UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ACATLÁN

“CERTIFICADOS DIGITALES Y SU INCORPORACIÓN AL SISTEMA FINANCIERO MEXICANO”

TESINA

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN MATEMATICAS APLICADAS Y COMPUTACION

PRESENTA

JUAN LEÓN VÁZQUEZ

ASESOR: MTRA. SOCORRO MARTÍNEZ JOSÉ

MAYO, 2013

DEDICATORIAS

A mí esposa, quien ha estado siempre a mi lado, alimentado nuestros sueños.

A mis 2 tesoros, que llenan nuestros corazones de amor.

A la memoria de mis padres, que siempre están conmigo en mis recuerdos.

A mis queridos amigos por su apoyo y palabras de ánimo.

AGRADECIMIENTOS:

A la Universidad Nacional Autónoma de México, por darme la oportunidad de pertenecer a esta gran institución.

A mi amiga y asesora, Mtra. Socorro Martínez José, por creer siempre en mí y por su infinita paciencia, que me impulsaron a terminar este trabajo.

A los sinodales: Act. Luz María Lavín Alanís, Lic. Alejandro Roberto Rubio Pérez, Lic. Areli Pineda Caballero, Mtro. Gabriel Díaz Mirón Mac Donough, por el tiempo invertido a la revisión de este trabajo.

Certificados digitales y su incorporación al sistema financiero mexicano

Introducción

En los últimos años se ha experimentado un vertiginoso crecimiento de las redes de comunicación y de los usuarios que las utilizan, lo que ha traído nuevos problemas a resolver, y uno de ellos es la seguridad.

Cuando las redes de comunicación eran de uso exclusivo de muy pocas personas (grandes empresas y universidades), se podía intercambiar información entre ellas, utilizando lo que hoy se le conoce como algoritmos de clave simétrica, lo cual era viable por el número tan pequeño de usuarios. Sin embargo, en la actualidad, el proporcionar una clave a un par de personas resulta una práctica imposible ya que una sola persona puede tener "n" número de interlocutores.

La forma en que diversas empresas han tratado de resolver este problema, es con lo que hoy se conoce como infraestructura de llave pública, donde la idea general es la de proveer de un solo par de claves (una pública y una privada) a cada usuario, sin importar el número de usuarios con quien desee comunicarse. Estas claves tienen la función de invertir la acción de la otra, es decir sí una cifra la otra descifra. Otra cualidad de las llaves radica en que no es posible saber cuál es la otra llave, si se conoce una de ellas.

Mediante un mecanismo de distribución, la llave pública puede ser conocida por diversas personas así como la identidad del propietario, mientras la llave privada debe ser custodiada por el usuario propietario de las llaves. De este modo, si un usuario desea enviar un mensaje seguro al usuario dueño de las llaves, utilizará la llave pública de éste para cifrar el mensaje; una vez cifrado será enviado y éste tendrá la certeza que solo el propietario de la llave privada será el único que podrá descifrarlo y leer el contenido.

Implementado el esquema de llave pública nos daría la impresión de que todos los problemas de seguridad quedarían resueltos, pero el utilizarlo trae un nuevo problema: el de la autentificación. ¿Cómo saber que la llave pública que estoy

utilizando para cifrar un mensaje es de la persona que dice ser y no de otra que está suplantando su identidad? La respuesta surge del concepto de certificación. La certificación consiste en que un tercero (conocido como agencia certificadora) garantiza que la identidad de la persona es de la que dice ser y que la llave pública también pertenece a esa persona.

En nuestro país diversas empresas privadas y entidades gubernamentales han realizado muchos esfuerzos para implementar éstas tecnologías, todo encaminado a reducir costos administrativos y mejorar los controles sobre los procesos que son susceptibles a la implementación de los certificados digitales.

Esto ha generado que el gobierno mexicano tenga la necesidad de legislar leyes para proporcionar mecanismos que simplifiquen tiempos de procesamiento, minimicen los costos y, sobre todo, que proporcionen un fuerte esquema de seguridad, tanto para las empresas como para las personas.

Diversos sectores productivos y paraestatales han comenzado a explotar la simplificación que representa la transferencia de información bajo esta infraestructura, un ejemplo claro es el envío de facturación entre empresas que agiliza los tiempos de entrega de productos y una forma de fiscalización más rápida y eficiente por parte del SAT.

Mientras más avancemos en la implementación de la tecnología de certificados digitales estaremos haciendo más eficientes los procesos en los cuales estamos inmersos.

Por tanto, el siguiente trabajo tiene como objetivo dar a conocer el concepto y uso de los certificados digitales, describiendo cómo esta tecnología se aplica actualmente al Sistema Financiero Mexicano. Pero en primera instancia se explicarán la necesidad de crear sistemas criptográficos, así como los conceptos más básicos de los mismos.

Capítulo I – Historia y conceptos de criptografía

Antecedentes

La criptografía es casi tan antigua como la misma escritura, siempre que ha habido comunicación entre dos personas o grupos de personas, hay un tercero que puede estar interesado en interceptar y leer esa información.

Entonces el principio básico de la criptografía es mantener la privacidad de la comunicación entre dos personas alterando el mensaje original de modo que sea incomprensible a toda persona distinta del destinatario.

Algunos indicios del uso de técnicas criptográficas se remontan al siglo V A.C. en la antigua Grecia, donde diversos pueblos utilizaban técnicas elementales de cifrado para proteger su información.

El primer método de cifrado reconocido como tal se debe a Julio César, su algoritmo consiste en el desplazamiento de tres posiciones hacia la derecha de los caracteres del texto sin cifrar, así sustituía cada letra del mensaje por su tercera siguiente en el alfabeto

Durante la primera guerra mundial se utilizaron técnicas criptográficas con muy mal resultado, lo que impulso al final de la guerra, el desarrollo de las primeras tecnologías electromecánicas. Un ejemplo de estos desarrollos es la máquina Enigma, utilizada por los alemanes para cifrar y descifrar sus mensajes durante la segunda mundial.

Conceptos Básicos

Para poder entender la criptografía debemos tener claros algunos conceptos básicos, los cuales sustentan y son la base de todas las teorías y esquemas que se han desarrollado alrededor del tema.

