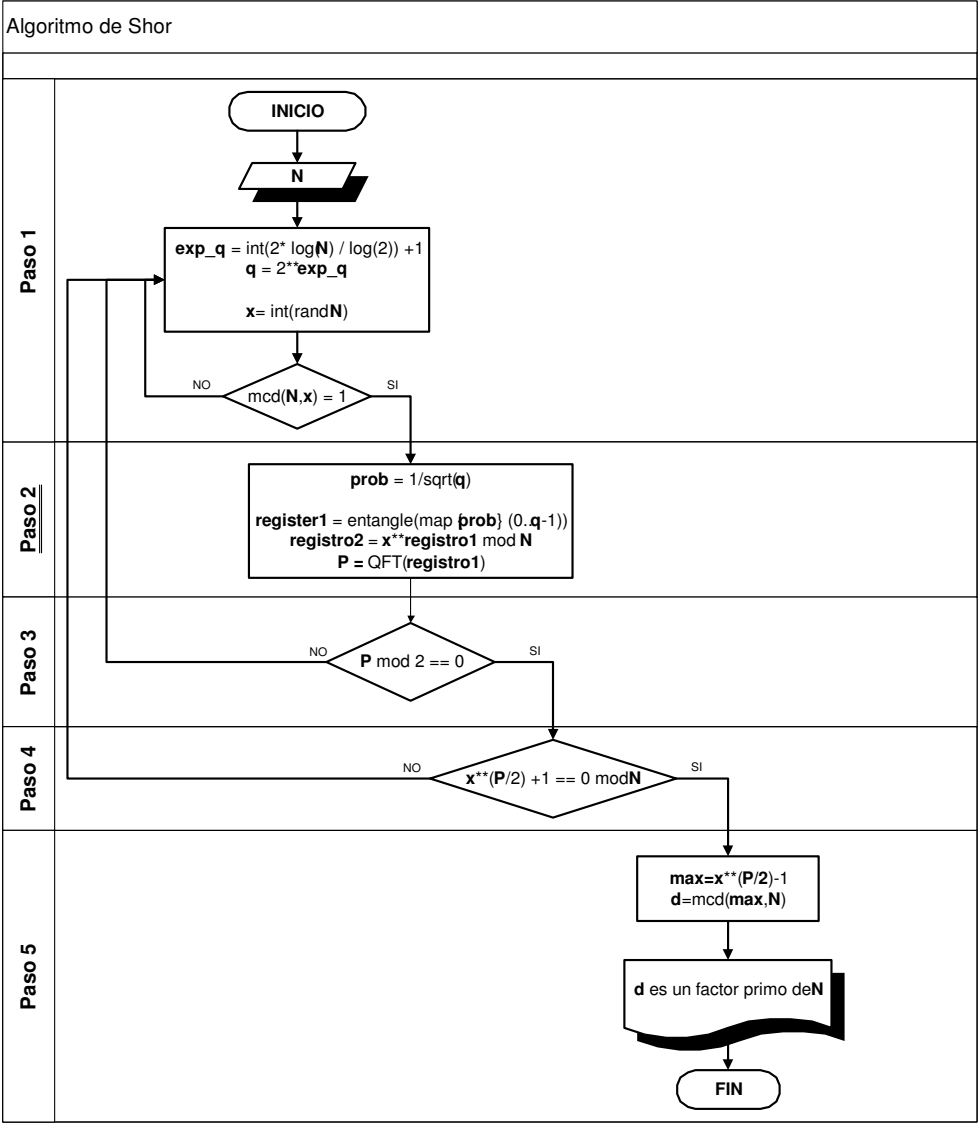
Así, la tarea de factorización un entero positivo impar N se reduce al problema siguiente:

Problema. Teniendo una función periódica

$$f : \mathbb{N} \rightarrow \mathbb{N}$$

encontrar el período P de f .

4.3.3 FLUJOGRAMA. ALGORITMO DE SHOR



4.3.4 EJEMPLO DEL ALGORITMO DE SHOR

El problema de hallazgo de los factores primos del número 15. El algoritmo consta de tres pasos importantes, se presentará esta explicación en 3 fases.

Fase 1

La primera fase del algoritmo es poner un registro de memoria en una superposición coherente de todos sus estados posibles. La letra 'Q' será usada para denotar un qubit que está en el estado coherente.

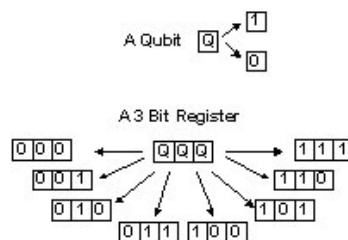


Figura 2. Un registro tres-qubit puede representar 8 estados clásicos simultáneamente.

Cuando un qubit está en el estado coherente, se puede pensar en cómo existir en dos universos diferentes. En un universo existe como un '1' y en el otro existe como un '0'. Extendiendo esta idea a el registro de 3 bits podemos imaginar que el registro existe en 8 universos diferentes, uno por cada uno de los estados clásicos que podría representar (i.e. 000, 001, 010, 011, 100, 101, 110, 111). Para tener el número 15, un cuarto bit es requerido (capaz de representar los números 0 a 15 simultáneamente en el estado coherente).

Un cálculo ejecutado en el registro se puede pensar como un grupo entero de cálculos ejecutados en paralelo, uno en cada universo. En efecto un cálculo ejecutado en el registro es un cálculo ejecutado en cada valor posible que un registro puede representar.

Fase 2

La segunda fase del algoritmo ejecuta un cálculo usando el registro. Los detalles de cuales son, es el siguiente:

- El número N es el número que deseamos factorizar, $N = 15$.
- Un número al azar X se escoge, donde $1 < X < N-1$.
- X es elevado a la potencia contenida en el registro (registro A) y entonces dividido por N.
- El resto de esta operación se pone en un segundo registro de 4 bits (registro B).

Después de ejecutar esta operación, el registro B contiene la superposición de cada uno de los universos resultantes. Esto se ilustra mejor con un ejemplo, si escogemos X igual a 2, entonces el contenido del registro B, por cada valor posible en registro A es como sigue:

Register B

Q Q Q Q

= X

Register A

Q Q Q Q

MOD N

Figura 3.Funcionamiento ejecutado en Fase 2

Register A	Register B
0	1
1	2
2	4
3	8
4	1
5	2
6	4
7	8
8	1
9	2
10	4
11	8
12	1
13	2
14	4
15	8

Notice that the contents of register B follows a repeating sequence (1,2,4,8,1,2,4,8...), the frequency at which this repeats can be named f. In this case the repeating sequence (1,2,4,8) has four values so f=4.

Tabla 1. Contenido del registro B, cuando N=15 y X=2.

Fase 3

La fase final es quizás la más difícil seguir. La frecuencia de repetición, f , puede ser encontrada usando una computadora cuántica. El valor resultante para f es entonces usado en la siguiente ecuación para calcular un posible factor.

$$\text{Factor } P = X^{f/2} - 1$$

Figura 4. Ecuación usada para calcular el factor.

En nuestro ejemplo el valor $f=4$ da una respuesta correcta de 3.

4.3.5 CÓDIGO FUENTE DEL ALGORITMO DE SHOR

```
#!/usr/bin/perl -w
```

```
DIE 'ERROR: ./SHOR.PL [NO SE ENCUENTRA EL NUMERO A FACTORAR]'  
UNLESS @ARGV;
```

```
use strict;  
use warnings;  
use Quantum::Entanglement qw(:DEFAULT :complex :QFT);  
$Quantum::Entanglement::destroy = 0;
```

```
my $num = $ARGV[0];
```

```
# algunas validaciones  
die "$num es un multiplo de dos ..." unless $num %2;  
die "$num no es entero ..." unless $num == int($num);  
die "$num es menor que 15" unless $num >= 15;
```

```
print "Desarrollando los pasos clásicos iniciales:\nPASO 1\n";  
# encontrando el valor de q (tamaño de los registros cuánticos)  
my $q_exp = int(2* log($num) / log(2)) +1;  
my $q = 2 ** $q_exp;
```

```

# seleccionando x tal que x es un primo relativo de n.
my $x;
do {
    $x = int(rand $num) + 1;
} until ($num % $x != 0 and $x > 2);

print "Utilizando q:$q, x:$x\nPASO 2:Iniciando parte cuantica\n";

# llenando el registro1 cuántico desde 1..q
my $prob = 1/sqrt($q);
my $registro1 = entangle(map {$prob, $_} (0..$q-1));

# Evaluando  $F = x^{|a\rangle} \bmod n$ , luego guardar en registro 2
# (función necesaria para evitar que p_func de desbordamiento **)

sub power_mod {
    my ($estado, $x1, $num1) = @_;
    my $rt = 1;
    return 1 if $estado == 0;
    return 1 if $estado == 1;
    for (1..$estado) {
        $rt = ($rt * $x1) % $num1;
    }
    return $rt;
}

print "Ejecución de  $F = x^{|a\rangle} \bmod n$ \n";
my $registro2 = p_func(\&power_mod, $registro1, $x, $num);

# Observamos que $registro2, esta colapsando en $registro1
my $k = "$registro2";

print "\$registro2 colapsado para $k\n";
print "Encontrando el período F (utilizando QCD)\n";

# tomando las amplitudes del registro1, y colocandolos en el registro3
my $registro3 = QFT($registro1);

my $lqnr = "$registro3"; # observese, que este debe ser multiplo de q/r
if ($lqnr == 0) {
    print "Período encontrado '0', deteniendo\n"; exit(0);
}
my $period = int($q / $lqnr + 0.5); # redondeando

print "El período de  $F = x^{|a\rangle} \bmod n$  es $period\n";

```

```

# teniendo el período, necesitamos resolver el factor de n
# resolviendo las dos formas:

if ($period % 2 != 0) {
    print "$period no es un numero par, duplicando para";
    $period *=2;
    print " $period\n";
}

my $uno = $x**($period/2) -1;
my $dos = $x**($period/2) +1;

# uno y dos son mcd en comun con n, para los cuales ahora encontramos...
print "$one * $two y $num son mcd (paso clasico)\n";
my ($max1, $max2) = (1,1);
for (2..$num) {
    last if $_ > $num;
    unless (($num % $_) || ($uno % $_)) {
        $max1 = $_;
    }
    unless (($num % $_) || ($dos % $_)) {
        $max2 = $_;
    }
}
print "$max1, $max2 podrían ser factores de $num\n";

```


4.4 ANÁLISIS DE RESULTADOS (SOBRE EL IMPACTO EN LA EMPRESA SALVADOREÑA)

Nuestro análisis está orientado a diferentes tipos de empresas de El Salvador tomando una población de las empresas que corresponden al área comercial, industrial, de comunicación, financieras y aduaneras que utilizan los servicios de Internet.

4.4.1 INTERPRETACIÓN DE LOS RESULTADOS DE ENCUESTAS

Después de haber realizado la investigación de campo por medio de las técnicas establecidas, se procesaron los datos recabados por medio de tablas estadísticas las cuales proporcionan información del objeto en estudio y, están conformadas por títulos, encabezado, concepto o columna matriz y cuerpo.

Los tipos de gráficos que se utilizan son de pastel o circular y el gráfico de barras agrupadas. El gráfico de pastel, consiste en una circunferencia cuya superficie está dividida en sectores circulares, cada una de las cuales representa la parte proporcional de los datos o la suma de todas las frecuencias. El gráfico de barras agrupadas, consiste en un plano cartesiano en el que se encuentran una serie de barras donde cada una representa una categoría; de tal manera que se pueden comparar los valores entre cada categoría de la serie. La razón por la que se utilizan estos tipos de gráficos, es debido a que por sus características la visualización de los resultados se hace más fácil.

ENTREVISTAS

a. Empresas

Las entrevistas a empresas se realizó de manera paralela con las encuestas, ya que para lograr obtener los datos solicitados en la misma fue necesario

concertar entrevistas con el personal involucrado. Los datos obtenidos en las mismas se recopiló en las encuestas.

b. Expertos en el tema

En esta etapa se realizó una entrevista con dos personas que por su experiencia y por su trabajo, tienen conocimiento sobre criptografía, la generación de las llaves, el uso de Certificados Digitales y Firmas Electrónicas. Esto con el objetivo de tener una base metodológica sobre el desarrollo e implementación de los Certificados Digitales.

De esta parte de la investigación, se obtuvo información de importancia para mostrar los tipos de Certificados Digitales, conocer sus ventajas y desventajas, el proceso, los tramites y costos para la obtención de estos.

De igual manera, se obtuvo información sobre las implementaciones que tienen los algoritmos asimétricos de cifrado y su funcionamiento.

Por otra parte, se coincidió en el hecho de que en el país existe muy poca información sobre los mecanismos de seguridad que utilizan las empresas de El Salvador, y que no existe una Institución o entidad que oriente a las empresas en este aspecto.

OBSERVACIÓN

Esta etapa se realizó en paralelo con las entrevistas y con las encuestas. Se logro obtener información sobre el tipo de mecanismos de seguridad que utilizan algunas de las empresas de El Salvador entrevistadas y encuestadas, De igual manera se obtuvo información sobre las actitudes, conocimientos y

tendencias de las empresas en cuanto a tecnología informática. Al igual que las entrevistas, la información obtenida se recopiló en las encuestas.

ENCUESTAS

OBJETIVO GENERAL

Recolectar información que permita analizar las consecuencias que tendría el desarrollo de la computación cuántica, determinando cuales son los mecanismos de seguridad que utilizan algoritmos asimétricos que poseen las empresas de El Salvador; así como determinar en que medida a las empresas les afecta tener presencia en Internet a través de un sitio web, el tipo de tecnología que utilizan para el mantenimiento de los mismos y sus capacidades y disponibilidad de inversión.

PRESENTACIÓN DE LOS RESULTADOS

Para poder realizar la investigación, se paso un cuestionario a empresas que poseen Internet en nuestro país, el cuestionario esta dividido en 3 partes, la primera parte va orientada a conocer acerca de los diferentes servicios utilizados en el Internet por las empresas, la segunda parte va orientada a la seguridad que poseen las empresas con respecto a los servicios de Internet que ellos poseen o utiliza y la tercera parte es orientada al conocimiento que se posee en la empresa acerca de temas como la criptografía y la computación cuántica, además de conocer si estos temas anteriores afectarían a ellas.

Parte 1.

Pregunta N°1

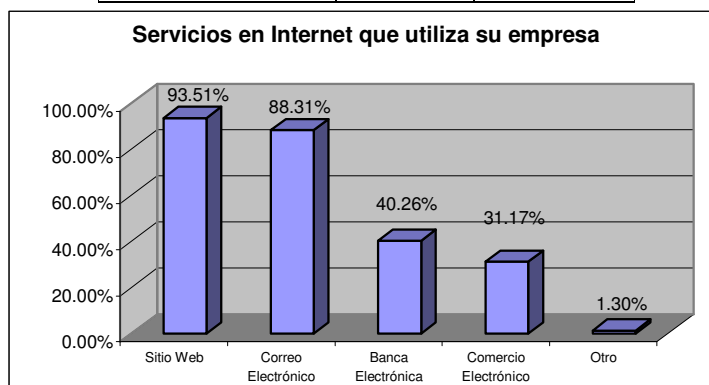
¿Cuál de los siguientes servicios de Internet utiliza su empresa?

Objetivo

Agrupar y conocer los diferentes servicios de Internet que utilizan las empresas en nuestro país.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
Sitio Web	72	93.51%
Correo Electrónico	68	88.31%
Banca Electrónica	31	40.26%
Comercio Electrónico	24	31.17%
Otro	1	1.30%



Hallazgo:

De acuerdo a los resultados de la gráfica anterior, de las 77 empresas encuestadas, el 93.51% poseen sitio Web, el 88.31% hacen uso del correo electrónico, también podemos observar que el uso de la banca electrónica es utilizado por las empresas en un 40.26% y el menor servicio utilizado sería el de comercio electrónico con un 31.17%.

Pregunta N°2

Esta orientada acerca del sitio web que posee la empresa.

Objetivo

Identificar las características que las empresas tienen en el uso de un servidor web. Esta pregunta se divide en 3 preguntas con la finalidad de darnos más información acerca de este tipo de servicio utilizado en la empresa

Pregunta N° 2A

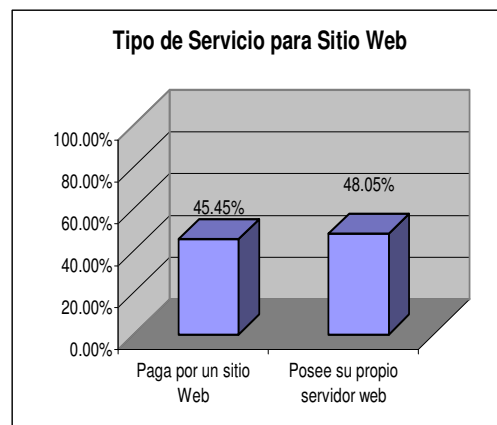
¿Tipo de servicio?

Objetivo

Identificar el tipo de servicio que utiliza la empresa para tener su sitio web.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
Paga por un sitio Web	35	48.61%
Posee su propio servidor web	37	51.39%
Total	72	100.00%



Hallazgo:

La grafica de la Pregunta 2A, nos muestra que de las 72 empresas que poseen sitio web, el 51.39% de ellas posee su propio servidor web para su sitio, mientras que solamente el 48.61% paga por un sitio web. Esto nos indica cuales empresas pueden poseer su propio certificado de seguridad; ya que solo las que tienen su propio servido web pueden adquirirlo. Dado que las que pagan por un sitio web es porque tienen alojado su sitio en un web hosting y el proveedor del web hosting será el encargado de proporcionar al cliente un servidor web seguro.