Criptografía

Primeramente precisaremos ¿Qué es la criptografía? El término criptografía proviene del griego kryptos "ocultar" y grafos "escribir", que literalmente significa escritura oculta y se puede describir como el arte de cifrar y descifrar información utilizando técnicas matemáticas que hacen posible el intercambio de información de manera que solo puedan ser leídos por las personas a quien van dirigidos.

Este término resulta poco acertado si lo aplicamos a nuestro entorno actual, ya que tenemos información en diversos formatos que necesitamos que se encuentre protegida de terceros. Por otra parte supone la existencia de una sola clave para cifrar y descifrar la información, cuando las técnicas actuales usan al menos 2 claves para realizar el ciclo completo.

En los primeros sistemas criptográficos la dificultad para descifrar un mensaje radicaba en encontrar el método con el cual se había cifrado la información, la fortaleza de los sistemas actuales radica en la complejidad para descifrar la clave con la cual se cifró el mensaje, ya que el método es conocido.

El objetivo de la criptografía puede resumirse en:

- Garantizar la confidencialidad en la comunicación entre dos entidades.
- Garantizar la autenticidad de la información en ambos sentidos de la comunicación.

- Garantizar la integridad de la información en ambos sentidos de la comunicación.

Criptosistema

Se puede definir a un criptosistema como un conjunto de tres elementos:

- Un conjunto de mensajes *M* que es la colección de todos los mensajes que pretendemos enviar.
- Un conjunto de claves *K*, cada clave determina un método de cifrado *CK* y un método de descifrado *DK*, tal que:
    - ***CK(M) = M cifrado***

    y

    - ***DK(M cifrado) = M***
- Y otro conjunto de mensajes *M* cifrados.

De tal forma que un criptosistema es la forma más simple de representar un sistema de encriptación.

Criptoanálisis

El término criptoanálisis proviene del griego kryptos "escondido" y analyein "desatar". El criptoanálisis es la ciencia complementaria de la criptografía ya que proporciona las herramientas necesarias para vulnerar los sistemas criptográficos demostrando las debilidades del algoritmo.

Para establecer las posibles debilidades del sistema, se asumen en el análisis las condiciones del peor caso:

- Se tiene acceso completo al algoritmo de encriptación.
- Se tiene una cantidad considerable de texto cifrado.
- Se conoce el texto descifrado de una parte de ese texto cifrado.

Cuando se realiza el análisis a los sistemas criptográficos es importante no olvidar que también existen aquellos donde solo se conoce el algoritmo de encriptación y donde el analista se concentra en probar cada una de las posibles claves del espacio de claves posibles hasta encontrar la correcta, a esta técnica se le llama de "fuerza bruta" o "ataque exhaustivo".

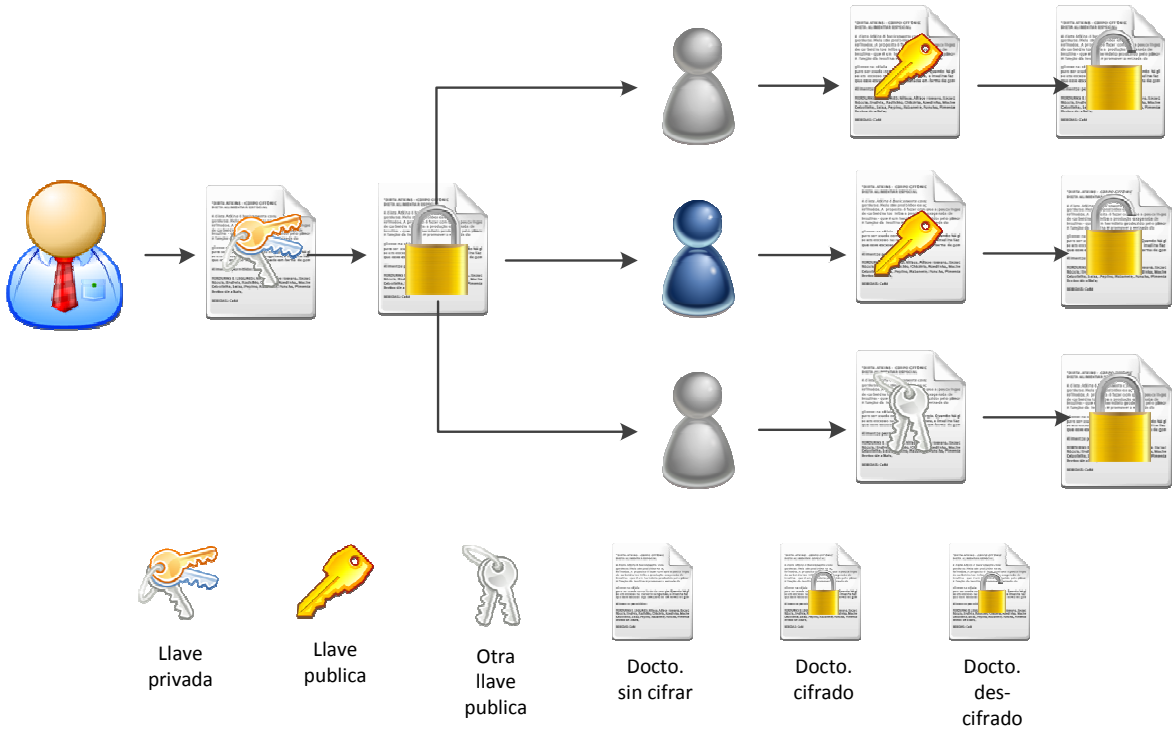
Existen dos técnicas básicas de cifrado basadas en caracteres:

- Técnicas de sustitución: Los caracteres y/o letras del mensaje sin cifrar se modifican o sustituyen por otros caracteres o letras en la cifra. El criptograma tendrá entonces caracteres distintos a los que tenía el mensaje sin cifrar.
- Técnicas de transposición o permutación: los caracteres o letras del mensaje sin cifrar se redistribuyen sin modificarlos según las reglas del algoritmo usado, dentro del criptograma. El criptograma tendrá entonces los mismos caracteres del mensaje sin cifrar pero con una distribución o localización diferente.