Pregunta N° 2B

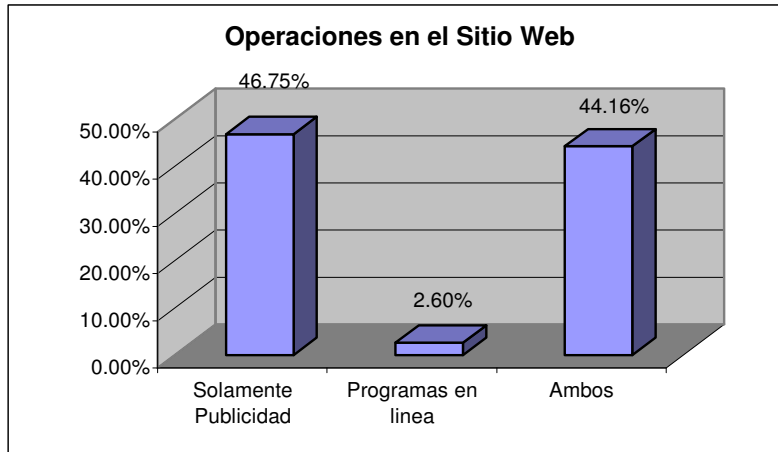
¿Qué operaciones realiza en el sitio web?

Objetivo

Conocer que operaciones se encuentran involucradas en el sitio web de la empresa y saber que tan importante es la información que manejan en el sitio web.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
Solamente Publicidad	36	50.00%
Programas en línea	2	2.78%
Ambos	34	47.22%
Total	72	100%



Hallazgo

De las empresas que poseen su sitio web, podemos observar en el grafico que el 50.00% realizan las operaciones de Publicidad y programas en línea, mientras que la mayoría se encarga solamente de publicidad con un 47.22% y lo que es solo programas en línea es bien bajo por que solo el 2.78% de las empresas lo hace.

Si una empresa utiliza el servidor web solo para publicidad, no es necesario que tenga seguridad, ya que no realiza transacciones.

Pregunta N° 2C

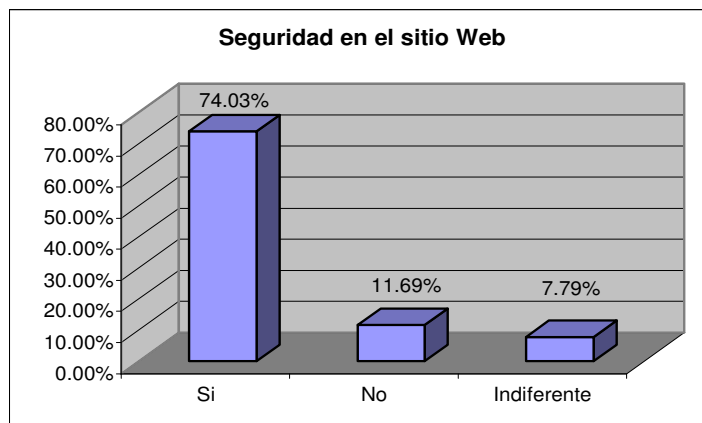
¿Considera necesaria la seguridad en este servicio?

Objetivo

Identificar que tan importante es para la empresa el tener seguridad en su servidor web.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
Sí	57	79.17%
No	9	12.50%
Indiferente	6	8.33%
Total	72	100%



Hallazgo

Según se nos muestra en el gráfico, de las empresas que poseen sitio web, el 79.17% de estas considera que la seguridad es muy importante, podemos observar que son pocas las empresas que consideran no necesaria la seguridad y mucho menor a los que le es indiferente.

Pregunta N°3

Esta orientada acerca del servicio de correo electrónico.

Pregunta N° 3A

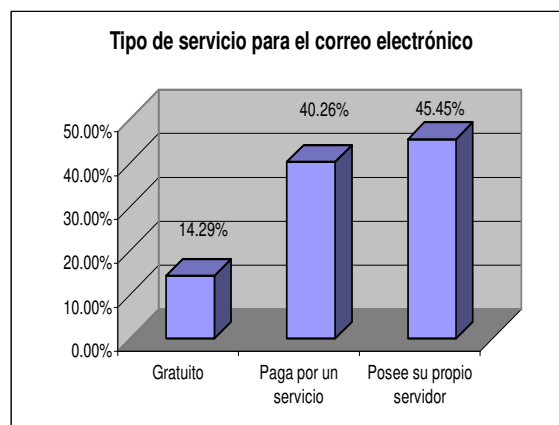
¿Qué tipo de servicio posee?

Objetivo

Conocer acerca del tipo de servicio que adquirió la empresa para el uso de sus correos electrónicos.

Resultado

ALTERNATIVA	EMPRESA	PORCENTAJE
Gratuito	2	2.94%
Paga por un servicio	34	50.00%
Posee su propio servidor	32	47.06%
Total	68	100%



Hallazgo

Según se nos muestra en el grafico la mayoría de empresas que utilizan el servicio de Internet de correo electrónico, poseen su propio servidor de este

servicio en un 51.47%. El 45.59% paga por el servicio y el resto lo utiliza gratuito solamente.

Pregunta N° 3B

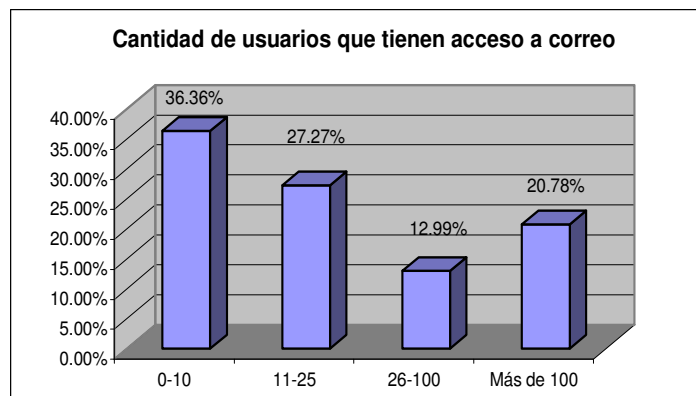
¿Cuántos usuarios tienen acceso al correo electrónico?

Objetivo

Determinar la cantidad de usuarios que hacen uso del servicio de correo electrónico en la empresa.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
0-10	25	36.76%
11-25	18	26.47%
26-100	9	13.24%
Más de 100	16	23.53%
Total	68	100%



Hallazgo

Según nos muestra el grafico, del total de empresas que utilizan el correo electrónico, se muestra que la cantidad de usuarios de 0-10 es la que tiene mayor acceso a este dando un 36.76%.

Pregunta N° 3C

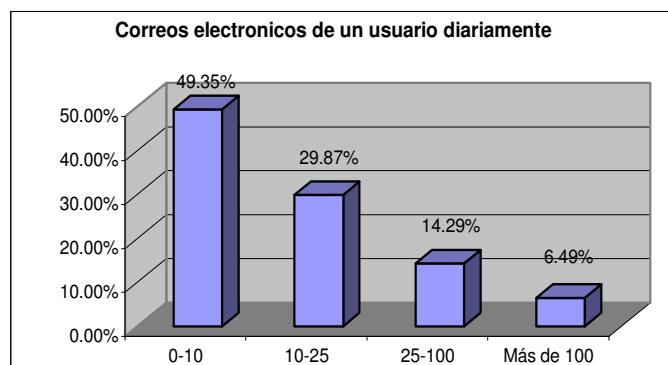
¿Aproximadamente cuantos correos electrónicos recibe y envía cada usuario diariamente?

Objetivo

Determinar la cantidad de correos que son enviados o recibidos dentro de la empresa en un día.

Resultado

ALTERNATIVA	EMPRESAS	PORCENTAJE
0-10	34	49.35%
10-25	22	29.87%
25-100	7	14.29%
Más de 100	5	6.49%
Total	68	100%



Hallazgo

El grafico nos muestra que del total de empresas que utilizan correo electrónico, el porcentaje mayor de enviar y recibir correos electrónicos anda de 0 a 10 correos diarios y el menor de estos anda en más de 100, como observamos el porcentaje mayor es de 50.00% y el menor es de 7.35%.

Pregunta N° 3D

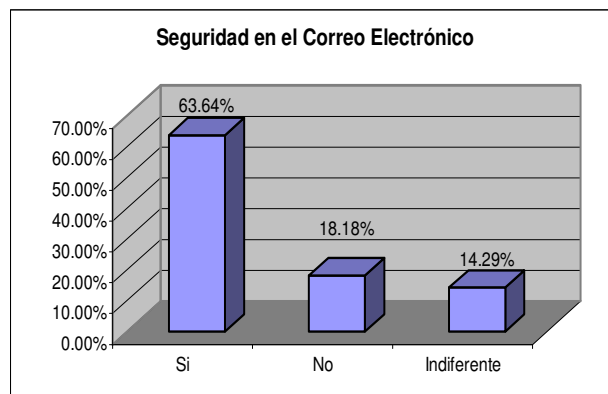
¿Considera necesaria la seguridad en este servicio?

Objetivo

Determinara que tan importante considera la seguridad la empresa en el uso del correo electrónico dentro de ella.

Resultado

ALTERNATIVA	EMPRESA	PORCENTAJE
Sí	49	72.06%
No	14	20.59%
Indiferente	5	7.35%
Total	68	100%



Hallazgo

El gráfico nos muestra que la mayoría de empresas que utilizan correo electrónico considera importante la seguridad en un 72.06%, mientras que el porcentaje de que es indiferente es el mas bajo con un 7.35%.

Pregunta N°4

Esta orientada acerca de la banca electrónica.

Pregunta N° 4A

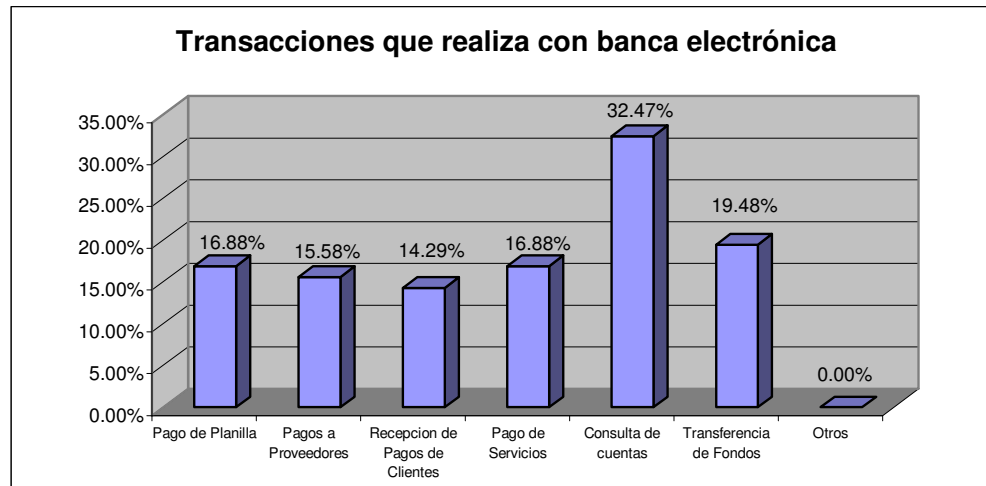
Si su empresa utiliza banca electrónica ¿Cuáles de las siguientes transacciones realiza?

Objetivo

Identificar los tipos de transacciones que se realizan dentro de la empresa, haciendo uso de la banca electrónica.

Resultados

ALTERNATIVAS	EMPRESAS	PORCENTAJE
Pago de Planilla	13	16.88%
Pagos a Proveedores	12	15.58%
Recepción de Pagos de Clientes	11	14.29%
Pago de Servicios	13	16.88%
Consulta de cuentas	25	32.47%
Transferencia de Fondos	15	19.48%
Otros	0	0.00%



Hallazgo

El grafico nos muestra que el servicio mas utilizado de la banca electrónica en el Internet es el de Consulta de Cuentas con un 32.47%, mientras que el menos utilizado es el de recepción de pagos de clientes con el 14.29%.

Pregunta N° 4B

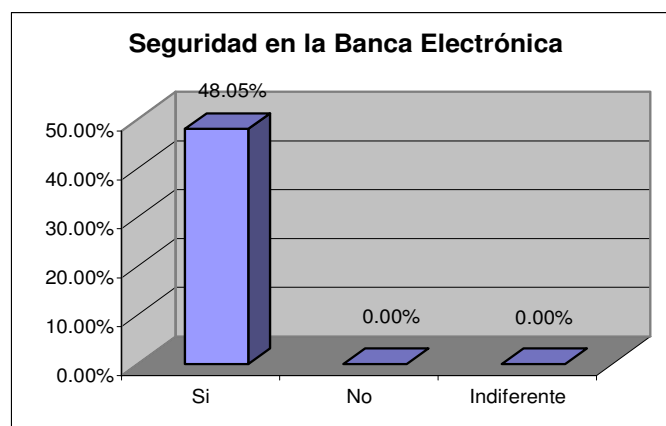
¿Considera necesaria la seguridad en este servicio?

Objetivo

Determinara que tan importante considera la seguridad la empresa en el uso de la banca electrónica para su empresa.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
Sí	31	100.00%
No	0	0.00%
Indiferente	0	0.00%
Total	31	100.00%



Hallazgo

Según observamos en el gráfico todas las empresas que hacen uso de la banca electrónica consideran que es muy necesaria la seguridad en este servicio que se provee en Internet.

Pregunta N°5

Esta orientada acerca del comercio electrónico.

Pregunta N° 5A

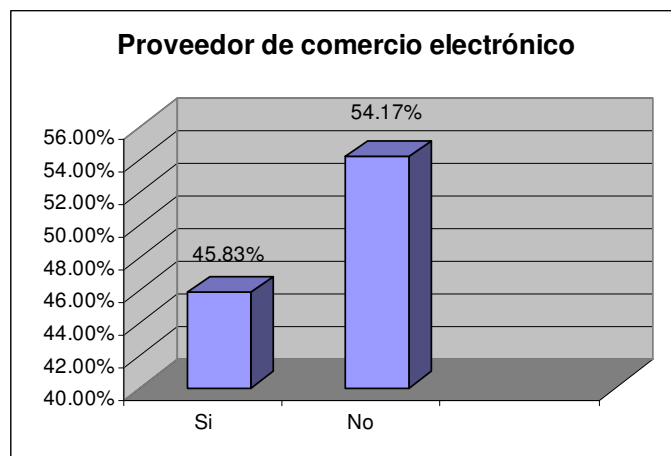
¿Su empresa es proveedor de comercio electrónico?

Objetivo

Determinar la cantidad de empresas que proveen comercio electrónico en nuestro país.

Resultados

ALTERNATIVA	EMPRESA	PORCENTAJE
Sí	11	19.48%
No	13	11.64%
Total	24	100.00%



Hallazgo

Según observamos en el grafico, del total de empresas que utilizan comercio electrónico, las empresas que proveen comercio electrónico representan el 45.83% y un 54.17% se consideran empresas clientes del comercio electrónico.

Pregunta N° 5B

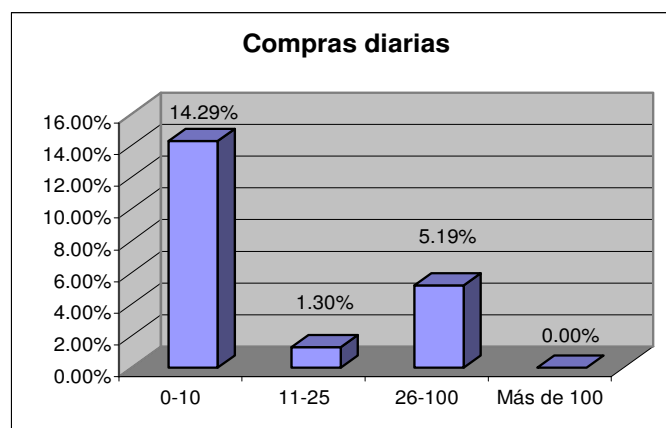
¿Si su empresa realiza compras a través de Internet, cuantas realiza diariamente?

Objetivo

Identificara el uso del comercio electrónico en las empresas de nuestro país.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
0-10	8	61.54%
11-25	1	7.69%
26-100	4	30.77%
Más de 100	0	0.00%
Total	13	100.00%



Hallazgo

El gráfico nos muestra que de las empresas que utilizan comercio electrónico, el rango más elevado de compras es de 0-10, si observamos el porcentaje es de 61.54%, mientras que el segundo nivel mas alto es el del rango de 26-100 que es de 30.77%.

Pregunta N° 5C

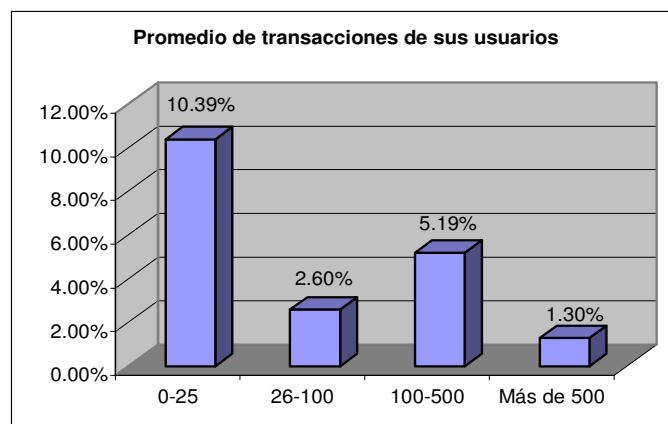
¿Si su empresa es proveedor de Comercio electrónico, cual es el promedio de transacciones de compra que los usuarios realizan diariamente?

Objetivo

Determinar cuantas transacciones se realizan en una empresa que sea proveedora de comercio electrónico.

Resultados

ALTERNATIVA	EMPRESA	PORCENTAJE
0-25	6	54.55%
26-100	3	27.27%
100-500	1	9.09%
Más de 500	1	9.09%
Total	11	100.00%



Hallazgo

Según se nos muestra en el grafico, del total de empresas que usas comercio electrónico, las empresas que son proveedoras de este servicio, muestran que sus usuarios están enviando en su mayoría entre 0 a 25 transacciones es decir el 54.55%.

Pregunta N° 5D

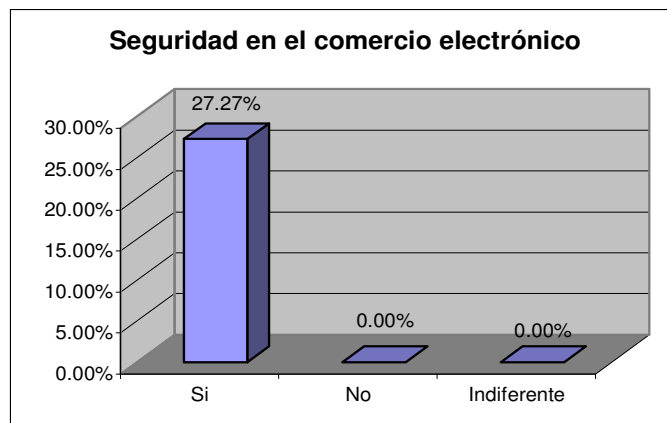
¿Considera necesaria la seguridad en este servicio?

Objetivo

Determinara que tan importante considera la seguridad la empresa en el uso del comercio electrónico.

Resultados

ALTERNATIVA	EMPRESA	PORCENTAJE
Sí	24	100.00%
No	0	0.00%
Indiferente	0	0.00%
Total	24	100.00%



Hallazgo

Según observamos en el grafico todas las empresas que hacen uso del comercio electrónico consideran que es muy necesaria la seguridad en este servicio en Internet.

Parte 2

Sobre la seguridad en los servicios de Internet que utiliza su empresa.

Pregunta N°6

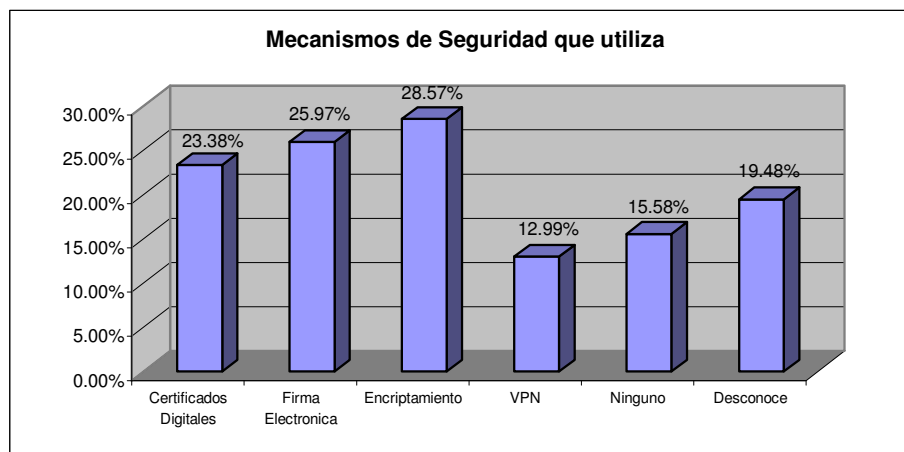
¿Qué mecanismo de seguridad utiliza?

Objetivo

Identificar los mecanismos de seguridad que posee la empresa para sus servicios de Internet

Resultados

ALTERNATIVA	MECANISMOS DE SEGURIDAD	PORCENTAJE
Certificados Digitales	18	23.38%
Firma Electrónica	20	25.97%
Cifrado de datos	22	28.57%
VPN	10	12.99%
Ninguno	12	15.58%
Desconoce	15	19.48%



Hallazgo

Según el gráfico determinamos que el mecanismo más utilizado por las empresas es el de Cifrado de datos con el 28.57%, luego continuamos con lo que es el mecanismo de la firma electrónica con el 25.67% y lo que es los certificados digitales con el 23.38%

Pregunta N°7

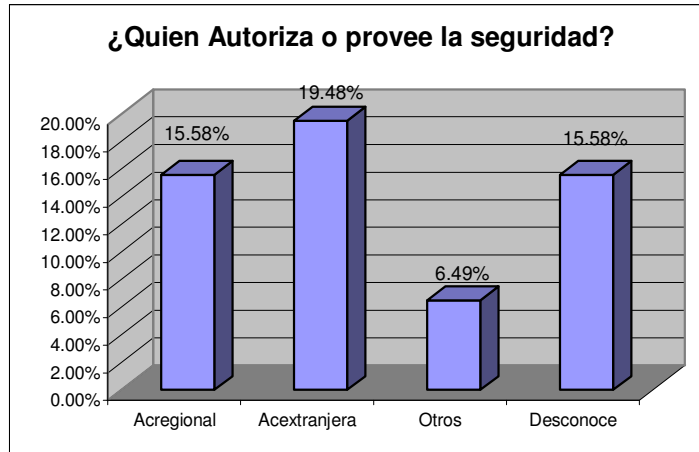
¿Quién autoriza o provee la seguridad?

Objetivo

Identificar la autoridad certificadora que provee la seguridad a las empresas de nuestro país según los mecanismos de seguridad utilizados.

Resultados

ALTERNATIVA	MECANISMOS	
	DE SEGURIDAD	PORCENTAJE
AC Regional	12	17.14%
AC Extranjera	15	21.43%
Autofirmado	5	7.14%
Desconoce	38	54.29%
Total	70	100.00%



Hallazgo

Tomando en cuenta la pregunta anterior se observó que un total de 70 mecanismos de seguridad son utilizados por las empresas, este total es tomado como base para identificar quien autoriza o provee dicha seguridad.

Es notorio que en la mayoría se desconoce quien provee la seguridad, pero de las que se conocen la AC Extranjera provee la seguridad a las empresas en un 21.43%, siendo esta forma la mayor utilizada.

Pregunta N°8

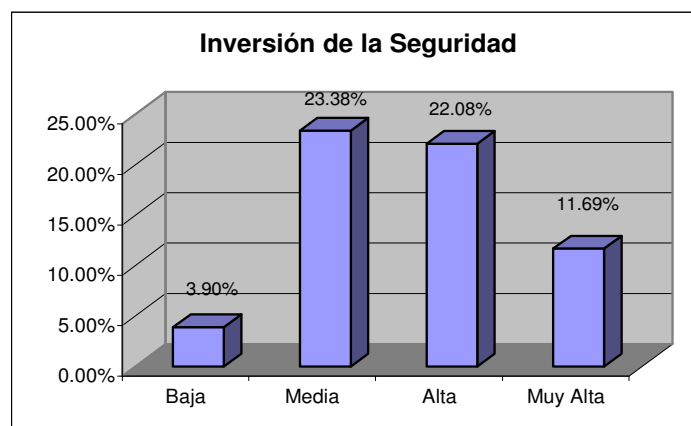
¿Cómo considera la inversión de la seguridad?

Objetivo

Identificar como considera la empresa que es la inversión realizada en la seguridad para los servicios de Internet de la empresa.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
Baja	10	12.99%
Media	29	37.66%
Alta	27	35.06%
Muy Alta	11	14.29%
Total	77	100%



Hallazgo

Según el grafico, con relación al total de las empresas encuestadas el 37.66% considera el nivel de Inversión en seguridad como media, como observamos es menor el porcentaje que considera que la inversión en la seguridad es baja.

Parte 3

Estas preguntas van dirigidas a la persona que contesto la encuesta.

Pregunta N°9

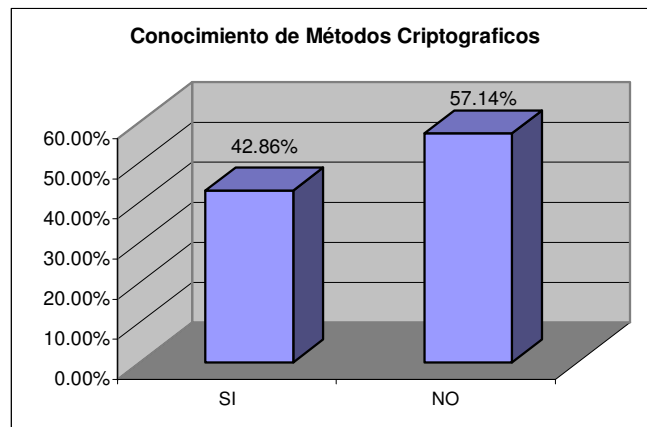
¿Tiene conocimiento de los métodos criptográficos que utiliza el mecanismo de seguridad de su empresa?

Objetivo

Identificar todas aquellas empresas en las cuales conozcan acerca de los métodos criptográficos que se utilizan para la seguridad.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
SÍ	33	42.86%
NO	44	57.14%
Total	77	100.00%



Hallazgos

Según el grafico se nos muestra que en las empresas, el 57.14% de las personas encargadas de los departamentos de informática desconoce sobre los métodos criptográficos de seguridad que utiliza y solo el 42.86% sabe que métodos criptográficos utilizan en su empresa, esto demuestra que aun no hay una orientación de la importancia que puede tener el conocimiento de métodos criptográficos para ciertas operaciones que se puedan realizar dentro de la empresa.

Pregunta N°10

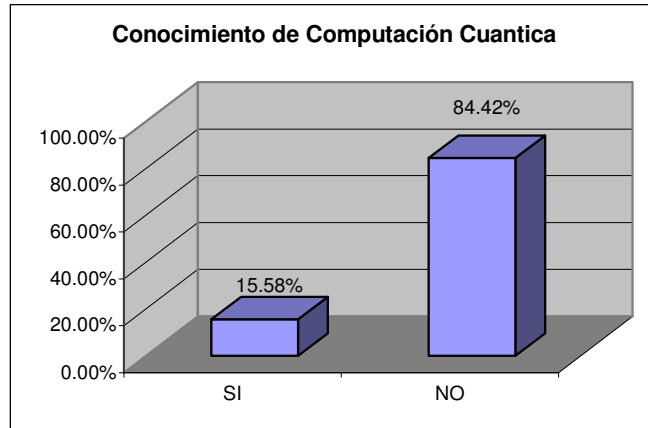
¿Tiene conocimiento de lo que es la computación cuántica?

Objetivo

Identificar todas aquellas empresas que realmente poseen o no un conocimiento acerca de lo que es la computación cuántica.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
SÍ	12	15.58%
NO	65	84.42%
Total	77	100.00%



Hallazgo

Según el grafico se nos muestra que en las empresas, el 84.42% de las personas encargadas de los departamentos de informática desconoce sobre la computación cuántica y solo el 15.58% conoce sobre este tema, esto nos llevan que las empresas no saben que el uso de la computación cuántica puede afectar sus métodos criptográficos en un futuro.

Pregunta N°11

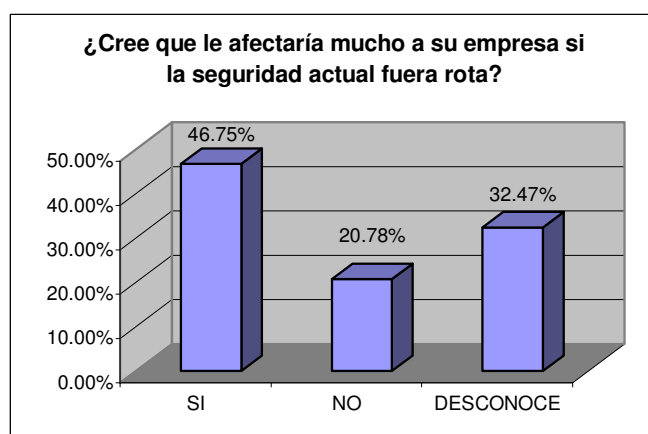
¿Cree que le afectaría mucho a su empresa si la seguridad actual fuera rota fácilmente y como les afectaría?

Objetivo

Identificar las empresas que consideran que si su seguridad fuera rota les afectaría, y determinar en que les afectaría más.

Resultados

ALTERNATIVA	EMPRESAS	PORCENTAJE
SÍ	36	46.75%
NO	16	20.78%
DESCONOCE	25	32.47%
Total	77	100.00%

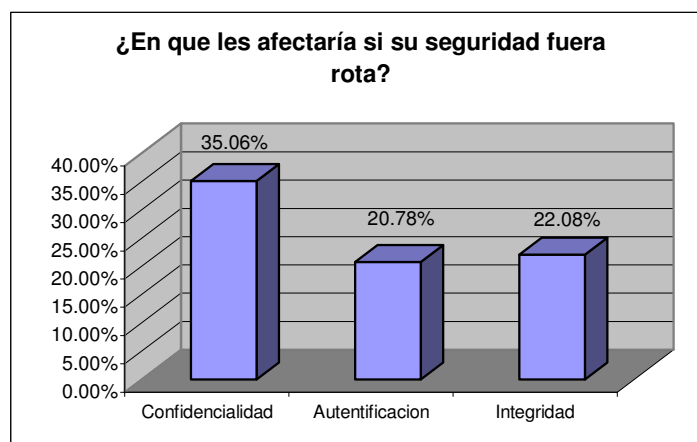


Hallazgo

Según se nos muestra en el grafico el 46.75% acepta que si su seguridad fuera rota les afectaría, mientras el 20.78% dice que si la seguridad fuera rota no afectaría en nada, pero el 32.47% desconoce si le afectase. Esto nos lleva a que es alto el nivel de empresas que desconocen acerca de que tan importante es la seguridad en su empresa.

Resultado

ALTERNATIVA	EMPRESAS	PORCENTAJE
CONFIDENCIALIDAD	27	35.06%
AUTENTIFICACION	16	20.78%
INTEGRIDAD	17	22.08%



Hallazgo

La mayoría de empresas determina que si su seguridad fuera rota lo que más les afectaría sería su confidencialidad.

4.4.2 ANÁLISIS DE LOS RESULTADOS OBTENIDOS

PORCENTAJES ABSOLUTOS. TOTAL DE EMPRESAS = 77

	SITIO WEB			CORREO ELECTRONICO		
	FR	%relativo	%absoluto	FR	%relativo	%absoluto
Paga por sitio web	35	49%	45%	34	50%	44%
Posee su propio servidor web	37	51%	48%	32	47%	42%
Gratis				2	3%	3%
Total	72	100%	94%	68	100%	88%
Solamente como publicidad	8	11%	10%			
Programas en línea	0	0%	0%			
Ambos	29	40%	38%			
Total	37	51%	48%			

ALTERNATIVA	CORREO ELECTRÓNICO					
	Usuarios que tienen acceso a correo electrónico			Correos que envía y recibe por día cada usuario		
	FR	%relativo	%absoluto	FR	%relativo	%absoluto
0-10	25	37%	32%	34	50%	44%
11-25	18	26%	23%	22	32%	29%
26-100	9	13%	12%	7	10%	9%
mas de 100	16	24%	21%	5	7%	6%
Total	68	100%	88%	68	100%	88%

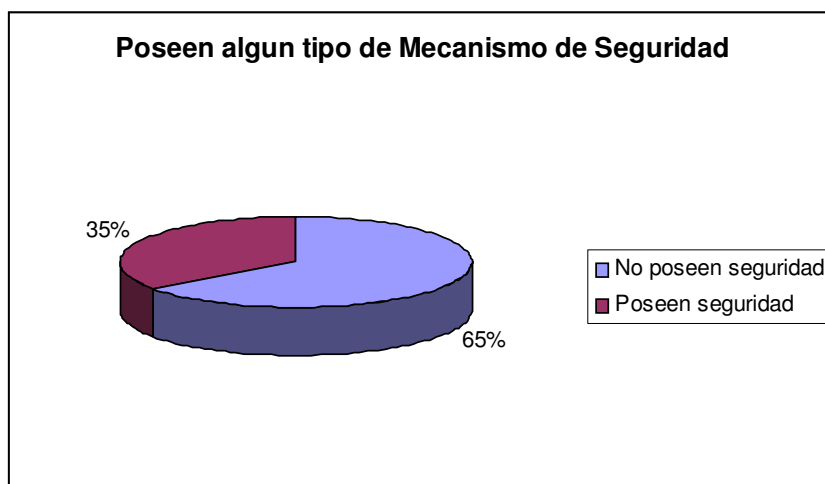
ALTERNATIVA	COMERCIO ELECTRÓNICO					
	Compras que realizan diariamente las empresas- (cliente)			Compras que se realizan diariamente a un comercio electrónico (proveedor)		
	FR	% relativo	%absoluto	FR	% relativo	%absoluto
0-10	8	62%	10%	6	55%	8%
11-25	1	8%	1%	3	27%	4%
26-100	4	31%	5%	1	9%	1%
más de 100	0	0%	0%	1	9%	1%
Total	13	100%	17%	11	100%	14%

ALTERNATIVA	SITIO WEB			CORREO ELECTRONICO			BANCA ELECTRONICA			COMERCIO ELECTRONICO		
	FR	% rel	% abs	FR	% rel	% abs	FR	% rel	% abs	FR	% rel	% abs
SÍ	57	79%	74%	49	72%	64%	31	100%	40%	24	100%	31%
NO	9	13%	12%	14	21%	18%	0	0%	0%	0	0%	0%
Le es indiferente	6	8%	8%	5	7%	6%	0	0%	0%	0	0%	0%
Total	72	100%	94%	68	100%	88%	31	100%	40%	24	100%	31%

RESUMEN DE TABULACIÓN relativa al total =77		
	Total	%
Tienen al menos 1 servicio	77	100%
Tienen sitio web o correo electrónico	68	88%
Tienen sitio web y posee servidor web propio	37	48%
Tienen servidor web propio y programas en línea y publicidad	29	38%
Tienen correo electrónico y servidor de correo propio	32	42%
Servidor web propio o servidor de correo propio	34	44%
Servidor web propio o servidor de correo propio y al menos un mecanismo de seguridad	27	35%

EMPRESAS QUE POSEEN ALGÚN TIPO DE SEGURIDAD

ALTERNATIVA	EMPRESAS	PORCENTAJE
No poseen seguridad	50	65%
Poseen seguridad	27	35%
Total	77	100%



Al haber tomado una muestra de 77 correspondiente a una población de 383 empresas de El Salvador que pertenecen al área industrial, comercial, de comunicación, financiero y aduanal; pudimos observar a través del resultado de las encuestas lo siguiente:

- Que en nuestro país el servicio de Internet mas utilizado es el sitio web, con un 93.51%, siguiéndole el correo electrónico en un 88.31%, la banca electrónica en un 40.26% y el comercio electrónico en un 31.17%.
- De las empresas que poseen sitio web un 48% posee su propio servidor web, de éstas un 38% solo utiliza para programas en línea y publicidad dando referencia para identificar cuales son las posibles empresas que son candidatas para que posean algún mecanismo de seguridad, se identifico también que en el ámbito de empresas un 74% considera que es necesaria la seguridad para este servicio.
- Con relación al correo electrónico un 42% posee su propio servidor de correo y un 64% considera que es necesaria la seguridad en este servicio. Por lo que podemos ver que los que poseen su propio servidor de correo son empresas candidatas a poseer su propio mecanismo de seguridad. El mayor porcentaje de empresas (32%), en las que los usuarios tienen acceso al correo electrónico corresponde a un rango entre 0-10. El mayor porcentaje de empresas (44%), en las que los usuarios reciben diariamente correos electrónicos corresponde a un rango entre 0-10.
- Con respecto a la banca electrónica podemos identificar que la transacción mas utilizada por las empresas es consulta de cuentas en un 32.47%. Esto nos da la pauta para ver que la autenticación y la confidencialidad son importantes para este servicio, y el total de las empresas que utilizan este servicio consideran necesaria la seguridad.