El desarrollo constante de la criptografía tiene como resultado el sistema criptográfico más usado: La PKI, misma que explicaremos en el siguiente capítulo.

Capítulo 2 - Infraestructura de clave pública

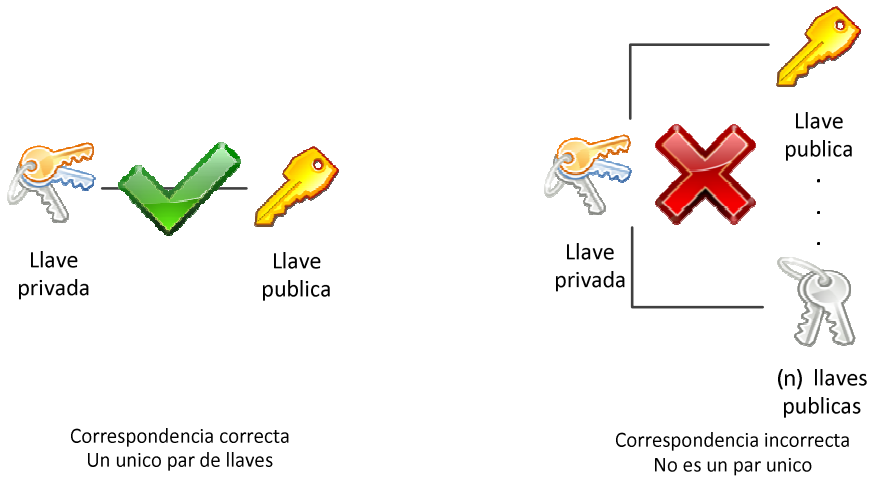
La tecnología de PKI (Public Key Infrastructure) ha tenido una gran evolución para tratar el problema de "autentificación distribuida" a gran escala.



PKI usa un sistema asimétrico que implica llaves matemáticamente relacionadas, pero diferentes, donde la llave pública está abierta y disponible para cualquiera que la necesite, y la llave privada la posee y sólo la puede "ver" el dueño de la misma, con estas llaves se llevan a cabo las operaciones criptográficas.

Cualquier persona puede utilizar la llave pública para cifrar un mensaje, aunque solo el poseedor de la llave privada podrá descifrar el mismo. De forma recíproca el poseedor de la llave privada podrá cifrar un mensaje y será descifrado por la persona que posea la clave pública.

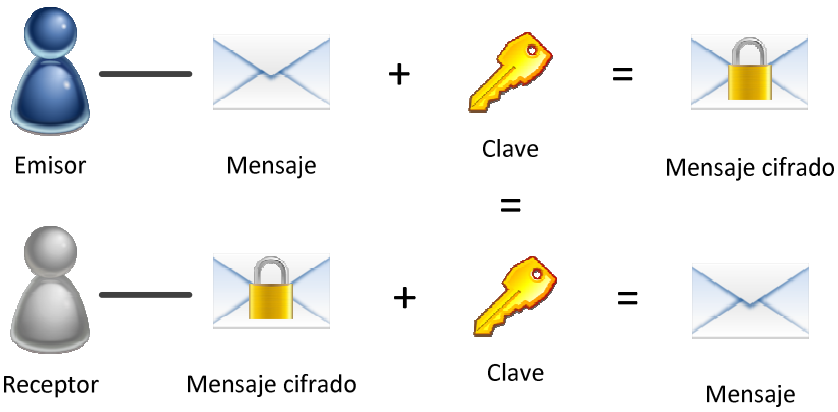
El utilizar una llave pública que no esté relacionada a la llave privada con la que se cifro el mensaje, dará como resultado la no legibilidad del mensaje ya que este será imposible de descifrar, ratificando el concepto de un par de llaves únicas.



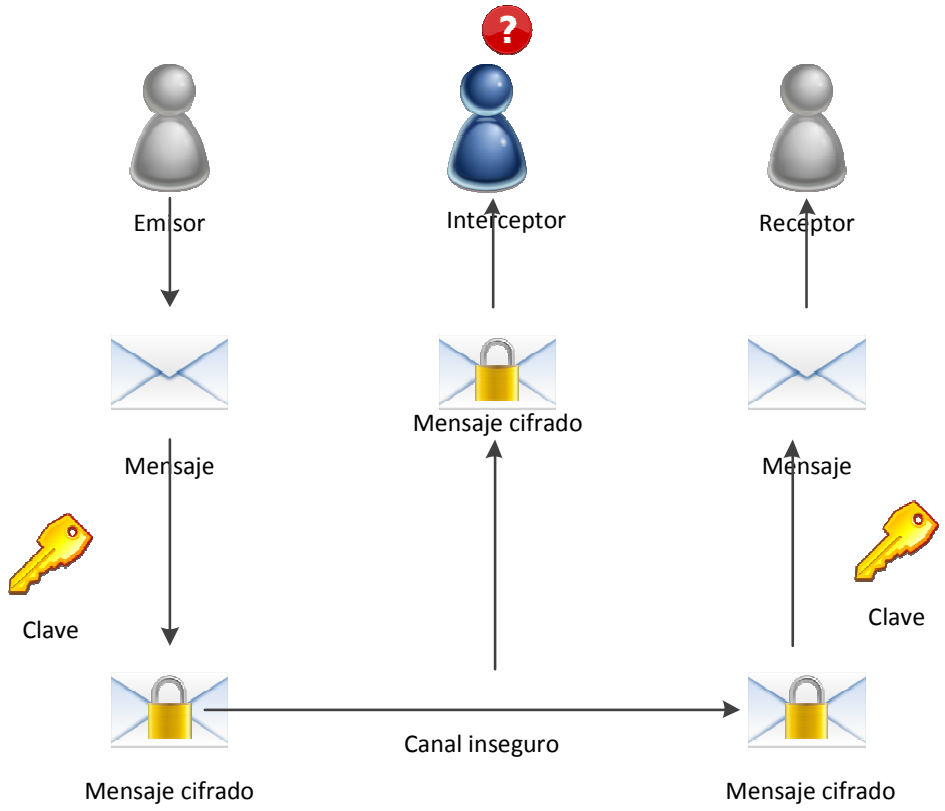
El uso de esta infraestructura es ideal para prestar servicios de autentificación de usuarios, el no repudio del mensaje, la integridad de la información, la auditabilidad de información y la confidencialidad de la misma.

Claves simétricas

El cifrado de información con claves simétricas, también llamado cifrado de claves compartidas o criptografía de clave secreta, utiliza una única clave que se encuentra en poder del remitente y el destinatario. Esta clave es utilizada tanto para el cifrado como para el descifrado y se denomina **clave secreta o simétrica**.



Todos los algoritmos que se ocupan para el cifrado de claves simétricas tienen el mismo objetivo: la transformación reversible de un texto sin formato en texto cifrado, el cual es ininteligible para quien no tenga la clave secreta para descifrar el texto, el esquema básico de estos algoritmos es:



Este proceso se lleva a cabo sustituyendo porciones del mensaje original por porciones de mensaje cifrado, utilizando la clave simétrica, la sustitución se puede hacer de diversas formas:

- Monoalfabéticas: Un carácter cifrado corresponde a un solo carácter del mensaje original y viceversa.
- Homofónica: Un carácter del texto original se cifra en varios caracteres del mensaje cifrado.
- Poligráfica: n caracteres del mensaje original generan n caracteres del mensaje cifrado.

- Polialfabética: n caracteres del mensaje original generan m caracteres del mensaje cifrado ($m \neq n$).

Si analizamos los diferentes tipos de sustituciones podemos concluir que la sustitución Homofónica y Poligráfica son casos particulares de la sustitución Poli alfabética.

Sistemas Monoalfabéticos y Polialfabéticos

Los algoritmos de cifrado por clave simétrica son monoalfabéticos si cada ocurrencia de un mismo carácter en el mensaje original es remplazada por un mismo carácter en el mensaje cifrado.

Por otro lado los algoritmos de cifrado por clave simétrica son polialfabéticos si para cada ocurrencia de un mismo carácter en el mensaje original es remplazado por distintos caracteres en el mismo mensaje.

Algunos de los sistemas de cifrado de clave simétrica son:

Criptosistema Caesar

El sistema Caesar o de desplazamiento es una de las técnicas de cifrado más simple y es el sistema más antiguo del que se tenga registro y es un sistema monoalfabético.

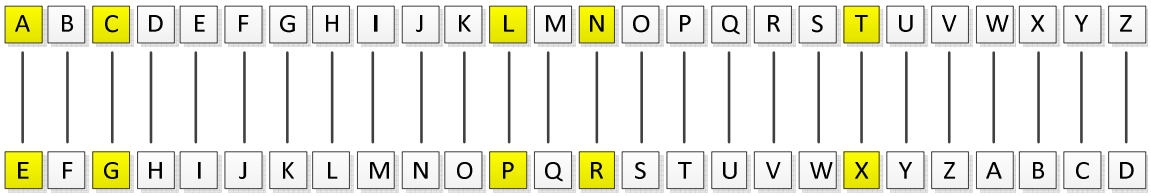
En este algoritmo el cifrado se hace por sustitución, cada carácter del mensaje original *M* se sustituye por otro carácter en el mensaje cifrado, el carácter cifrado se obtiene avanzando *K* pasos en el alfabeto a partir del carácter original, donde *K* es la clave.

Ejemplo:

Si le asignamos clave: *K = 4*

y mensaje original: *M* = "ACATLAN"

Entonces aplicando la clave obtenemos:



Entonces el mensaje cifrado es "EGEXPER".

Criptosistema Hill

Se basado en el uso de álgebra lineal y es el primer sistema criptográfico polialfabético que era práctico para trabajar con más de 3 símbolos simultáneamente

Las letras se enumeran en orden alfabético de forma tal que *A=0*, *b=1*, … ,*Z=25*

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*

Se elige un entero d que determina bloques de d elementos que son tratados como un vector de d dimensiones

Se determina de forma aleatoria una matriz de *d* por *d* elementos, donde los elementos serán enteros entre 0 y 25, además la matriz debe ser inversible en $\mathbb{Z}_{26}^{n}$.

El cifrado del texto se lleva a cabo dividiendo el texto en bloques de *d* elementos los cuales se multiplican por la matriz *d* por *d*, todas las operaciones se llevan a cabo en módulo 26, aplicando:

$M \times Pi = Ci$, donde *Ci* es el código cifrado para el mensaje original *Pi*

Ejemplo:

Si $d = 3$

y

$$M = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix}$$

Para cifrar el mensaje "ACATLAN" debemos de dividir el mensaje en bloques de d caracteres cada uno, teniendo el siguiente resultado:

$$P_1 = "ACA" = \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} \qquad P_2 = "TLA" = \begin{pmatrix} 19 \\ 11 \\ 0 \end{pmatrix} \qquad P_3 = "NXX" = \begin{pmatrix} 13 \\ 23 \\ 23 \end{pmatrix}$$

Para cumplir con la premisa de dividir el mensaje en tramos de tamaño *d* utilizamos un carácter de relleno, en este caso X.

Procedemos a aplicar $M \times Pi = Ci$,

$$M * P_1 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 34 \\ 46 \\ 22 \end{pmatrix} = \begin{pmatrix} 8 \\ 20 \\ 22 \end{pmatrix} (\mathrm{mod}\, 26)$$

El primer bloque "ACA" se codifica como "IUW"

$$M * P_2 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix} \begin{pmatrix} 19 \\ 11 \\ 0 \end{pmatrix} = \begin{pmatrix} 282 \\ 424 \\ 159 \end{pmatrix} = \begin{pmatrix} 22 \\ 8 \\ 3 \end{pmatrix} (\mathrm{mod}\, 26)$$

El segundo bloque "TLA" se codifica como "WID"

$$M * P_3 = \begin{pmatrix} 5 & 17 & 20 \\ 9 & 23 & 3 \\ 2 & 11 & 13 \end{pmatrix} \begin{pmatrix} 13 \\ 23 \\ 23 \end{pmatrix} = \begin{pmatrix} 916 \\ 715 \\ 578 \end{pmatrix} = \begin{pmatrix} 6 \\ 13 \\ 6 \end{pmatrix} (\mathrm{mod}\, 26)$$

El Tercer bloque "NXX" se codifica como "GNG".