- En cuanto al comercio electrónico, el porcentaje mayor en el ámbito de empresas (10%) que son clientes de comercio electrónico realizan compras diariamente entre 0-10 transacciones. Y el porcentaje mayor en el ámbito de empresas (8%) que proveen comercio electrónico, muestran que diariamente los usuarios realizan entre 0 - 10 transacciones; Esto nos indica que también son empresas que deben poseer seguridad, además todas las empresas que utilizan comercio electrónico consideran que es necesaria la seguridad en este servicio.
- Se pudo observar que el mecanismo de seguridad mas utilizado por las empresas es el cifrado de datos en un 28.57% y un 23.38% el certificado digital. Del total de mecanismos de seguridad que son utilizados se puede observar que han adquirido su certificado digital a través de una AC extranjera un 21.43%, el 17.14% de un AC regional, y el 7.14% un certificado digital autofirmado y el resto desconoce. Con relación al ámbito de las empresas un 35% posee algún mecanismo de seguridad y el mayor porcentaje de 37.66% considera la inversión de la seguridad como media mientras que solo el 14.29% considera que la inversión en la seguridad debe ser muy alta.
- Con respecto a las preguntas dirigidas a la persona que respondió la encuesta se pudo determinar que solo el 42.86% conoce sobre los métodos criptográficos que utiliza el mecanismo de seguridad de su empresa y un 15.58% sabe algo de lo que es la computación cuántica. Un 46.76% considera que si la seguridad fuera rota en su empresa les afectaría en gran escala lo que representa la confidencialidad en un 35.06%, 20.78% la autenticación y un 22.08% la integridad de la información.

Comentario [CL5]: Contexto

4.5 VALIDACIÓN DE RESULTADOS

En la mayoría de los casos carece de interés calcular el tiempo de ejecución concreto de un algoritmo en una computadora, e incluso algunas veces simplemente resulta imposible. En su lugar emplearemos una notación de tipo asintótico, que nos permitirá acotar dicha magnitud. Normalmente consideraremos el tiempo de ejecución del algoritmo como una función $f(n)$ del tamaño n de la entrada. Por lo tanto f estará definida para los números naturales y devolver valores en \mathbb{R}^+ .

Diremos que un algoritmo es polinomial si su peor caso de ejecución es de orden $O(n^k)$, donde n es el tamaño de la entrada y k es una constante. Adicionalmente, cualquier algoritmo que no pueda ser acotado por una función polinomial, se conoce como exponencial. En general, los algoritmos polinomiales se consideran eficientes, mientras que los exponenciales se consideran ineficientes.

Un algoritmo se denomina subexponencial si en el peor de los casos, la función de ejecución es de la forma $e^{o(n)}$, donde n es el tamaño de la entrada. Son asintóticamente más rápidos que los exponenciales puros, pero más lentos que los polinomiales.

Como podemos observar mediante el criptoanálisis realizado se demuestra que la conjetura en la cual se encuentran basados algunos algoritmos asimétricos (como es el caso de RSA que es uno de los más usados hoy en día) que es la factorización de enteros grandes (200 a 300 dígitos) en una computadora clásica requiere tiempo súper-polinomial, es decir que hasta la fecha el algoritmo clásico más eficiente conocido es el tamiz teórico del número el cual factoriza un entero en un tiempo de $O(e^{[(\log N)^{1/3} (\log \log N)^{2/3}]})$ siendo N el número de dígitos. El algoritmo de Shor toma asintóticamente $O((\log N)^2 (\log \log N) (\log \log \log N))$ en una computadora cuántica.

Por ejemplo multiplicar 1234 por 3433 es fácil de resolver, pero calcular los factores de 4236322 no es fácil. La dificultad de factorizar un número crece rápidamente con dígitos adicionales. Tomó 8 meses y 1600 usuarios de Internet obtener RSA 129 (un número con 129 dígitos). Tomaría más que la edad del universo calcular RSA¹⁸ 140. De cualquier modo que, usando una computadora cuántica, que corre el algoritmo de Shor, el número de dígitos en la llave tiene efecto pequeño en la dificultad del problema. Obtener RSA 140 tomaría segundos.

¹⁸ Dato tomado de <http://www.rsasecurity.com>

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1 La computación cuántica parece ser por el momento la opción más viable para el futuro de la computación ya que esta basa sus principios en la Mecánica Cuántica, es decir en la representación de la información por medio de partículas subatómicas permitiendo de esta forma:

- i. La miniaturización de los componentes lo cual ha sido una de las grandes barreras a las cuales se a enfrentado la computación actual.
- ii. Procesamiento paralelo masivo sin necesidad de tener arreglos de procesadores o computadores. Esto permite poder realizar más procesos en menos tiempo o disminuir el tiempo de un proceso. Actualmente en una computadora clásica el procesamiento en paralelo consiste en repartirse los procesos, mientras que en una posible computadora cuántica consiste en la utilización de la superposición (múltiples estados a la vez) y el enredo (entanglement).
- iii. Rapidez en las comunicaciones o transacciones de información, puesto que ya no se trabajaría con pulsos eléctricos pues las computadoras cuánticas utilizan fotones (haz de luz) tanto interna como externamente.

Al mismo tiempo se reconoce que el desarrollo de esta tecnología se encuentra aun distante, ya que existen ciertas barreras que aun no han podido ser superadas siendo por el momento la más importante la imposibilidad de leer toda esa información sin desestabilizar el sistema llamada incoherencia computacional.

2 Se determinó que el algoritmo de Shor romperá los sistemas criptográficos que existen si se logra desarrollar la computación cuántica, ya que los sistemas criptográficos actuales más utilizados se encuentran basados en

el problema de la factorización de números primos grandes (200 a 300 dígitos), lo cual en una computadora actual (clásica) es prácticamente imposible de realizar, pero en una computadora cuántica utilizando el algoritmo de Shor como se explicó anteriormente es una tarea sencilla.

- 3 Se realizó la investigación de los diferentes algoritmos asimétricos de cifrado, estudiando sus principios y fundamentos, desde las bases matemáticas que engloba cada algoritmo, diferenciando los problemas en que esta basado cada uno; por lo que se pudo determinar que el algoritmo RSA presenta el problema de la factorización de números grandes, siendo que por este problema posiblemente sea afectado con la computación cuántica. Además el algoritmo RSA, es el que más esta siendo utilizado porque se encuentra en diferentes productos comerciales de software como Apple, Microsoft, Novell; por lo que es él mas conocido, tomando en cuenta que forma parte de diferentes estándares en el ámbito mundial. Esta investigación sirvió para completar la parte de la hipótesis de trabajo planteada, ya que fue establecida como variable dependiente porque se iba a determinar en cual algoritmo asimétrico de cifrado afectaría el desarrollo de la computación cuántica, sobre la base de las teorías establecidas.
- 4 En cuanto a los métodos de encriptamiento utilizados por las empresas de El Salvador se encuentra determinado por el uso de certificados digitales, y es este el que determina el tipo de encriptamiento que se utiliza. Los certificados utilizados por las entidades certificadoras y autofirmados actualmente utilizan RSA, dado que este es un estándar actual adoptado por el SSL e incluido en la mayoría de sistemas operativos tales como Apple, Microsoft, Novell, Sun.

- 5 Según el análisis realizado a las empresas en el Salvador, se concluyó que los métodos de encriptamiento utilizados en ella, están basados en los algoritmos RSA, determinando así que los mecanismos de seguridad de las empresas son los certificados digitales, firma electrónica y cifrado de datos. Si la computación cuántica se desarrollara en su totalidad en este momento, haría uso del algoritmo de Shor y este podría romper todos los métodos de seguridad que las empresas manejan, provocando en ellas un conflicto total, ya que aquellas empresas que poseen servicios de Internet que obligatoriamente necesitan de seguridad serían rotas, provocando así una crisis en dichas empresas, afectando la Confidencialidad, la Autenticación, y hasta la Integridad de los datos.
- 6 Este documento si puede servir como base para que los informáticos encargados de administrar las operaciones que realizan en su empresa utilizando algún tipo de seguridad, conozcan el funcionamiento y los principios de los algoritmos de cifrado asimétrico que utilizan los mecanismos de seguridad, su implementación, sus usos; así como también conozcan lo que es la computación cuántica, los avances que va teniendo cada día, y por ende el algoritmo de Shor; ya que en algún momento podría afectar en su empresa y más aún para las empresas que quieran dar un servicio seguro a sus clientes a través de un servidor web seguro por el www. También sirve de base para que este tema innovador de lo que es la Computación Cuántica sea conocido por aquellas personas que pertenecen o no pertenecen al área de informática, como alumnos, docentes y que sirva de inicio para llevar el seguimiento de los avances que va teniendo cada día.

7 Conclusión general

El análisis de los avances de la computación cuántica conocidos hasta la fecha nos permiten determinar que si se logrará desarrollar la computadora cuántica los sistemas criptográficos actuales como RSA quedarán obsoletos. Por tanto afectará a las empresas que utilizan criptografía en El Salvador, aunque su impacto no tenga mucha relevancia, ya que en nuestro país el desarrollo o utilización de sitios seguros no es muy alto, actualmente un 93.51% de las empresas encuestadas de El Salvador cuentan con un sitio web, el 35% de estas utilizan criptografía, siendo alrededor de un 17% las que utilizan certificados extranjeros, 13% certificados nacionales y 5% certificados autofirmados, dependiendo estos del tipo de operaciones que las empresas realizan en sus sitios web, como es el caso del 17% son proveedores de banca electrónica o comercio electrónico, el 13% empresas relacionadas con el sistema aduanero y el 5% son intranets o sistemas en línea propios de cada empresa. Lo cual nos indica que la repercusión del desarrollo de la computación cuántica afectará en con mayor medida al sector bancario y de comercio.

8 Otras conclusiones:

En relación a los certificados digitales:

Los certificados digitales sirven para garantizar:

1. La identidad del emisor y del receptor de la información (**autenticación** de las partes).
2. Que el mensaje no ha sido manipulado por el camino (**integridad** de la transacción).
3. Que sólo emisor y receptor vean la información (**confidencialidad**).

4. Que una vez aceptada la comunicación, ésta no pueda ser negada de haber sido emitida (**no repudio**).

La confianza en el sistema viene dada por la **confianza y prestigio** que tenga quien garantiza los datos contenidos en el certificado (**Autoridad de Certificación**). Por eso se dice que ejerce de "tercera parte de confianza" (Trusted Third Party o TTP).

En la práctica, mediante un certificado se puede:

1. Asegura la entrada (**autenticación**) a sitios restringidos en la World Wide Web (reemplazando los peligrosos controles de acceso a través de usuario y palabras clave)
2. **Firmar** mensajes asegurando su procedencia y autoría
3. **Cifra** la comunicación de manera que sólo el destinatario pueda verla.

Con relación a los resultados de la encuesta, la observación y las entrevistas:

El desarrollo del comercio electrónico avanza a pasos lentos en nuestro país. Mientras que las naciones desarrolladas crean cada vez más instrumentos que facilitan esa nueva herramienta de hacer negocios, en el país el tema se mira como algo complicado o como un proyecto a largo plazo.

Pese a que ya existen varias empresas salvadoreñas que se anuncian en Internet, que cuentan con páginas electrónicas o incluso otras que efectúan algún tipo de transacción "virtual", el comercio electrónico (e-commerce) todavía está por desarrollar todo su potencial, para el caso según el ámbito de las empresas en nuestro país solamente el 14% son proveedores.

Por el momento, lo que se está efectuando en el país son intercambios electrónicos de datos (EDI, por sus siglas en inglés) que permiten enviar documentos como órdenes de compra, catálogos de productos, facturas, entre otros.

Hace aproximadamente 2 años en nuestro país surge la necesidad de contar con mecanismos de seguridad para proteger la información que viaja por Internet, resultando que DIESCO en conjunto con Certic@mara (parte de la Cámara de Comercio) es la primera Autoridad Certificadora cerrada del país, se dice que es cerrada porque esta a disposición únicamente de la Dirección General de Renta de Aduanas.

Por lo que se observó que en su mayoría las empresas comerciales o financieras que cuentan con mecanismos de seguridad como certificado digital, firma electrónica o cifrado de datos, recurren a autoridades extranjeras para que les proporcionen la seguridad, pues en nuestro país no existe una Autoridad Certificadora abierta.

RECOMENDACIONES

- 1 Permanecer informados de los avances del desarrollo de la computación cuántica, a pesar que se dice que falta mucho para su desarrollo, este puede ser impredecible.
- 2 Al igual que la recomendación anterior el algoritmo de Shor depende totalmente del desarrollo de la computación cuántica, lo que sí se asegura es que a través de su funcionamiento romperá los métodos criptográficos actuales; ya que estos se encuentran basados en el tiempo de procesamiento de la factorización, lo cual sería una tarea fácil para el algoritmo de Shor, si este se aplicara. También se recomienda el estar al tanto de los avances de los sistemas criptográficos cuánticos¹⁹ y del hardware que utilizará la computadora cuántica, los cuales están siendo desarrollados y ya no se basan en el tiempo de procesamiento.
- 3 Es importante la investigación y el conocimiento del tema expuesto en este documento, porque está relacionado con algo muy delicado que es la seguridad en el intercambio electrónico de datos, y en el envío de información; por lo que nosotros recomendamos que los encargados de administrar la seguridad, los encargados de informática y en general los informáticos tengan siempre algún conocimiento con este tipo de información, especialmente los que están relacionados directamente con empresas de El Salvador que debe proporcionar algún tipo de seguridad al tener presencia en Internet.
- 4 A las empresas que brinden algún tipo de servicio que esté relacionado con envío de información, o intercambio electrónico de datos se les

¹⁹ Ver ANEXO 5

recomienda que utilicen algún mecanismo de seguridad como Certificado Digital (siendo una implementación del algoritmo asimétrico de cifrado RSA), para que sus usuarios confíen plenamente en ellos al realizar alguna transacción.

- 5 Sería bueno que todas aquellas empresas que manejan métodos de encriptamiento dieran el conocimiento necesario a los empleados que estarán a cargo de los departamentos de informática, con el fin de que estos sepan como se desarrolla la seguridad en la empresa, además de saber que mecanismos de seguridad están utilizando dentro de ella.
- 6 En este momento no se ha desarrollado la computación cuántica y aun se están haciendo pruebas con el uso del algoritmo de Shor, se le recomendaría a la empresa, conocer acerca de que métodos de seguridad existen en sus empresas, para que estén alerta de cualquier anomalía que pueda pasar en el manejo de sus datos y evitar así que su seguridad sea rota en algún momento.
- 7 Que todos aquellos que estén interesados en el tema expuesto en este documento, no se queden con las bases de esta investigación, sino, que sigan investigando los avances que cada día van apareciendo en el medio con relación a éste tema, porque solo así podremos llegar a estar seguros de que en el futuro como suponen los expertos, pueda existir un cambio radical llegando a lo que es la Criptografía Cuántica.

8 Otras recomendaciones:

Recomendaciones para el uso de certificados digitales:

Tipo de Certificado

Para decidir el tipo de Certificado a utilizar en su servidor web seguro, debe tomar en cuenta los siguientes aspectos y considerar la opción que mejor se adapte a sus necesidades:

Un certificado firmado por una CA proporciona dos importantes capacidades para su servidor:

- 1- Los navegadores (normalmente) reconocen automáticamente el certificado y permiten establecer la conexión segura sin preguntar al usuario.
 - 2- Cuando una CA emite un certificado firmado, ellos garantizan la identidad de la organización que está proporcionando las páginas web al navegador.
- Un certificado de una CA con buena reputación garantiza que un sitio web está asociado a una compañía u organización particular.
 - Si su servidor seguro está siendo accedido por todo el mundo, necesitará un certificado firmado por una CA, así la gente que acceda a su sitio web sabrá que dicho sitio es propiedad de la organización que proclama ser la dueña. Antes de firmar un certificado, una CA verifica que la organización peticionaria de dicho certificado es realmente quien proclama ser.
 - Puede generar un certificado autofirmado para su servidor seguro, pero tenga claro que dicho certificado no proporciona la misma funcionalidad que

uno firmado por una CA. Un certificado autofirmado no será reconocido automáticamente por los navegadores de los usuarios, además de no proporcionar ninguna garantía concerniente a la identidad de la organización que provee el sitio web. Un certificado firmado por una CA proporciona ambas importantes características a un servidor seguro. Si su servidor seguro será usado en un ambiente de producción, probablemente necesite un certificado firmado por una CA.