Entonces el texto cifrado "ACATLANXX" equivale a "IUWWIDGNG", como podemos ver la "A" aparece 3 veces, mismas que tienen 3 valores diferentes dentro del texto cifrado "I","W" y "D"

El procedimiento para descifrar el mensaje es idéntico al anterior, pero utilizando la matriz inversa en módulo 26 de la matriz la utilizada para cifrar.

El uso de métodos de claves simétricas es eficiente para el cifrado de grandes cantidades de datos; sin embargo, al utilizar la misma clave para cifrar como para descifrar los mensajes, la seguridad del proceso depende de la posibilidad de que una persona no autorizada consiga la clave simétrica. Esto implica que las personas que deseen utilizar los algoritmos de claves simétricas deben de intercambiar de forma segura la clave antes de intercambiar datos cifrados.

Al utilizar algoritmos de clave simétrica de *"n"* bits de longitud para encriptar textos de más de n bits se aplica una técnica particular, donde la más simple consiste en dividir el mensaje a cifrar en bloques de igual longitud que la clave que se está utilizando *(n)* y cifrar cada uno en forma independiente, este método se le conoce como Electronic Code Block (ECB), otras técnicas más son:

- CBC: Cipher Block Chainning
- CFB: Chipre Feedback
- OFB: Output Feedback

En la actualidad se han desarrollado algoritmos de clave simétrica mucho más complejos y que se emplean para proporcionar soluciones a diferentes esquemas de seguridad.

La efectividad de los algoritmos simétricos radica en el tamaño de la clave, mientras mayor sea la clave, más grande será el universo de posibilidades para encontrar la clave correcta con la que se cifraron los datos. Algunos de los algoritmos simétricos más utilizados son:

- **RC2, de128 bits:** Es un algoritmo que toma como entrada bloques de 64 bits del mensaje, la clave es de tamaño variable y no hay un número de iteraciones definido para hacer el cifrado, este método se utilizó en los navegadores que utilizan las implementaciones **S**ecure **S**ockets **L**ayer (SSL) versión 2.0, el cual es un protocolo para la capa de conexión segura.

- **RC4, de128 bits:** Es un sistema de cifrado de flujo, la clave es de tamaño variable con operaciones a nivel de byte, se basa en permutaciones aleatorias, se utiliza principalmente para encriptar archivos y comunicaciones con protocolos como el SSL.

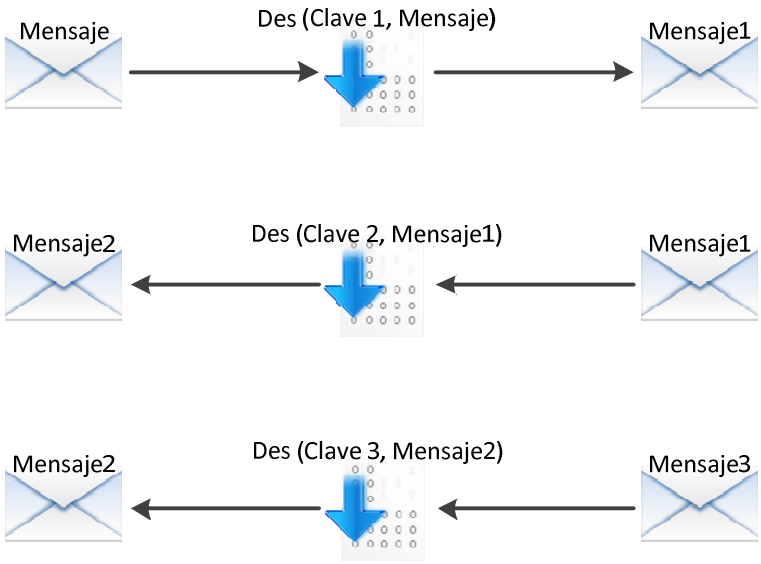
- **DES, de 56 bits:** Es un sistema que toma como entrada bloques de 64 bits del mensaje y éstos se someten a 16 iteraciones, con una clave de 64 bits, de los cuales 56 son utilizados para el cifrado y 8 son de paridad y se usan para detectar errores durante el proceso.

  Dependiendo de la aplicación que se le dé al algoritmo, éste se puede implementar de cuatro formas diferentes:

  i. ECB (Electronic Codebook Mode) para mensajes cortos de menos de 64 bits,
  ii. CBC (Cipher Block Chaining Mode) para mensajes largos,
  iii. CFB (Cipher Block Feedback) para cifrar bit por bit o byte por byte

iv. OFB (Output Feedback Mode) el mismo uso que CFB pero evitando la propagación de error

- **3DES, de 168 bits:** Es un sistema que aplica sistemáticamente tres veces el algoritmo DES; cada iteración del algoritmo tiene su propia clave. En la primera iteración se aplica el algoritmo de forma normal, el resultado de este alimenta la segunda iteración donde se aplica el proceso de descifrado con la segunda clave, en la iteración tres se vuelve a aplicar el método clásico pero utilizando la tercera clave:

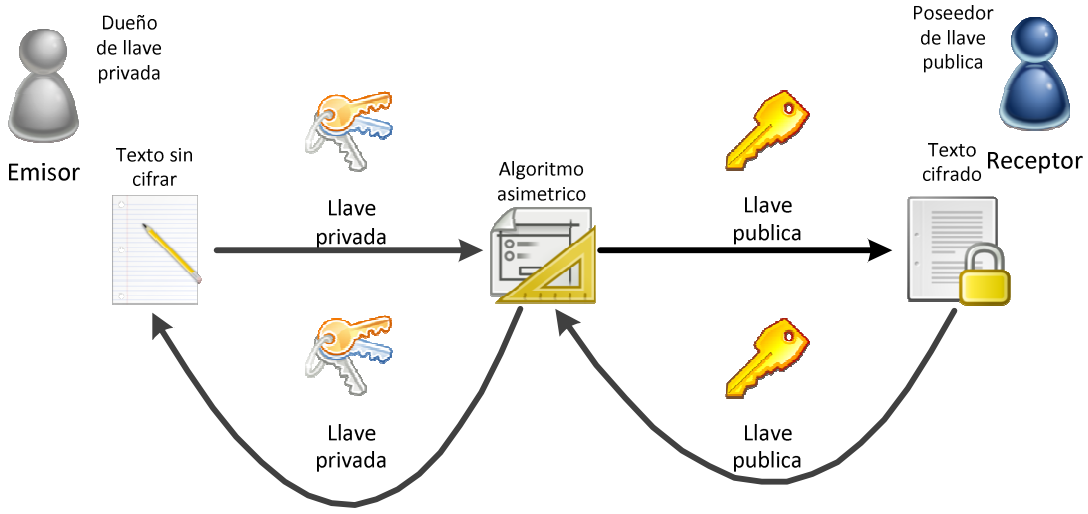


Claves Asimétricas

Los algoritmos asimétricos también llamados *algoritmos de llave pública*, utilizan dos claves: una pública y una privada (siempre formando un par), las claves se encuentran matemáticamente relacionadas entre sí. Estos algoritmos son ecuaciones matemáticas complejas en las que se utilizan números muy grandes, lo que plantea un problema muy difícil de resolver para alguien que intente descifrar el mensaje.

Los algoritmos asimétricos utilizan claves de longitud mayor que los algoritmos simétricos, la recomendación para la longitud de claves asimétricas es de 1024 bits, el principal inconveniente de esta forma de trabajo radica en la relativa lentitud del algoritmo.

En los algoritmos de llave pública, como ya lo comentamos anteriormente, se utilizan dos claves:



- **Clave pública:** puede intercambiarse libremente entre las partes involucradas, o publicarse en repositorios públicos.
- **Clave privada:** pertenece solamente a una entidad, la cual tiene la responsabilidad de custodiarla, ya que si ésta clave fuera conocida por un tercero, rompería con el esquema.

El principio básico de estos algoritmos es:

- Los datos cifrados con una clave privada solo podrán ser descifrados con su respectiva clave pública.
- Nunca se podrá descifrar un mensaje con la misma clave que se cifró, es decir una clave privada no podrá descifrar un mensaje que haya sido cifrado con ésta, esto también aplica para el uso de la claves públicas.

Los algoritmos de clave pública más utilizados son:

Algoritmo	Longitud de Clave	Uso
RSA	1024 bits a 2048 bits	Encriptación y firma digital
DSA	56 bits	Firma digital
Diffie-Hellman	1536 bits	Firma digital
DSS (Digital Signature Standard)	160 bits	Firma digital

RSA

El algoritmo RSA (por las iniciales de sus inventores Ron Rivest, Adi Shamir y Leonard Adleman) es el algoritmo de clave pública más utilizado, especialmente para la información que se envía a través de Internet, está integrado a varios navegadores, como Netscape e Internet Explorer, así como a otros muchos productos.

El uso frecuente de este algoritmo se debe a que se puede utilizar para firmas electrónicas y para el intercambio de claves, además al usar longitudes grandes para la clave, la dificultad para encontrar ésta en términos reales se vuelve casi imposible con las computadoras actuales.

Procedimiento del algoritmo RSA

1. Encontrar aleatoriamente 2 grandes números primos *p* y *q* (secretos).
2. Calcular el número *n* (público) mediante su producto *n = p * q* comúnmente conocido como módulo.
3. Se calcula *f(n) = (p-1) (q-1)*
4. Calcúlese un número natural de manera que *MCD(e, fi(n))=1* , es decir *e* debe ser primo relativo de *fi(n).*
   Es lo mismo que buscar un número impar por el que dividir *fi(n)* que de cero como resto.
5. Se calcula *d = ((Y * fi (n)) + 1) / e* para *Y=1,2,3,...* hasta encontrar un *d* entero.
6. El par de números *(e, n)* son la clave pública.
7. El par de números *(d, n)* son la clave privada.
8. Cifrado: La función de cifrado es *C = M^e mod n*

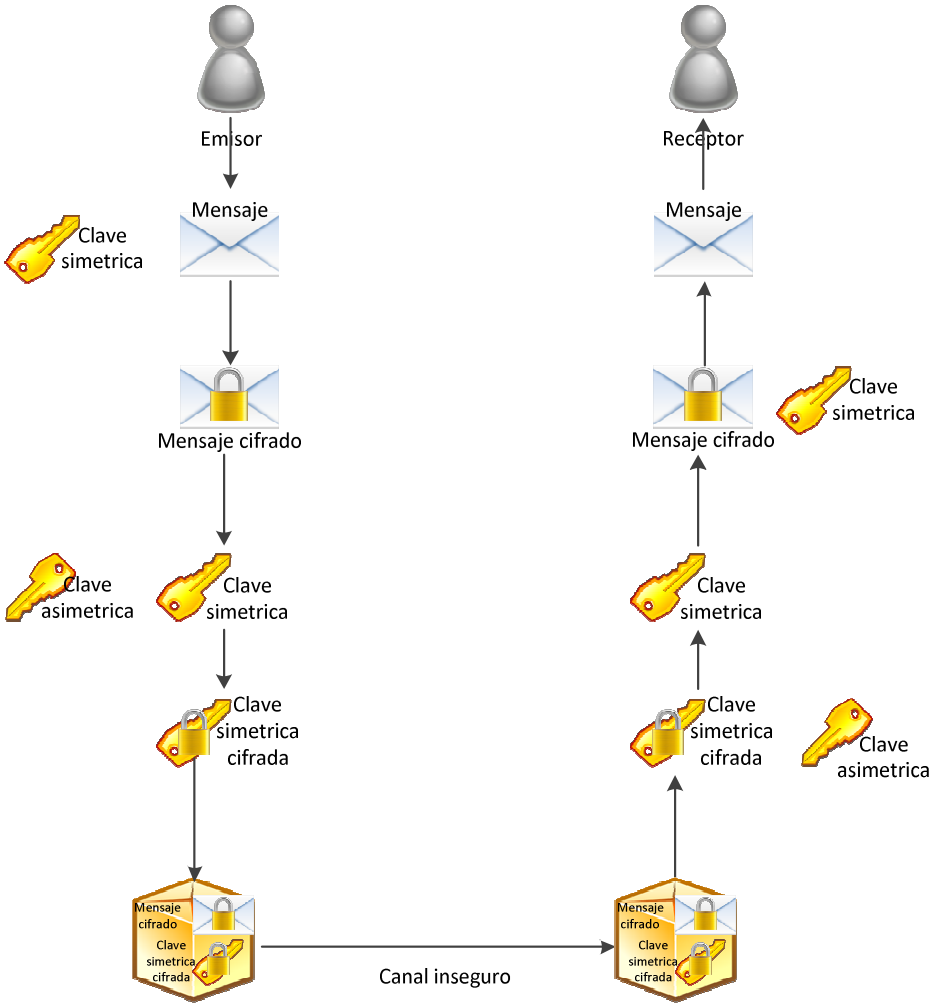
9. Descifrado: La función de descifrado es *M = C^d mod n*