- El uso de certificados autofirmados a nuestro criterio puede ser utilizado en sistemas empresariales, en los cuales los usuarios son los mismos empleados de las empresas y por lo general solo es necesario autenticarse, por lo cual no se requiere de una CA que respalde dicho certificado. También pueden ser usados en certificados digitales personales para correo electrónico.
- Es recomendable que una CA emita el Certificado digital cuando vaya a ser utilizado en empresas financieras, comercio electrónico o aduaneras.

Petición del Certificado Digital

Dependiendo del tipo de certificado debe procederse de una u otra forma.

Por ejemplo, en el caso de la petición de certificados personales, la lógica y la operativa apuntan a que la petición sea on-line. Es decir, a la hora de pedir un certificado personal se debe rellenar un cuestionario con nuestros datos personales directamente en la web a una CA y, dependiendo de la clase de certificado, remitir una fotocopia de la documentación a la Autoridad de Certificación o personarnos físicamente en la Autoridad de Registro al efecto.

Comentario [CL6]: lo mismo que el primer comentario

Una vez superados estos trámites la CA firmará el certificado y se lo entregará a su titular.

El caso de la petición postal resulta indicado, por ejemplo, para la petición de Certificados para Servidor. De hecho resulta un sistema mixto, pues como contacto inicial debe enviarse una copia de la CSR por e-mail y después, a través de correo postal, la documentación necesaria (contrato, documentación acreditativa, etc.)

GLOSARIO DE TERMINOS

Términos de Computación cuántica.

Bit: La información esta discretizada en paquetes irreductibles. Su unidad clásica es el *bit* (por *binary digit*), o información almacenable en un sistema clásico con tan solo dos estados 0 y 1. Cada bit puede ser guardado físicamente; en los ordenadores clásicos, un bit se registra como un estado de carga de un condensador (0 = condensador descargado; 1 = condensador cargado). Son estados microscópicamente diferenciados, robustos y estables. Su lectura no les afecta, y pueden ser clonados o replicados sin problemas.

Qubits: La unidad de información cuántica es el *qubit*, o bit cuántico. Es la información almacenable en un sistema cuántico con dos estados: un spin 1/2 , la polarización de un foton, átomos con 2 estados relevantes, etc., son qubits. Aparte de los estados 0 y 1, los qubits poseen otros estados intermedios, que ni son 0 ni 1, sino ambos a la vez, flotando en una neblina entre estos dos valores.

Términos sobre criptografía.

Autenticidad: se refiere a estar seguros de la identidad de una entidad, ya sea mensaje, persona, servidor, etc.

Certificado digital: físicamente es un archivo de hasta 2K de tamaño que contiene principalmente, los datos de una entidad, una persona o un servidor, la clave pública de esa entidad, y la firma de una autoridad certificadora que es reconocida con la capacidad de poder comprobar la identidad de la persona (o servidor) y valida la clave pública que es asociada a la entidad.

Cifrar: es la acción que produce un texto cifrado (ilegible) a partir de un texto original.

Criptografía: es el conjunto de técnicas (entre algoritmos y métodos matemáticos) que resuelven los problemas de autenticidad, privacidad, integridad y no rechazo en la transmisión de la información.

Criptoanálisis es la técnica de descifrar un criptograma sin tener la autorización.

Descifrar: es la acción inversa de cifrar, es decir, convierte un texto cifrado a otro legible (texto original).

Criptografía asimétrica: es el conjunto de métodos que permite establecer comunicación cifrada, donde una de las claves es pública y la otra clave es privada (secreta). Cada usuario tiene un par de claves una pública y otra privada.

Criptografía simétrica: es el conjunto de métodos que permite establecer comunicación cifrada, con la propiedad de que ambos lados de la comunicación tienen la misma clave, y ésta es secreta.

Clave simétrica: es la clave secreta que tienen ambos lados de una comunicación en la criptografía simétrica.

Clave privada: es la clave que se usa en la criptografía asimétrica.

Comercio electrónico: es todo lo relacionado con realizar comercio principalmente por Internet.

Clave pública: es la clave públicamente conocida, que se usa en la criptografía asimétrica.

CSR: Certificate Signing Request. Generación de la petición del Certificado Digital.

DES: Data Encryption Standard.

Diffie – Hellman: Algoritmo asimétrico. Solamente se puede utilizar para intercambiar claves simétricas.

Familia criptográfica: es el conjunto de sistemas criptográficos que basan su seguridad en el mismo problema matemático, actualmente las familias criptográficas más conocidas son las que basan su seguridad en el Problema de factorización Entera (RSA, RW), los que la basan en el problema del logaritmo discreto (DH, DSA), y los que la basan en el problema del logaritmo discreto elíptico (DHE, DSAE).

Firma digital: es un método que usa criptografía asimétrica y permite autenticar una entidad (persona o servidor), tiene una función igual que la firma convencional. Consiste en dos procesos, uno de firma y otro de verificación de la firma. Físicamente es una cadena de caracteres que se adjunta al documento.

Integridad: se refiere a que la información no sea modificada.

No-rechazo: se refiere a no poder negar la autoría de un mensaje o de una transacción.

Privacidad: se refiere a tener control en el acceso de la información y solo permitirlo a personas autorizadas.

Par de claves: se refiere al par de claves una privada y otra pública usadas en la criptografía asimétrica.

PGP: Pretty Good Privacy, protocolo que permite cifrar y firmar mensajes de correo electrónico basándose en un sistema de claves públicas.

RSA: Algoritmo de clave pública creado en 1978 por Rivest, Shamir y Adleman que dan nombre al algoritmo, y es el sistema criptográfico asimétrico más conocido y usado.

Texto original: es un documento antes de ser cifrado.

Texto cifrado: es un documento que ha sido cifrado.

Patentaron el algoritmo y cuando alcanzó popularidad fundaron la empresa RSA Data Security Inc. para la explotación comercial.

Sistema RSA: Se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya se tiene un divisor del número.

Secure Sockets Layer (SSL) Norma emergente sobre la seguridad en la transmisión de documentos en hipertextos a través de Internet utilizando HTTP seguro (HTTPS).

Server Ver *servidor*. Computadora o programa de computación que ejecuta pedidos solicitados desde otra computadora o programa (cliente) que se interconecta directamente con el usuario.

Servidor Ordenador o programa que proporciona un determinado servicio a otro programa denominado cliente y que acostumbra a ejecutarse en otro ordenador. También puede denominarse servidor a un ordenador que ejecute uno o más programas servidores. Por ejemplo, un Web Server en Internet es una computadora que contiene páginas de la Red, las cuales pueden ser examinadas por los usuarios utilizando un programa diseñado especialmente para ese fin, como el Netscape o Internet Explorer.

Session key Código secreto utilizado por el Secure Secret Layer para cifrar los datos transmitidos a través de una conexión segura.

S-MIME Abreviatura de Secure/MIME, una nueva versión del protocolo MIME que soporta codificación de mensajes. Está basado en una tecnología que usa una llave pública para interpretar el mensaje. Se espera que S/MIME sea usado ampliamente, lo cual permitirá que la gente envíe mensajes seguros a través

del correo electrónico, aunque ambos usuarios estén utilizando diferente programa de e-mail.

Vocabulario matemático utilizado en criptografía.

Algoritmo: es un conjunto de reglas que permiten obtener un resultado determinado a partir de ciertas reglas definidas. Otra definición sería, algoritmo es una secuencia finita de instrucciones, cada una de las cuales tiene un significado preciso y puede ejecutarse con una cantidad finita de esfuerzo en un tiempo finito. Ha de tener las siguientes características: legible, correcto, modular, eficiente, estructurado, no ambiguo y a ser posible se ha de desarrollar en el menor tiempo posible.

Función Hash: Una función 'hash' es una función múltiple que asigna su entrada a un valor dentro de un grupo finito. Por regla general este grupo es un rango de números naturales. Un modelo simple de función 'hash' es $f(x) = 0$ para todo entero x . Una función hash más interesante es $f(x) = x \bmod 37$, que asigna x al resto de la división x entre 37.

Generador probabilístico de números primos: es un proceso que tiene como entrada un número entero y como salida un probable número primo con gran grado de aceptación.

Método de factorización: es un método que tiene como entrada un número compuesto (no primo) y como salida uno de sus factores no triviales (diferentes a 1 y al mismo).

Números "Grandes": se considera que un número es grande si tiene longitud al menos de 512 bits (155 dígitos).

Número primo: es un número entero que no tiene divisores diferentes a 1 y así mismo, ejemplo 2,3,5,7,11,...

Primo industrial: es un número primo generado probabilísticamente que tiene a lo más $1/(2^{100})$ de probabilidad de error (de no ser número primo).

Problema de factorización: es el problema inverso a la multiplicación, es decir, el problema de encontrar los factores conocido el producto. En criptografía los números a factorizar son los productos de dos números primos de la misma longitud, el producto tiene al menos 768 bits. Actualmente se han podido factorizar números de hasta 5125 bits (155 dígitos) producto de dos primos del mismo tamaño (256 bits).

Problema del logaritmo discreto: es el problema de encontrar el número de veces que hay que multiplicar un número conocido para obtener como resultado, otro también conocido, por ejemplo dado 1024 y el 2, ¿cuántas veces hay que multiplicar el 2 para obtener 1024? La respuesta es 10 y se dice que 10 es el logaritmo de 1024 base 2.

Problema del Logaritmo Discreto Elíptico: en este caso el problema es encontrar cuantas veces hay que sumar un punto racional para obtener otro conocido. Dado P y Q encontrar x tal que $xP = Q$.

BIBLIOGRAFÍA

Referencias de Internet.

Computación Cuántica

<http://www.albanet.com.mx/articulos/>

http://www.qubit.org/oldsite/Intros_Tuts.html/

Factorización de grandes números

<http://www.albanet.com.mx/articulos/concuant.htm>

Criptografía Asimétrica, Sistema RSA

http://www.htmlweb.net/seguridad/cripto_p/cripto_princ_4.html

Modulo de Perl Quantum::Entanglement

<http://www.cpan.org/>

Algoritmos Cuánticos

<http://uk.arXiv.org>

SSL

<http://www.apache.org>

<http://www.openssl.org>

<http://www.modssl.org>

<http://www.verisign.com>

<http://www.belsign.be>

<http://www.ips.es>

<http://www.entrust.com/>

<http://www.diescoean.com.sv/certicamara/seguridata/index.html>

Libros

- Manuel José Lucena López
Criptografía y Seguridad en Computadores
Tercera Edición. Versión 1.14 Marzo 2002

- Bruce Schneier

Applied Cryptography,

Second Edition: Protocols, Algorithms, and Source Code in C, 01/01/96

- AGUIRRE, Jorge Ramiro.

Curso Seguridad Informática y Criptografía.

Universidad Politécnica de Madrid. 3ª Edición

Publicaciones

- arXiv:quant-ph/9906059 v1 16 Jun 1999

Implementation of the Quantum Fourier Transform

Yaakov S. Weinstein*, Seth Lloyd**, David G. Cory***

* d'Albeloff Laboratory for Information Systems and Technology Department
of Mechanical Engineering, M.I.T., Cambridge, MA 02139

** Department of Nuclear Engineering, M.I.T Cambridge, MA 02139

*** Author to whom correspondence should be addressed

December 4, 2001

- arXiv:quant-ph/0010034 v1 9 Oct 2000

Shor's Quantum Factoring Algorithm

Versión 1.1

Samuel J. Lomonaco, JR.

- [ArXiv:quant-ph/9707033](https://arxiv.org/abs/quant-ph/9707033) v1 17 Jul 1997

Quantum Algorithms and the Fourier Transform

Richard Jozsa; School of Mathematics and Statistics; University of Plymouth; Plymouth, Devon PL4 8AA, England.

ANEXOS

ANEXO 1.

EL PRINCIPIO DE INCERTIDUMBRE DE HEISENBERG

Elaborada en 1927 por Werner Heisenberg, esta ley establece que existen situaciones en el mundo subatómico en las que no es posible conocer al mismo tiempo los valores de dos magnitudes diferentes de una partícula elemental, ya que el hecho de medir la primera interfiere con nuestra capacidad de medir la segunda.

Biografía de Werner Karl Heisenberg ²⁰

Heisenberg, Werner Karl (1901-1976), físico y Premio Nóbel alemán, que desarrolló un sistema de mecánica cuántica y cuya indeterminación o principio de incertidumbre ha ejercido una profunda influencia en la física y en la filosofía del siglo XX. Heisenberg nació el 5 de diciembre de 1901 en Wurzburg y estudió en la Universidad de Munich. En 1923 fue ayudante del físico alemán Max Born en la Universidad de Gotinga, y desde 1924 a 1927 obtuvo una beca de la Fundación Rockefeller para trabajar con el físico danés Niels Bohr en la Universidad de Copenhague. En 1927 fue nombrado profesor de física teórica en la Universidad de Leipzig. Después fue profesor en las universidades de Berlín (1941-1945), Gotinga (1946-1958) y Munich (1958-1976). En 1941 ocupó el cargo de director del Instituto Kaiser Wilhelm de Química Física (que en 1946 pasó a llamarse Instituto Max Planck de Física). Estuvo a cargo de la investigación científica del proyecto de la bomba atómica alemana durante la II Guerra Mundial. Bajo su dirección se intentó construir un reactor nuclear en el que la reacción en cadena se llevara a cabo con tanta rapidez que produjera

²⁰ Tomado de:

<http://www.geocities.com/CollegePark/Plaza/4692/heisenberg.html>

una explosión, pero estos intentos no alcanzaron éxito. Estuvo preso en Inglaterra después de la guerra. Heisenberg, uno de los primeros físicos teóricos del mundo, realizó sus aportaciones más importantes en la teoría de la estructura atómica. En 1925 comenzó a desarrollar un sistema de mecánica cuántica, denominado mecánica matricial, en el que la formulación matemática se basaba en las frecuencias y amplitudes de las radiaciones absorbidas y emitidas por el átomo y en los niveles de energía del sistema atómico (véase Teoría cuántica). El principio de incertidumbre desempeñó un importante papel en el desarrollo de la mecánica cuántica y en el progreso del pensamiento filosófico moderno. En 1932, Heisenberg fue galardonado con el Premio Nóbel de Física.

ANEXO 2.

DIFFIE-HELLMAN

Este algoritmo de encriptación de Whitfield Diffie y Martin Hellman supuso una verdadera revolución en el campo de la criptografía, ya que fue el punto de partida para los sistemas asimétricos, basados en dos claves diferentes, la pública y la privada. Vio la luz en 1976, surgiendo como ilustración del artículo "New directions in Cryptography".

Su importancia se debe sobre todo al hecho de ser el inicio de los sistemas asimétricos, ya que en la práctica sólo es válido para el intercambio de claves simétricas, y con esta funcionalidad es muy usado en los diferentes sistemas seguros implementados en Internet, como SSL (Secure Socket Layer) y VPN (Virtual Private Network).

ANEXO 3.

PRESENTACIÓN DE ENCUESTA.

Reciba un cordial saludo, somos estudiantes en proceso de graduación de la Universidad Don Bosco, y estamos realizando una investigación referente al tema "INVESTIGACIÓN DE LA CONSECUENCIA DEL DESARROLLO DE LA COMPUTACION CUANTICA EN LOS SISTEMAS DE SEGURIDAD QUE USAN CRIPTOGRAFÍA ASIMÉTRICA EN EL SALVADOR", para lo cual solicitamos su valiosa colaboración y agradecemos de antemano su participación por darnos su opinión con respecto al siguiente cuestionario. Aclaremos que no se va a divulgar la información si así lo solicita la empresa, solo será tabulada y no pondremos en riesgo su seguridad.

Sección 1 - Datos de la Empresa

Nombre de la Empresa:

Persona entrevistada:

Puesto:

Sección 2 - Datos de la Encuesta

Parte 1 – Sobre los servicios de Internet

1. ¿Cuál de los siguientes servicios de Internet utiliza su empresa?

- ☐ Sitio o página en la Web ☐ Correo Electrónico ☐ Banca Electrónica
☐ Comercio electrónico ☐ Otro(especificar)

2. Acerca del sitio web que utiliza su empresa.

A. Tipo de servicio:

- ☐ Paga por un sitio web ☐ Posee su propio servidor web

B. ¿Que operaciones realizan en su sitio web?

- ☐ Solamente como publicidad ☐ Programas en línea ☐ Ambos

C. ¿Considera necesaria la seguridad en este servicio?

- ☐ Sí ☐ No ☐ Le es indiferente

3. Acerca del correo electrónico que utiliza su empresa.

A. ¿Qué tipo de servicio posee?

- ☐ Gratuito ☐ Paga por un servicio ☐ Posee su propio servidor de correo

B. ¿Cuántos usuarios tienen acceso al correo electrónico?

- ☐ 0 - 10 ☐ 11 - 25 ☐ 26 - 100 ☐ más de 100

C. ¿Aproximadamente cuantos correos electrónicos recibe y envía cada usuario diariamente?

☐ 0 - 10 ☐ 11 - 25 ☐ 26 - 100 ☐ más de 100

D. ¿Considera necesaria la seguridad en este servicio?

☐ Sí ☐ No ☐ Le es indiferente

4. Acerca de la Banca Electrónica.

A. Si su empresa utiliza Banca Electrónica. ¿Cuáles de las siguientes transacciones realiza?

☐ Pago de planilla ☐ Pago a proveedores ☐ Recepción de pagos de clientes
☐ Pago de servicios ☐ Consulta de cuentas ☐ Transferencia de fondos
☐ Otros(especifique) _____

B. ¿Considera necesaria la seguridad en este servicio?

☐ Sí ☐ No ☐ Le es indiferente

5. Acerca del Comercio Electrónico.

A. ¿Si su empresa utiliza compras a través de Internet, cuantas realiza diariamente?

☐ 0 - 10 ☐ 11 - 25 ☐ 26 - 100 ☐ más de 100

B. ¿ Su empresa es proveedor de comercio electrónico?

☐ Si ☐ No

C. ¿ Si su empresa realiza compras a través de Internet, cuantas realiza diariamente?

☐ 0 - 25 ☐ 26 - 100 ☐ 100 - 500 ☐ más de 500

D. ¿Si su empresa es proveedor de Comercio Electrónico, cual es el promedio de transacciones de compra que los usuarios realizan diariamente?

☐ 0 - 25 ☐ 26 - 100 ☐ 100 - 500 ☐ más de 500

E. ¿Considera necesaria la seguridad en este servicio?

☐ Sí ☐ No ☐ Le es indiferente

Parte 2 – Sobre la seguridad en los servicios de Internet que utiliza su empresa.

6. ¿Qué mecanismo de seguridad utiliza?

☐ Certificados digitales ☐ Firma electrónica ☐ Cifrado de datos ☐ VPN's ☐ Ninguno

7. ¿Quién autoriza o provee la seguridad?

☐ Autoridad Certificadora Regional (Ej. DIESCO) ☐ Autoridad Certificadora extranjera (especifique)_____ ☐ Otros (Especifique)_____

8. ¿Cómo considera la inversión de la seguridad?

☐ Baja ☐ Media ☐ Alta ☐ Muy alta

Parte 3 - Preguntas dirigidas a usted como administrador de la informática, desarrollador, o encargado de la informática de su empresa.

9. ¿Tiene conocimiento de los métodos criptográficos que utiliza el mecanismo de seguridad de su empresa?

☐ Sí ☐ No

10. ¿Tiene conocimiento de lo que es la Computación Cuántica?

☐ Sí ☐ No

11. ¿Cree que le afectaría mucho a su empresa si la seguridad actual fuera rota fácilmente y como les afectaría?

☐ Sí ☐ No

Si su respuesta fue si, en cual de estas opciones le afectaría:

☐ Confidencialidad ☐ Autenticación ☐ Integridad de la información ☐ Otros _____

ANEXO 4.



DIESCO EAN
EL SALVADOR



Requisitos para Solicitar Certificados Digitales y Firma Electrónica

Requisito para Persona Natural

- a) Fotocopia de NIT y de la Cédula de Identidad Personal por ambos lados.
- b) Copia de acuerdo de autorización (actualizado) por Ministerio de Hacienda/Aduana para realizar trámites con dicha dependencia y copia de la Autorización de Aceptación de la Fianza por el Ministerio de Hacienda.
- c) Referencias Bancarias (Estado de Situación)
- d) Constancia de trabajo.

Requisitos para Persona Jurídica

- a) Fotocopia de la cédula de identidad, NIT de los representantes legales.
 - b) Fotocopia de constitución de la empresa
 - c) Copia de las seis últimas declaraciones de IV A.
 - e) Copia de acuerdo de autorización por Ministerio de Hacienda / Aduana para realizar trámites con dicha dependencia (autorización de tramitador) y Copia de autorización de la Fianza por parte de dicha Dependencia.
- I. Si la persona jurídica correspondiese a una **Sociedad Anónima**, se requerirán fotocopias autorizadas de la escritura de la sociedad y del acta de directorio en que se nombran a los apoderados, con una vigencia de 90 días.
 - II. Si la persona jurídica fuese una **Sociedad de Responsabilidad Limitada** se solicitará copia de la escritura de constitución y fotocopia de la copia de la inscripción del extracto de la escritura constitución de la sociedad en el Registro de Comercio on una vigencia de 90 días.
 - III. En el caso que las personas naturales o los representantes de las personas jurídicas sean **ciudadanos extranjeros**, se les requerirá la copia de Pasaporte y/o cédula de identidad extranjera vigente y la acreditación de la calidad actual en El Salvador -visa temporal, residencia definitiva, etcétera.

* **DUI**



Prácticas de Certificación Digital.

**Cámara de Comercio e Industria de El
Salvador a través de
DIESCO EAN EL SALVADOR**



DIESCO EAN 
EL SALVADOR

Versión 1.0
Noviembre / 2002.

Antecedentes

El contenido de las de Prácticas de Certificación Digital constituye los términos y condiciones que rigen la prestación de los Servicios de Certificación Digital Cerrada ofrecidos por CERTI-C@MARA por sí misma o en el contexto del Sistema de Teledespacho por Internet. Incluyendo la emisión, administración, almacenamiento y revocación de los Certificados Digitales que ésta emite. En dichas Prácticas se encuentra incorporada por referencia en cada uno de esos certificados digitales.

Estas Prácticas han sido elaboradas en el contexto de la declaración de prácticas de certificación a que se refiere el proyecto de régimen uniforme para las firmas digitales, en correlación con la ley modelo sobre comercio electrónico, elaborados por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) y su finalidad es constituirse en el mecanismo formal de difusión y comunicación, para con los titulares de un certificado digital emitido por CERTI-C@MARA, así como para con cualquier persona que pretenda usar y/o confiar en dichos certificados.

Cualquier usuario (personas física o jurídica) que desee hacer uso de los servicios de certificación digital o pretenda utilizar o confiar en los certificados digitales emitidos por CERTI-C@MARA, deberá reconocer y aceptar las políticas y procedimientos establecidos en la presente Declaración de Prácticas de Certificación Digital. La sola utilización de dichos servicios o certificados constituye por sí misma manifestación expresa de aceptación y sujeción a la presente.

Ámbito de Aplicación

CERTI-C@MARA es una Autoridad Certificadora/Registradora Cerrada, es de carácter privado y los certificados emitidos son utilizados para el Sistema de Teledespacho por Internet y ha sido creada para la emisión de certificados personales o jurídicas.

La finalidad de los servicios de certificación digital ofrecidos por CERTI-C@MARA, es crear un marco razonable de seguridad jurídica y tecnológica, en el que CERTI- C@MARA, se constituye en un tercero confiable para las partes involucradas en una transacción electrónica con la Aduana.

Servicios

Los Servicios de Certificación Digital que serán prestados por CERTI-C@MARA comprenderán entre otros, los siguientes:

- A. Emisión de Certificados: personales ó Personas Jurídicas

- B. Revocación de Certificados: para efecto de dar por terminada anticipadamente la vigencia de un certificado, ya sea por voluntad de su titular o porque concurrieron una o más de las causales descritas en la sección correspondiente de este documento.
- C. Publicación de Certificados: una vez que el certificado digital haya sido emitido, éste será publicado en un directorio bajo las especificaciones X.509, u otra bajo cualquier otra especificación, de manera que terceros interesados puedan tener acceso a él.
- D. Almacenamiento de Certificados: los certificados digitales emitidos y la lista de de certificados revocados (CRL's), son almacenados por un período determinado de tiempo debido a que el documento firmado digitalmente, por sí mismo, puede poseer un período de validez o vigencia más amplio que el del certificado utilizado para firmar.

Tipos de Certificados

Por sí misma como Autoridad Certificadora, CERTI-C@MARA podrá emitir la siguiente clase de Certificados Personales ó Jurídicas

- A. Certificados Nivel 0: son certificados personales para efectos de PRUEBAS, no tienen valor legal alguno, son emitidos con el único fin de facilitar las pruebas de transmisión de información entre partes que utilizan Internet y desean un entorno más seguro en el envío y recepción de mensajes.

Por su propia naturaleza, al no ser necesaria la presencia física del solicitante, generalmente se emiten, suspenden, revocan o renuevan en línea y con respecto a ellos CERTI-C@MARA no reconoce responsabilidad alguna de ninguna naturaleza.

- B. Certificados Nivel 1: son certificados personales para E-MAIL, su valor legal deriva del contrato entre las partes y se emiten por instrucción o bajo la responsabilidad de la entidad interesada.
Son emitidos con el único fin de facilitar la transmisión de información entre partes que utilizan Internet y desean un entorno más seguro en el envío y recepción de mensajes, básicamente por medio de correo electrónico. la seguridad que proporcionan sólo está referida a la confirmación del nombre de una persona y la dirección de correo electrónico con la que esa persona ha sido vinculada. Ambos elementos constituyen el único objeto de validación que CERTI-C@MARA les reconoce.

- C. Certificados Nivel 2: son certificados personales, su valor legal deriva del contrato entre las partes y se emiten por instrucción o bajo la responsabilidad de la entidad interesada para entornos APLICATIVOS. Al surgir de un proceso de identificación realizado por la entidad solicitante a la que pertenece el titular del certificado, sólo poseen la propiedad de autenticar la identidad y facultades de un sujeto determinado en términos de su pertenencia a dicha entidad.
- E. Certificados Nivel 3: son certificados personales o Jurídicos, con valor legal pleno. Son emitidos en un entorno más seguro y revestido de ciertos formalismos no sólo respecto de la identificación del solicitante del certificado, sino incluso respecto del proceso de emisión, ya que para ello resulta indispensable la comparecencia personal (física) del titular ante el Agente Certificador. Estas formalidades, realizadas en el contexto del marco jurídico existente proporcionan una mayor seguridad en las transacciones de comercio electrónico y garantizan al mismo tiempo la posibilidad de exigir su cumplimiento mediante los procedimientos jurisdiccionales tradicionales.

Tecnología Utilizada

los certificados emitidos en el ámbito de Teledespacho por Internet están basados en los sistemas de criptografía de clave pública de RSA y cumplen con los estándares definidos para la versión 3 001 formato X.509.

la tecnología aplicada en los productos utilizados por CERTI-C@MARA ha sido desarrollada por su socio tecnológico SeguriDATA y han sido creados utilizando el más alto nivel de criptografía, siguiendo el modelo de criptografía de clave pública más reconocido y utilizado a nivel internacional (RSA) y de acuerdo a los estándares emergentes. los productos no violan ningún derecho de gobierno o compañías extranjeras, así como tampoco están sujetos a sus restricciones.

De esta forma, CERTI-C@MARA puede ofrecer el más alto nivel de seguridad (claves RSA de hasta 2048 bits de extensión y claves simétricas de 128 bits de longitud) .

Las claves privadas de las Autoridades Certificadoras de CERTI-C@MARA han sido generadas y almacenadas en dispositivos de seguridad que cumplen con las especificaciones internacionales FIPS 140-1 en cuanto a su nivel de seguridad.

Procedimientos de Certificación

Todo servicio y/o proceso de certificación digital ofrecido por CERTI-C@MARA está sujeto y regulado además por la celebración de un convenio expreso entre CERTI-C@MARA y sus clientes.

Generación de Claves

La generación de las claves pública y privada necesarias para la emisión de un certificado digital deberá realizarse bajo el absoluto control de quien será el titular de dicho certificado y será exclusiva responsabilidad de éste el tomar las medidas de seguridad que considere necesarias para el resguardo de la clave privada y la contraseña de acceso a ésta.

Tratándose de certificados personales ó de personas Jurídicas, la generación de dichas claves podrá realizarse a través del sitio Web de ésta (www.diescoean.com.sv), Ó si el usuario lo requiere podrá solicitar a Certi-C@mara que le genere dichas claves (es opcional), pero bajo la estricta responsabilidad del usuario.

Requerimiento de Certificación

Sea que se trate de certificados personales o de personas Jurídicas, en ambos casos el proceso de certificación sólo puede ser iniciado con la presentación del requerimiento de certificación, tanto en su forma escrita como en su forma electrónica, ante la entidad solicitante si se trata de certificados digitales niveles 1 y 2, 3.

En dicho requerimiento, el usuario deberá proporcionar todos y cada uno de los datos que ahí se le solicitan sin omisiones. La falta de requerimiento o la omisión de alguno de los datos solicitados dará lugar a la negación de los servicios de certificación.

Emisión de Certificados

Cumplidos los requisitos para la obtención de los certificados digitales, CERTI-C@MARA, procederá a emitirlos y en su caso a ponerlos a disposición de su titular en el sitio Web, previa notificación que se haga a éste por medio de correo electrónico.

El proceso de solicitud de un certificado digital puede iniciarse a través del sitio Web de CERTI-C@MARA, ó el usuario puede presentarse a las oficinas de dicha institución a solicitar la emisión de dicho documento electrónico,

pero invariablemente deberá concluirse en los términos indicados en los procesos anteriores.

Registro de Certificados

Independientemente de que los certificados digitales emitidos por CERTI-C@MARA serán incorporados a la Base de Datos administrada por ésta para efectos de la publicación de las Listas de Revocación de Certificados o CRL's (por sus siglas en inglés) y para la prestación de servicios de información el tiempo real sobre el estado de revocación o vigencia de dichos certificados.

Uso y Verificación de Certificados

La tecnología en la cual se sustenta la prestación de los servicios de certificación digital y la emisión, administración, almacenamiento y revocación de los certificados digitales ofrecidos por CERTI-C@MARA, le imprime confidencialidad, autenticidad, integridad y no repudiación de la información enviada o recibida a través de medios electrónicos; sin embargo, es responsabilidad del titular de un certificado su adecuada utilización y los alcances y repercusiones de dicho uso.

Autenticidad

Al transmitir un mensaje electrónico utilizando certificados digitales de CERTI-C@MARA un individuo puede determinar si cierta persona es el autor de tal mensaje o documento electrónico o bien, si reconoce el contenido del mismo.

Para autenticar un mensaje electrónico, un usuario deberá utilizar la clave pública de la persona que firmó digitalmente el mensaje electrónico recibido, si la clave pública corresponde a la clave privada con la cual se firmó, es decir, que el mensaje pueda ser interpretado, esto significa que dicho mensaje fue realmente creado por el titular de dicho certificado o que está reconociendo como propio su contenido.

Confidencialidad

Esta característica de los mensajes electrónicos transmitidos con certificados digitales de CERTI-C@MARA garantiza al usuario que la información enviada electrónicamente sólo podrá ser leída por la o las personas a las cuales va dirigida. Esto se logra porque, al firmar digitalmente un mensaje utilizando además la clave pública del destinatario, éste es protegido (ensobretado) de tal forma que no podrá ser accedido más que por el poseedor de la clave privada vinculada a esa clave pública.

Integridad

Con los certificados digitales de CERTI-C@MARA, también se evita que la información transmitida a través de medios electrónicos sea modificada en el transcurso de su envío y/o recepción, por el nivel de seguridad de la tecnología utilizada por CERTI-C@MARA para la emisión de certificados digitales.

La integridad de los mensajes puede ser verificada revisando que el resumen (digestión) de un mensaje electrónico generado por remitente y adherido al final de dicho mensaje, sea igual al resumen del mensaje electrónico obtenido por el receptor. Este proceso de revisión ofrece la propiedad de determinar que cualquier cambio en el mensaje electrónico resultará forzosamente en un resumen diferente.

No Repudiación

Ya sea por un mecanismo de contratación previo que contempla la aceptación de los certificados digitales de CERTI-C@MARA como medios de identificación electrónica, los titulares de un certificado o los terceros interesados podrán establecer una cadena de confianza para garantizar que ni la parte receptora ni la emisora puedan negar haber realizado la transacción.

CERTI-C@MARA buscará adicionalmente establecer los mecanismos para proporcionar servicios seguridad y confianza (time stamping) sobre la fecha y hora de realización de dichas transacciones.

listas de Revocación

Las Autoridades Certificadoras/Registradoras de CERTI-C@MARA darán publicidad al estatus de revocación de los certificados digitales emitidos por dichas AC's mediante las Listas de Revocación de Certificados que serán puestas a disposición del público en general con una periodicidad de al menos cada 24 horas. No obstante, CERTI-C@MARA se reserva el derecho de llevar a cabo la difusión del estatus de revocación con una periodicidad y por medios distintos a las Listas de Revocación de Certificados (CRL's), si por disposición expresa de la ley, por así solicitarlo una autoridad competente o por solicitud expresa del titular del certificado así resulta conveniente.

Quien desee hacer uso de los servicios de certificación digital o pretenda utilizar o confiar en los certificados digitales emitidos por CERTI-C@MARA, deberá verificar las Listas de Revocación de Certificados.

Suspensión y Revocación de Certificados

No obstante que los certificados digitales son emitidos por regla general por un período determinado, a petición de su titular, de un tercero facultado o de una autoridad competente, éstos pueden ser revocados antes de que dicho

período termine, ya sea por voluntad, por que la clave ha sido revelada o conocida por un tercero no autorizado, por que la clave haya sido revocada o por que simplemente concurren circunstancias que ameriten dicha revocación.

Causas de Suspensión o Revocación

Un certificado digital, puede ser suspendido o revocado a solicitud expresa de su titular o del representante legal de éste, si para ello concurren una o más de las circunstancias que a su criterio ameriten la terminación anticipada de la vigencia de dicho certificado. Tales circunstancias son:

- A. El olvido o extravío de la contraseña de la clave privada.
- B. El robo o extravío de la propia clave privada.
- C. La sospecha de utilización de su clave privada por parte de un tercero.
- D. El cambio de alguno de los datos contenidos en el certificado digital.
- E. La solicitud expresa de alguna autoridad competente.

La suspensión y la revocación son de naturaleza distinta, ambas son definitivas en cuanto a sus efectos y concluyen con la terminación anticipada de la vigencia de un certificado digital; sin embargo, la suspensión es un paso previo, por razones de urgencia, a la revocación.

Solicitud de Suspensión o Revocación

Tratándose de la suspensión o revocación de los certificados digitales niveles 1 y 2, la petición podrá ser realizada y concluida a través del sitio Web de CERTI- C@MARA o por la vía telefónica, a través de su área de atención a clientes, cumpliendo en ambos casos con los requisitos que para validar el proceso se le requieran al solicitante, particularmente en cuanto al conocimiento de la clave de anulación. Sin la satisfacción de dichos requisitos, la solicitud será rechazada.

Para el caso de suspensión o revocación de los certificados digitales nivel 3, el proceso podrá ser iniciado igualmente a través del sitio Web de CERTI- C@MARA o por la vía telefónica, cumpliendo con los requisitos correspondientes; sin embargo, el proceso invariablemente deberá ser concluido de manera presencial ante Certi-C@mara y previa comunicación a La Aduana de El Salvador.