Ejemplo (se utilizaran números pequeños):

1. Escogemos dos números primos, por ejemplo *p=3* y *q=11*.
2. Calculamos el numero *n = 3 * 11 = 33*.
3. Calculamos *fi(n) = (3-1) * (11-1) = 20*.
4. Buscamos *e*: *20/1=0, 20/3=6.67. e=3*.
5. Calculamos *d* como el inverso multiplicativo módulo *z* de *e*, por ejemplo, sustituyendo *Y* por *1,2,3,...* hasta que se obtenga un valor entero en la expresión: *d = ((Y * fi(n)) + 1) / e = (Y * 20 + 1) / 3 = 21 / 3 = 7*
6. El par de números *e=3* y *n=33* son la clave pública.
7. El par de números *d=7* y *n=33* son la clave privada.
8. Cifrando el mensaje, *m=5*, *C = M^e mod n = 5^3 mod 33 = 26*
9. Descifrado el mensaje, *M = C^d mod n = 26^7 mod 33 = 8031810176 mod 33 = 5*

Sistemas de cifrado híbrido

Utiliza claves simétricas y claves asimétricas. El proceso consiste en cifrar una clave simétrica con una clave asimétrica, donde previamente ya se cifró el mensaje con la llave simétrica. En cada mensaje la clave simétrica puede ser diferente, por lo que si un atacante pudiera descubrir la clave simétrica, solo le serviría para descifrar ese mensaje.



La infraestructura de clave pública utiliza sistemas de cifrado híbrido con la finalidad de ser eficiente ya que si un mensaje se cifrara solo con una clave asimétrica y el mensaje fuera muy grande el costo computacional sería muy grande.

Funciones Hash (Resumen)

Una función hash nos permite obtener un resumen a partir de un mensaje, dicho resumen es más pequeño que el mensaje original y es muy difícil encontrar otro mensaje que tenga el mismo resumen.

Las principales características de una función hash son:

- La función es irreversible, es decir que a partir del resultado de la función nunca se podrá obtener el documento original.
- Cualquier cambio en el documento por mínimo que sea, generará un resultado completamente distinto que el obtenido en el documento original.

Los algoritmos más utilizados para obtener un resumen de documentos son MD2, MD4, MD5 y SHA, éste ultimo de 160 bits.

MD5

MD5 es el algoritmo de resumen de mensaje (hash) más utilizado en el mundo, éste algoritmo fue diseñado por el profesor Ronald Rivest del Instituto tecnológico de Mássachussets en 1991. Su trabajo se basa en los algoritmos MD2 y MD4 los cuales mostraron que tenían diversos problemas de seguridad. El profesor utilizó los algoritmos como base pero eliminó los problemas de seguridad que éstos presentaban.

MD5 es un algoritmo de 128 bits que toma como entrada un mensaje de tamaño arbitrario y produce como salida un resumen de 128 bits que es representado por un número de 32 dígitos hexadecimales. El algoritmo no sirve para cifrar un mensaje ya que no hay forma de recuperar el contenido original del mensaje a partir del resumen del mismo.

El algoritmo se utiliza para:

- **Integridad del software:** en Internet se usa para proporcionar integridad al software descargado; los desarrolladores publican el resultado del algoritmo MD5 aplicado al archivo en el mismo lugar donde se encuentra la liga de la descarga, el usuario que ha hecho la descarga aplica el algoritmo MD5 al archivo descargado y lo compara con el resultado publicado, si es igual, el usuario puede tener la confianza de que el archivo es el que fue publicado por el desarrollador y que no se trata de software malicioso; esto protege al usuario de posibles caballos de Troya y virus, adicionalmente también sirve como apoyo para validar que la descarga fue completa y que no fue corrompida.

- **Encriptación:** se usa en los sistemas UNIX y Linux para encriptar las claves de los usuarios. Se guarda el resultado del algoritmo MD5 aplicado a la clave del usuario, cuando éste quiere entrar en el sistema se compara el resumen de la clave digitada contra el resumen de la que está guardada en el sistema, si son idénticas la clave es la misma y el usuario es autentificado.

- **Integridad de información:** En forma general se puede decir que el algoritmo se puede utilizar para determinar la integridad de cualquier tipo de información, ya sea correo electrónico, cartas, pedidos, etc.

Ejemplos de la función hash MD5:

Dato	Resumen
FES ACATLAN	64bc124c1b142390e8ff9dbd089fb3f7
FES ACATLAn	13b620286fba4845cf21aa806194d6df
fES ACATLAN	3cc5584837b8e1546fc8f9d3026c6c88
FES ACATLAN	267f1add5fe97063fefed95ca34e46c2
 00001000000103214478.cer	4a3ad6b7320bee9d8fe62a4ceb74b550

Se utilizó el software ***Hashcalc*** para obtener los resultados de los ejemplos anteriores.