En caso de que la solicitud de suspensión o revocación sea presentada por una autoridad competente, sea que se trate de certificados digitales niveles 1 y 2 o de certificados digitales nivel 3, invariablemente la solicitud deberá ser con la formalidad que caracterice las actuaciones de orden público de dicha autoridad.

Efectos de la Suspensión o Revocación

El efecto inmediato de la suspensión de un certificado digital es la eliminación temporal de su capacidad para la generación legítima de derechos y obligaciones por un término no mayor a 24 horas, concluido dicho período la eliminación de esa capacidad será absoluta.

Los efectos inmediatos de la revocación de un certificado digital son la expiración instantánea de su vigencia y la eliminación absoluta de su capacidad para la generación de legítima de derechos y obligaciones.

En ambos casos, el certificado digital de que se trate pasará a formar parte de la Lista de Revocación de Certificados correspondiente.

Notificación de Suspensión o Revocación

No obstante que quienes deseen hacer uso o pretendan confiar en los certificados digitales emitidos por CERTI-C@MARA deberán verificar, bajo su propio riesgo, el estatus de vigencia, suspensión o revocación de un certificado digital antes de proceder a la realización de una transacción electrónica, CERTI- C@MARA procederá a publicar dicho estatus a través de:

- A. Una lista simple de certificados revocados disponibles a través de un canal seguro en su sitio Web;
- B. Una lista de revocación de certificados (CRL) que será publicada con una periodicidad de al menos 24 horas.
CERTI-C@MARA podrá llevar a cabo la notificación en tiempo real sobre el estatus de suspensión, revocación o vigencia a solicitud expresa de los interesados, mediante la utilización de sus servicios de publicación de certificados.

Expiración y Renovación de Certificados

Por regla general, en concordancia con los estándares internacionales, los certificados digitales emitidos por CERTI-C@MARA tienen una vigencia por un año; sin embargo, la vigencia puede ser menor a petición expresa del solicitante. Nunca se expedirán certificados digitales con vigencia mayor a un año,

Expiración de Certificados

Los Certificados Digitales emitidos por CERTI-C@MARA tienen por regla general una vigencia de un año; sin embargo, a solicitud expresa de su titular podrán ser emitidos por un período de vigencia menor. En cualquier caso, el inicio de vigencia surtirá sus efectos en el momento mismo de su emisión y su

expiración en el día y hora también ahí expresados, considerando para tales efectos el tiempo universal coordinado (UTC).

No obstante la vigencia expresamente definida en los certificados digitales emitidos por CERTI-C@MARA, sus titulares podrán dar por terminados sus efectos por solicitud expresa siguiendo el procedimiento de revocación correspondiente al tipo de certificado de que se trate.

Renovación de Certificados

En concordancia con los estándares internacionales, CERTI-C@MARA podrá renovar los certificados digitales por ella emitidos. Para ello, los titulares de dichos certificados deberán seguir el procedimiento establecido para la emisión original del certificado de que se trate, así como llevar a cabo nuevamente la acreditación de los elementos de identificación necesarios para su emisión.

CERTI-C@MARA hará su mejor esfuerzo para notificar, con un mes de anticipación, a los titulares de un certificado digital por ella emitido sin embargo, será responsabilidad exclusiva de su titular y de quien pretenda utilizar o confiar en dichos certificados la verificación de su estatus de vigencia o revocación.

Almacenamiento y Respaldo de Certificados

La información personal o empresarial obtenida por CERTI-C@MARA en la prestación de sus servicios de certificación digital y en la emisión de certificados digitales, es administrada en los términos que se definen en sus Políticas de Privacidad; sin embargo, los usuarios de los servicios de CERTI-C@MARA o los titulares de un certificado emitido por ésta reconocen y aceptan la necesidad de publicación de los datos inherentes al tipo de certificado que hayan solicitado, para lo cual hacen manifestación expresa en ese sentido.

Período de Almacenamiento y Respaldo

Todos los certificados digitales emitidos por CERTI-C@MARA serán almacenados por un período no menor a 5 años para los certificados nivel 3. En ambos casos dicho período empezará a computarse a partir del momento mismo de su emisión.

No obstante lo anterior, CERTI-C@MARA podrá extender el período de almacenamiento de dichos certificados sin importar su nivel, ya sea por disposición expresa de la ley o por solicitud expresa de su titular.

Procedimiento de Almacenamiento y Respaldo

CERTI-C@MARA llevará a cabo el almacenamiento a que se refiere el punto anterior incluyendo en ello toda la información que resulte aplicable al certificado digital de que se trate, en términos de su emisión, suspensión, revocación o expiración, así como la documentación y las prácticas de

certificación digital que haya regido durante su período de validez. Los registros correspondientes incluirán toda la evidencia relevante y disponible para CERTI-C@MARA relacionada con:

- A. La obtención de certificados por parte de terceros interesados;
- B. El intercambio con otras Autoridades Certificadoras;
- C. La peticiones de revocación o suspensión hechas por una autoridad competente;
- D. La peticiones de revocación o suspensión hechas por un tercero interesado;
- E. Los registros que para efectos de auditoría por disposición legal o por prácticas de la industria se deban conservar.

CERTI-C@MARA hará su mejor esfuerzo para conservar y proteger la integridad de los archivos correspondientes, así como su disponibilidad para su consulta.

Medios de Almacenamiento y Respaldo

La información resultante de la operación normal de CERTI-C@MARA y la proporcionada por los usuarios de los servicios de certificación digital y por los titulares de los certificados digitales emitidos por ésta, será almacenada en los medios que a criterio de CERTI-C@MARA garanticen razonablemente su integridad y disponibilidad para su consulta.

Los respaldos y la protección de esa información se realizarán de conformidad con las políticas y procedimientos que en su momento defina CERTI-C@MARA en documentos complementarios de uso reservado o acceso restringido.

Uso y Publicación de la Base de Datos

La información resultante de la operación normal de CERTI-C@MARA y la proporcionada por los usuarios de los servicios de certificación digital y por los titulares de los certificados digitales emitidos por ésta, no será revelada, compartida, rentada o vendida a terceras personas o empresas, bajo ninguna circunstancia. No obstante lo anterior, CERTI-C@MARA se reserva el derecho de revelar dicha información, sin autorización expresa de su titular, si ésta resulta necesaria para identificarlo, contactarlo o ejercer cualquier acción legal en su contra, por la violación de los términos y condiciones que regulan el uso de tales servicios o certificados. De igual manera, CERTI-C@MARA podrá revelar la información personal, sin necesidad de autorización expresa de su titular, cuando le sea solicitada expresamente por alguna autoridad jurisdiccional o administrativa facultada para exigir dicha revelación.

Controles de Seguridad

En la prestación de sus servicios de certificación digital y en la emisión, administración, almacenamiento y revocación de certificados digitales CERTI-C@MARA ha implementado tecnología, mecanismos y procedimientos de seguridad del más alto nivel, los cuales son revisados y actualizados con cierta regularidad. La seguridad es revisada y evaluada en términos de instalaciones físicas, de telecomunicaciones, de CERTI-C@MARA llevará a cabo una investigación inicial de todo el personal que es candidato para servir en posiciones de confianza, con el fin de proporcionar una seguridad razonable en la determinación de su confiabilidad y competencia. hardware, de software y de personal y de acuerdo a los convenios que tiene con sus prestadores de servicios de outsourcing.

Controles de Seguridad de Personal

CERTI-C@MARA hará su mejor esfuerzo para implementar controles de seguridad y administración del personal que tiene acceso a las operaciones criptográficas, emisión, suspensión, o revocación de los certificados digitales emitidos por ésta, con el fin de proporcionar una seguridad razonable de la confiabilidad y competencia de sus empleados y de la ejecución satisfactoria de sus responsabilidades.

Aceptación de las Prácticas de Certificación Digital

Por el hecho de obtener o tener acceso a dichas Prácticas y/o formularios, convenios o acuerdos de certificación digital, sean de sitio seguro o de identidades digitales, posteriormente firmar dos ejemplares impresos y cancelar las tarifas respectivas, se entiende que el suscriptor o signatario del servicio de certificación digital acepta la totalidad del contenido de las presentes Prácticas y, en particular, que declara expresa y solemnemente cumplir con los requisitos establecidos para la categoría de certificado(s) que solicita.

Garantías y Límite de Responsabilidades

Excepción hecha de lo manifestado expresamente en este documento y en los documentos o contratos complementarios, CERTI-C@MARA no ofrece garantía expresa ni tácita sobre sus servicios de certificación digital o los certificados digitales emitidos por ésta y por lo mismo, no será responsable por los daños o perjuicios que sufran sus usuarios, si éstos derivan de la mala ó indebida utilización de tales servicios o certificados ó por la presentación de documentación falsa por parte del usuario.

Garantías

Las garantías que otorga CERTI-C@MARA con respecto a los certificados digitales emitidos por ella, aplican única y exclusivamente a los usuarios y/o titulares de dichos servicios y certificados, más no a cualquier otro tercero participante, y están definidas en razón del tipo de certificado de que se trate.

- A. Tratándose de los certificados digitales niveles 1 y 2, CERTI-C@MARA no verificará la información suministrada en el requerimiento de certificación por parte de la entidad solicitante o por parte de quien será su titular. Como consecuencia, CERTI-C@MARA no es ni será considerada como responsable de la veracidad de cualquiera de los datos contenidos en dichos certificados y quienes pretendan confiar en los certificados digitales niveles 1 y 2 deberán reconocer que sus titulares y/o la entidad solicitante son responsables por cualquier declaración falsa hecha a CERTI-C@MARA.

En este sentido, CERTI-C@MARA no garantiza bajo ninguna circunstancia la no repudiación de las transacciones realizadas por el titular de un certificado nivel 1 o 2, dado que esa circunstancia queda regida exclusivamente por los términos y condiciones que las partes se hayan expresado mutuamente, ya sea en forma verbal o escrita, así como por las leyes aplicables.

- B. Tratándose de los certificados digitales nivel 3, la verificación de la información suministrada en el requerimiento de certificación por parte de quien será su titular por su representante legal, será realizada previa autorización de la Aduana y presentación de los documentos antes mencionados.

De igual forma la Cámara de Comercio e Industria de El Salvador, ha presentado una fianza de fiel cumplimiento por el servicio de Certificación Electrónica Cerrada a favor del Ministerio de Hacienda.

Responsabilidades

En la prestación de los servicios de certificación digital por parte de CERTI-C@MARA, la responsabilidad estará delimitada por las consecuencias legales y económicas que deriven del cumplimiento o incumplimiento de los requisitos establecidos para los distintos procesos y niveles de certificación.

La definición de dicha responsabilidad deberá partir de la base de considerar el rol que cada parte ejerce en el proceso de certificación, y que tiene como finalidad:

- A. Por parte de los Agentes Certificadores verificar y validar:

- 1) Que un sujeto determinado acredita su identidad y su capacidad legal para obligarse;
- 2) Que un sujeto determinado manifiesta su voluntad de que se le certifique la correspondencia de veracidad entre su identidad y la que dice ser su clave pública.
- 3) Que un sujeto determinado manifiesta expresamente su sujeción a los términos y condiciones contenidos en esta Declaración de Prácticas de Certificación.

B. Para las Autoridades Certificadoras verificar y validar:

- 1) Que un Agente Certificador ha cumplido con todos y cada uno de los requisitos necesarios para ejercer dicha función;
- 2) Que existe correspondencia de veracidad entre la identidad de un Agente Certificador y su clave pública, con respecto a un certificado digital emitido por este.
- 3)

C. Para CERTI-C@MARA verificar y validar que en la operación de los servicios de certificación digital:

- 1) Que ha implementado y aplicado los estándares de seguridad y criptografía necesarios con un nivel razonable de confiabilidad;
- 2) Que los servicios estarán en operación las 24 horas del día, durante los 365 días del año; y
- 3) Que aplicará su mejor esfuerzo para garantizar la permanente actualización de la tecnología utilizada y la consecuente aplicación de los estándares nacionales e internacionales que corresponda

Excluyentes

En la prestación de los servicios de certificación digital por parte de CERTI-C@MARA, por parte de quienes deseen hacer uso de dichos servicios o pretenda utilizar o confiar en los certificados digitales emitidos por aquellos, se reconocen y manifiestan expresamente las siguientes causas excluyentes de responsabilidad:

- A. Ni CERTI-C@MARA, será responsable por los daños o perjuicios de cualquier naturaleza incluyendo, pero sin limitar, pérdida de utilidades, interrupción de operaciones, pérdida de información comercial o cualquier otro daño pecuniario; si éstos derivan de la mala o indebida utilización de los servicios de certificación digital por parte de los usuarios finales; de la mala o incorrecta interpretación, análisis, síntesis o conclusión a que los usuarios finales lleguen en el uso de dichos

servicios; e incluso, si el solicitante de un certificado digital aporta datos o documentos falsos para la obtención de dicho certificado;

- B. Ni CERTI-C@MARA, será responsables por la interrupción o alteración temporal de los servicios de certificación digital por causas ajenas a su voluntad, fuerza mayor y/o casos fortuitos, propiciada por condiciones climatológicas adversas, fallas en la energía eléctrica, fuego, actos vandálicos, huelga o cualquier otro motivo similar que afecte sus instalaciones; así como por la interrupción o alteración temporal de los servicios de certificación digital por causas similares o por errores, omisiones o negligencia que afecten las instalaciones de transmisión, enlace y bases de repetición de los proveedores de telecomunicaciones de CERTI-C@MARA;
- C. Ni CERTI-C@MARA, será responsables de la interrupción temporal del servicio ocasionada por acciones gubernamentales que coarten o restrinjan la libertad en las comunicaciones civiles o que impidan su transmisión privada o incluso, por cualquier otro motivo de naturaleza análoga.

Arbitrajes

Todas y cualquier controversia que se suscite entre Certi-C@mara y los suscriptores ó signatarios que suscriban estas Prácticas de Certificación Digital, las Partes acuerdan que sus representantes comerciales se reunirán para intentar resolver la disputa a través de la negociación. En el evento de que la disputa no sea resuelta por negociación, ésta será sometida a un arbitraje de Derecho en El Salvador. Las reglas del arbitraje serán las del Centro respectivo de la Cámara de Comercio e Industria de El Salvador, o si no existiere, las reglas que contiene el Reglamento UNCITRAL. Ambas partes se someten a dichas reglas. Cada parte nombrará a un árbitro dentro de los diez días de ser requerido el arbitraje por la otra. Si en el plazo expresado, la parte que deba nombrar su árbitro, no lo hace, podrá pedir la otra que lo nombre el Presidente de la Asociación Nacional de la Empresa Privada de El Salvador quien deberá hacerlo dentro de los quince días siguientes a la solicitud de la parte interesada. Los dos árbitros nombrados deberán nombrar al tercer árbitro dentro de los quince días siguientes a la fecha de aceptación de la designación por el último árbitro nombrado por las partes.

Si no se pusieren de acuerdo en dicho nombramiento, dentro del plazo expresado, podrá pedir cualquiera de ellas al Presidente de la Asociación Nacional de la Empresa Privada de El Salvador que lo designe, dentro del plazo de quince días desde la fecha de la solicitud respectiva. Los costos y honorarios razonables relacionados con el procedimiento arbitral serán cubiertos por ambas partes conjuntamente y por montos iguales.

Cada Parte cubrirá el costo de sus propios abogados y expertos, inicialmente, y en el laudo arbitral, el Tribunal determinará la condenación en costas.

Disposiciones Generales

En lo conducente, la presente declaración de prácticas de certificación recogerá o asimilará el marco regulatorio que se haya implementado en el país ó en su defecto la ley de simplificación aduanera y sus reformas.

Propiedad Intelectual

Cualquier otra referencia a nombres y marcas en este documento se hace a título informativo y los derechos de propiedad intelectual corresponden a su titular. Las claves pública y privada son propiedad de su legítimo poseedor o titular en términos del contrato celebrado entre éste y CERTI-C@MARA.

Los certificados contienen material con derechos de autor, marcas, y otra información propietaria. No se permite el copiado, ingeniería inversa, hojeador automatizado o vaciado de computadora, distribución, publicación o explotación comercial del material o información disponible en o por medio de los certificados, excepto como expresamente sea permitido bajo los términos y condiciones de esta Declaración de Prácticas de Certificación.

Glosario de Términos

Para los efectos legales a que haya lugar y para la adecuada interpretación del presente documento, en lo sucesivo deberá entenderse que cada vez que se citen, los siguientes términos significan:

Conceptos claves:

Que es un Certificado Digital?

Documento electrónico que proporciona información de la identidad del titular del certificado, la clave pública (llave) a la cual esta vinculado, la identidad de la Autoridad Certificadora que emite el certificado así como su clave pública con fines de verificar la veracidad del Certificado Digital.

¿Que es el proceso de Certificación Digital?

Proceso de verificación de identidad realizado por una identidad de confianza (tercero confiable) y la cual emite un Certificado Digital a nombre del titular del certificado que quiere hacer uso del proceso de firma electrónica / digital ó la identificación de servidores que consiste en la generación de claves y requerimiento de certificación, identificación del titular del requerimiento, emisión del certificado por un Autoridad Certificadora y registro del certificado.

¿Que es una Autoridad Certificadora?

Entidades encargadas de emitir los certificados digitales de los requerimientos que cumplan a satisfacción con los requisitos para su obtención. Realiza además las funciones de revocación, publicación, almacenamiento y registro de certificados. Se constituye en un tercero confiable para las partes involucradas en una transacción electrónica.

¿Qué es una Firma Electrónica / Digital?

Es un método electrónico de firmar un documento, constituyéndose en un medio seguro de garantizar el autor y emisor del documento.

¿Qué valor tiene la firma Electrónica / digital?

Técnicamente puede demostrarse que ofrece más garantías que la firma real, ya que no puede duplicarse ni puede ser imitada. Pero debido a la calidad del proceso de registro que se siga en cada caso, tiene la calidad que éste le aporte, y la seguridad con la que se han generado las llaves digitales (pública/privada).

¿ Que es Criptografía?

Es la ciencia que utiliza las matemáticas para mantener las comunicaciones privadas y proteger información sensible creando un alto grado de confianza en el mundo electrónico.

¿Que es una llave pública (clave)?

En la criptografía de clave pública, esta clave se hace pública a todo el mundo y es utilizada para descryptar información y verificar firmas digitales.

¿Que es una llave privada (clave)?

Es utilizada para la generación de las firmas electrónicas/digitales y también para encriptar información. Esta clave NUNCA debe de compartirse ni difundir la frase de seguridad que permite el acceso a ella.

¿Que es Encriptar (Encripción)?

La transformación de un texto legible en otro totalmente diferente e inteligible a simple vista por medio de un proceso matemático y el cual sólo pueda ser leído por quien tiene la clave que descrypta el texto.

¿Que es Descryptar (descrpción)?

Proceso de interpretar ó convertir un texto encriptado a su estado original mediante el uso de la clave que descrypta el texto.

Certificados X.509:

Estándar utilizado para guardar la información contenida en los Certificados Digitales, así como a las Firmas Digitales que los protegen.

Criptografía de Clave Pública o Asimétrica:

Es un sistema criptográfico que utiliza dos claves distintas para los procesos de encriptación y desencriptación. Las dos claves son la Clave Pública y la Clave Privada (la cual es conservada en secreto), los datos encriptados con la Clave Pública sólo pueden ser desencriptados con la correspondiente Clave Privada.

Prácticas de Certificación Digital:

Documento que contiene los términos y condiciones que rigen la prestación de los Servicios de Certificación Digital ofrecidos por la Autoridad Certificadora.

Digestión:

Método para reducir un mensaje de cualquier longitud a una longitud fija llamada "digestión del mensaje" de la cual es computacionalmente imposible encontrar dos mensajes distintos con la misma digestión o encontrar un mensaje a partir de una digestión conocida. Este método es utilizado como parte del proceso de Firma Digital.

Ensobretado:

Proceso mediante el cual se "ensobreta digitalmente" o "sella digitalmentet" un documento por medio del cual nadie más que el receptor indicado puede abrir.

Expiración:

Los Certificados Digitales y las Claves tienen un periodo de vida limitado, para lo cual las fechas de expiración son utilizadas.

Listas de Revocación de Certificados (CRL):

Contiene los certificados revocados, manteniéndose ahí hasta su fecha de expiración.

Mensajes:

Es la representación digital de la información y que es generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología.

No Repudiación:

Propiedad de los sistemas criptográficos por medio de la cual los usuarios no pueden negar acciones realizadas por ellos.

Requerimiento de Certificación:

Documento electrónico que contiene los datos de identificación del solicitante del certificado y contiene una clave pública a la cual se está vinculando, este documento será presentado al Agente Certificador para que realice las indagaciones necesarias para verificar la identidad del solicitante y la posesión de la clave privada correspondiente a la clave pública que ostenta.

Revocación:

Es la anulación de un Certificado Digital antes de su fecha de Expiración, esta anulación puede ser por: robo, olvido o extravío de la contraseña de la clave privada o de la propia clave privada, la sospecha de utilización de la clave privada por parte de un tercero no autorizado, cambio de alguno de los datos contenidos en el certificado digital o a solicitud expresa de alguna autoridad competente.

Suspensión:

La suspensión es un paso previo a la Revocación del Certificado, la cual aplica por razones de urgencia.

UTC:

Tiempo Universal Coordinado.

Time Stamping:

Registro que matemáticamente liga a un documento con una fecha y hora de creación o de firmado o de transmisión.

ANEXO 5.

CRIPTOGRAFÍA CUÁNTICA: LA ÚLTIMA FRONTERA²¹

Si anteriormente nos estremecíamos con los peligros que representa la computación cuántica para la criptografía, dada la longitud actual de claves, que debería ser doblada, nos fascinaremos a continuación con la forma como la criptografía cuántica sería capaz de implementar por primera vez una cinta aleatoria segura, soslayando el talón de Aquiles de su precaria distribución. Lo que con una mano quita la computación cuántica, con la otra repone.

La piedra angular de la criptografía cuántica es el principio de incertidumbre de Heisenberg, que, como aprendimos en la Universidad, nos enseña que no pueden conocerse simultáneamente con exactitud dos variables complementarias, como la posición y la velocidad, de una partícula. Supongamos entonces que tenemos un fotón que puede estar polarizado en una de cuatro direcciones distintas: vertical ($|$), horizontal ($--$), diagonal a la izquierda (\backslash) o diagonal a la derecha ($/$). Estas cuatro polarizaciones forman dos bases ortogonales: $|$ y $--$, y $/$ y \backslash , respectivamente.

Pues bien, el principio de incertidumbre de Heisenberg, por irracional que nos parezca, impide que podamos saber en cuál de las cuatro posibles polarizaciones se encuentra el fotón. Para conocerla, deberíamos utilizar un filtro, que podríamos imaginarnos como una ranura en una lámina, que tuviera la orientación, por ejemplo, vertical ($|$). Es evidente que los fotones con la misma polarización pasarán, mientras que los polarizados horizontalmente, y por lo tanto, perpendiculares al filtro, no pasarán. Sorprendentemente, ¡la mitad de los polarizados diagonalmente pasarán y serán reorientados verticalmente!

²¹ **FUENTE:** Boletín Criptonómico. 1997-2000 Gonzalo Álvarez Marañón, Instituto de Física Aplicada del CSIC.

Por lo tanto, si se envía un fotón y pasa a través del filtro, no puede saberse a ciencia cierta si poseía polarización vertical o diagonal, tanto $|$ como $/$. Igualmente, si no pasa, no puede afirmarse que estuviera polarizado horizontal o diagonalmente. En ambos casos, un fotón con polarización diagonal podría pasar o no con igual probabilidad.

Para utilizar estos increíbles resultados en criptografía, se acuerda representar un 1 ó un 0 de información según la polarización de los fotones que se envían. Así, en la base rectangular, que llamaremos (+), un 1 vendría representado por una polarización $|$, mientras que un 0, por $--$; mientras que en la base diagonal (x), el 1 sería la polarización $/$ y el 0, \backslash . En estas condiciones, para enviar un mensaje binario, Alicia va enviando fotones a Bernardo con la polarización adecuada, cambiando aleatoriamente de una base a otra.

Si un intruso, Ignacio, intercepta los fotones y mide su polarización utilizando un filtro, digamos ($|$), debido al principio de incertidumbre nunca podrá saber si los fotones pertenecían a la base + o x, y por lo tanto nunca sabrá qué mensaje se envió, da igual qué tipo de filtro utilice. Ahora bien, algún lector ya se estará dando cuenta de que si Ignacio se encuentra con este dilema, lo mismo le ocurrirá a Bernardo.

Efectivamente, emisor y receptor no pueden acordar de antemano qué bases se utilizarán para enviar cada fotón, porque entonces nos encontraríamos con el problema de cómo hacerse llegar mutuamente de forma segura esa lista de bases y volveríamos al principio. Tampoco pueden utilizar RSA, porque, si recuerdan, la criptografía cuántica la habría hecho zozobrar. ¿Qué solución tomar entonces?

En 1984 Charles Bennet y Gilles Brassard idearon el siguiente método para hacer llegar el mensaje al destinatario sin necesidad de recurrir a otros canales

de distribución. En primer lugar, debe allanarse el camino mediante los siguientes tres pasos:

Paso 1: Alicia le envía a Bernardo una secuencia aleatoria de 1's y 0's, utilizando una elección aleatoria entre las bases + y x.

Paso 2: Bernardo tiene que medir la polarización de estos fotones. Para ello, utiliza aleatoriamente las bases + y x. Claro está, como no tiene ni idea de qué bases utilizó Alicia, la mitad de las veces estará eligiendo mal la base, por lo que, en promedio, 1 de cada 4 bits que Bernardo recibe será erróneos.

Paso 3: para resolver esta situación, Alicia llama a Bernardo por teléfono, o se conectan a un chat, o utilizan cualquier otro canal de comunicaciones inseguro, sin preocuparse si son espiados por Ignacio, y le cuenta qué base de polarización utilizó para cada fotón que envió, + o x, aunque no le dice qué polarización concreta. En respuesta, Bernardo le cuenta a Alicia en qué casos ha acertado con la polarización correcta y por lo tanto recibió el 1 ó 0 sin error. Ahora ya, ambos eliminan los bits que Bernardo recibió con las bases erróneas, quedando una secuencia menor que la original, que constituye la clave de una cinta aleatoria 100% segura, puesto que se generó de forma completamente aleatoria por ser derivada de una secuencia original de 1's y 0's aleatoria.

¿Y qué ocurre con el malvado Ignacio? Para su desgracia, aunque intercepte los mensajes de Alicia y Bernardo, no obtendrá ninguna información útil para él, ya que nunca sabrá qué polarizaciones concretas en que cada base utilizó Alicia. Más aún, la mera presencia de Ignacio en la línea será detectada, ya que si mide la polarización de un fotón con el detector equivocado, la alterará. Lamentablemente, como el lector avisado se dará cuenta, esta alteración impediría que Alicia y Bernardo pudieran ponerse de acuerdo acerca de la secuencia aleatoria a usar como cinta, debido a que, si Ignacio cambió la

polarización de un fotón por el camino, podrían obtener distintos bits incluso aunque utilicen las mismas bases.

Por consiguiente, hace falta un método para detectar que Ignacio no esté haciendo de las suyas. En realidad, resulta tan sencillo como sigue: Bernardo le cuenta a Alicia, utilizando el mismo u otro canal inseguro, cuáles son los primeros, digamos que, 50 bits de su clave aleatoria. Si coinciden con los de Alicia, entonces saben que Ignacio no les espió ni el canal tiene ruido y utilizan con seguridad el resto de los bits generados. Si no coinciden, ya saben que Ignacio metió la manzana por medio o utilizaron un canal muy ruidoso y por lo tanto deben desechar la clave entera.

En 15 años, puede decirse que no se han producido muchos más avances teóricos en el campo de la criptografía cuántica, aunque se han dado pasos de gigante en cuanto a la implementación tecnológica de lo que, de otra forma, habrían terminado como elucubraciones mentales para juegos de salón. Manipular fotones individuales constituye todo un desafío de ingeniería, que fue aceptado con entusiasmo por Bennet y un estudiante. Y así, en 1989, consiguieron la primera transmisión de señales cuánticas de la historia a una distancia de 32 cm. ¡El sueño de la distribución cuántica de claves (QKD) por fin se hacía realidad! En 1995, investigadores de la Universidad de Ginebra lo consiguieron utilizando una fibra óptica de 23 Km de longitud. Actualmente, el récord de distancia de transmisión lo ostenta el laboratorio de Los Álamos en 50 km. Por su parte, en enlaces aéreos la distancia más larga ha sido de 1.6 km. Si se progresara en las transmisiones inalámbricas, incluso podría utilizarse la QKD en comunicaciones por satélite, aunque hoy por hoy todavía son inalcanzables.

Queda por resolver la cuestión de cuán segura es la QKD, ya que en la práctica el protocolo presenta ligeras debilidades (¿cómo sabe Alicia que está hablando con Bernardo?, ¿Qué ocurre si alguien interrumpe su comunicación?), y el

estado del arte actual de la tecnología no es capaz de fabricar aún fibras, transmisores y detectores con la perfección requerida por la QKD, como para evitar otros ataques basados en física cuántica (espejos en la fibra que dejan pasar la mitad del fotón, emisión de dos fotones simultáneamente, etc.). Hasta ahora, la única prueba rigurosa de la seguridad de QKD se debe a los investigadores Lo y Chau, quienes demostraron que, contando con la existencia de ordenadores cuánticos, la distribución cuántica de claves a lo largo de distancias arbitrarias puede tener lugar de forma incondicionalmente segura. Claro que, dado que ni en la actualidad ni en un futuro cercano se prevé la existencia de tales ingenios, el problema de la seguridad de la QKD con los sistemas actuales permanece como un problema abierto.

Estos primeros resultados en cualquier caso tan alentadores permiten acariciar la idea de anillos de fibra óptica para redes LAN o pequeñas redes WAN que conecten de la forma más segura jamás conocida distintos edificios ministeriales u oficinas bancarias de una misma ciudad. Sería el Olimpo de la criptografía. El triunfo definitivo de la seguridad y la privacidad.

Citando una vez más las palabras de Simon Singh, autor de la excelente obra "[The Code Book](#)", si los ingenieros consiguen hacer funcionar la criptografía cuántica a través de largas distancias, la evolución de los algoritmos de cifrado se detendrá. La búsqueda de la privacidad habrá llegado a su fin. La tecnología garantizaría las comunicaciones seguras para gobiernos, militares, empresas y particulares. La única cuestión en el tintero sería si los gobiernos nos permitirían a los ciudadanos usarla. ¿Cómo regularán los Estados la criptografía cuántica, enriqueciendo la Era de la Información, pero sin proteger al mismo tiempo las actividades criminales?

LA CRIPTOGRAFÍA CUÁNTICA SUPERA LOS 100 KILÓMETROS²²

Es una tecnología teóricamente inviolable desarrollada con fines comerciales.

Un grupo de investigadores de Toshiba Research Europe, en el Reino Unido, ha conseguido romper la barrera de los 100 kilómetros en la criptografía cuántica transmitida a través de fibra óptica, una tecnología teóricamente inviolable que según Andrew Shields, que ha capitaneado el proyecto, será desarrollada con fines comerciales en menos de tres años.

Los científicos han presentado su récord en la CLEO (Conference on Lasers and Electro-Optics), que anteriormente ostentaban una compañía japonesa y que databa de Noviembre de 2002 con 87 kilómetros de distancia.

Las claves criptográficas de hoy en día (usadas en el protocolo SSL para transacciones seguras entre clientes y bancos, por ejemplo), se componen de cadenas aleatorias de números y letras. Para comenzar una transacción segura, estas claves deben ser intercambiadas entre los interlocutores. En este paso previo es donde se producen la mayor parte de los espionajes, interceptando la clave (encriptada a su vez con otros mecanismos) en el momento de la transmisión cuando viaja electrónicamente por redes convencionales. Si todo ha ido bien, el otro interlocutor puede desencriptar el mensaje con una copia de la clave empleada originalmente.

La criptografía cuántica consigue conectar cada dígito de la clave a un mínimo conjunto de fotones, enviados en un minúsculo haz de luz. Al contrario que con la tecnología electrónica de hoy en día, leer la clave en su viaje alteraría el estado cuántico de los fotones de tal forma que el receptor sabría que ha sido manipulada o leída de alguna manera. Es en esto donde radica su seguridad, pero la atenuación periódica que sufren los estados de los fotones según la

²² FUENTE: Centre of Quantum Computation (www.qbit.org)

distancia recorrida y el medio en el que viajen, limita el uso de esta técnica a pequeñas redes experimentales hasta que se vayan desarrollando nuevas tecnologías de transmisión y ganando en distancia.

La carrera por la distancia está abierta en dos frentes, la fibra óptica, donde ya se han alcanzado los 100 kilómetros, y el aire como transmisor. En octubre de 2002, científicos de la firma [QinetiQ](#), la rama comercial de la agencia británica de investigación de defensa, consiguieron enviar con éxito una clave criptográfica a una distancia de más de 23 kilómetros de espacio abierto entre dos montañas en Alemania. Se espera que dentro de seis años, esta técnica esté lista para enviar claves a cualquier parte del mundo utilizando satélites de órbita baja.

UN GRAN OBSTÁCULO DE COHERENCIA²³

Desde los inicios de la mecánica cuántica se conoce la extraña interacción existente entre un estado cuántico y su entorno: cualquier modificación del mismo transforma el sistema cuántico. De esta forma, si pretendemos observar el estado de un qubit cambiaremos automáticamente su estado, porque no es posible realizar dicha observación sin alterar el entorno. Entonces, ¿es imposible operar con qubits?. El último experimento de Isaak L. Chuang, de IBM (en la foto), y Neil Gershenfeld, del MIT, consiguió realizar una implementación simple del algoritmo de Shor con una agrupación de siete qubits. Los expertos del grupo de computación cuántica de la Facultad de Informática de la UPM afirman en un manifiesto conjunto que no, porque "existen códigos correctores de errores cuánticos", algo sorprendente si tenemos en cuenta que no se puede observar el estado cuántico. "Se ha demostrado - añaden - que la computación

²³ Fuente:

<http://www-i.laprensa.com.ni/archivo/2003/junio/17/informatica/informatica-20030617-01.html>

cuántica tolerante a fallos es viable por debajo de un determinado umbral de ruido", que en términos cuánticos se denomina decoherencia. Si se consigue que los cambios en el sistema cuántico sean mínimos, es decir, que la decoherencia permita realizar operaciones con una fidelidad razonable, no hay ninguna ley física que impida la construcción de un ordenador de este tipo. "El principal obstáculo para hacer actualmente un ordenador cuántico es la decoherencia", afirma uno de los pioneros de este emergente campo científico, David Deutsch, físico de la Universidad de Oxford, Inglaterra. "Una vez superado, estoy seguro de que será construido - añade - aunque todavía estamos a décadas de conseguir uno". La mayoría de los científicos involucrados en las investigaciones coinciden en señalar que todavía habrá que esperar bastante tiempo para gozar de la potencia de cálculo de estos "supercomputadores", que, sin duda, reportaría beneficios enormes a la sociedad. "Los avances en su comprensión - dice Vicente Martín - son avances en nuevos materiales, nuevos fármacos, nuevos procesos de síntesis química, nuevos dispositivos electrónicos: circuitos, sensores, displays...". Cuanto menos, esta tecnología ha generado una gran expectación en el ámbito científico, habiendo sido citada como una de las "10 tecnologías emergentes que cambiarán el mundo" por la revista MIT Technology Review.