La aplicación más extensa de la infraestructura de la PKI está sustentada en los certificados digitales.

Capítulo 3 - Certificados digitales

Los certificados digitales son documentos digitales que hacen posible la identificación de las personas que están realizando trámites electrónicos; es la forma análoga de la identificación oficial que una persona presenta cuando acude a realizar algún trámite. Con el empleo de un certificado digital las personas pueden asegurar a amigos, socios comerciales, entidades financieras y gubernamentales:

- La autentificación del usuario/entidad, al firmarse un documento, en la firma digital viaja la identidad de la persona que lo firma, al validar dicha firma se puede tener la certeza de que la persona que dice firmar el documento, es en realidad quien dice ser.

- La confidencialidad del mensaje, donde el certificado sirve para codificar una comunicación entre dos personas, haciendo que toda la información transmitida sea confidencial.

- La integridad del documento, cuando un documento ha sido firmado puede comprobarse en cualquier momento si el documento ha sido modificado.

- El no repudio del mensaje, una vez verificada la integridad del documento varios participantes pueden agregar sus firmas con el objetivo de aceptar los términos y/o condiciones del documento, mientras que el documento no sea alterado ninguno de los firmantes podrá negar el conocimiento o la aceptación del mismo.

- Firma de software, el certificado también sirve para firmar software, permitiendo a la entidad que va a utilizar el software, garantizar la autoría de la misma, de esta forma no se expone a peligros como: la instalación de software malicioso, alterado o la propagación de virus.

- Identificación para acceso restringido, en la actualidad para tener acceso a un sistema restringido solo es necesario contar con un usuario y un

password, dando como resultado un sistema con muy pobre seguridad, con el uso de los certificados digitales solo el poseedor de un certificado podrá tener acceso a los sistemas con una validación más segura de la identidad de la persona y asignando a este el nivel de privilegios que tendrá dentro del sistema.

Poco a poco el uso de certificados digitales se está volviendo la práctica más común para realizar transacciones electrónicas seguras, sin importar el tipo o la importancia de estas. Para este fin los certificados se basan principalmente en la infraestructura de clave pública (PKI) y solo son útiles si existe alguna autoridad certificadora que los valide y soporte.

Existen dos tipos primarios de certificados de clave pública:

- **Certificados de entidad final:** Se expiden a un usuario o entidad que no es un expedidor de otros certificados de clave pública, básicamente son los certificados digitales que utilizan las personas para realizar sus transacciones electrónicas y no sirve para firmar o dar validez a otro certificado.

- **Certificados de Agencia certificadora:** Es expedido por una agencia certificadora y que la entidad a quien se le expide es otra agencia certificadora y que, por lo tanto, puede a su vez expedir certificados digitales de clave pública. Los certificados de agencia certificadora pueden agruparse en los siguientes tipos:

    - ***Certificado auto expedido:*** Se da cuando el expedidor y la entidad certificada es la misma agencia certificadora, este procedimiento es común cuando se realiza una renovación de clave, donde se pasa la confianza de una clave antigua a una clave nueva, solo las grandes compañías certificadoras pueden llevar a cabo este proceso, ya que cuentan con un gran prestigio y son conocidas en el medio, es decir que hay confianza en el proceso.

- **Certificado autofirmado:** Es un caso especial de certificado auto expedido, en donde se utiliza la clave privada de la agencia certificadora para firmar el certificado correspondiente a la llave privada que está certificando, esto se utiliza principalmente cuando la misma institución firmante requiere de diversos certificados que tendrán funciones muy específicas y diferentes.

- **Certificado cruzado:** Es aquel donde el expedidor y la entidad certificada son diferentes agencias certificadoras, se utiliza para autorizar la existencia de otra agencia certificadora o agencia registradora.

Uso de los certificados digitales

Al contar con un certificado digital este puede ser usado de diferentes formas:

Cifrado

Podemos definir el cifrado como el tratamiento de un conjunto de datos con el fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos, esto constituye la base para la seguridad de cualquier red.

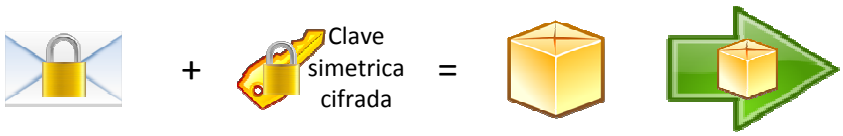
En la infraestructura de clave pública se utilizan claves simétricas y asimétricas para cifrar información donde para cifrar el mensaje se utiliza una clave simétrica que son algoritmos rápidos y posteriormente se cifra la clave simétrica con una clave pública (asimétrica).

1. Tenemos una persona A, que tiene un mensaje, una clave simétrica y una clave asimétrica (puede ser la parte pública o la privada) y tiene que enviar el mensaje cifrado a la persona B.

2. Primero cifra el mensaje con la clave simétrica (por su rapidez) y obtiene un mensaje cifrado, el cual es más vulnerable que si se hubiera hecho con una clave asimétrica (pero este hubiera sido más lento).

3. Cifra la clave simétrica con la clave asimétrica y obtiene una clave simétrica cifrada.

4. La persona A envía el mensaje cifrado y la clave simétrica cifrada en solo paquete a la persona B.



5. La persona B recibe el paquete con el mensaje y la clave simétrica cifrados, adicionalmente posee la pareja de la clave asimétrica.

6. Descifra la clave simétrica cifrada con su clave asimétrica, la cual tiene que ser el par de la clave con que se cifró el mensaje, no la misma.

7. Posteriormente con la clave simétrica descifrada, se utiliza para descifrar el mensaje cifrado, obteniendo el mensaje en claro.

Con este procedimiento se logra que solo el poseedor de la clave privada o pública (asimétrica) pueda descifrar la clave simétrica con la cual podrá descifrar el mensaje.

Firma digital

Las firmas tradicionales nos ratifican el acuerdo que tiene una persona con los términos de un contrato, o cualquier documento en general, esa firma es única y auténtica basada en la forma en la persona firma su nombre, pero puede ser falsificada fácilmente.

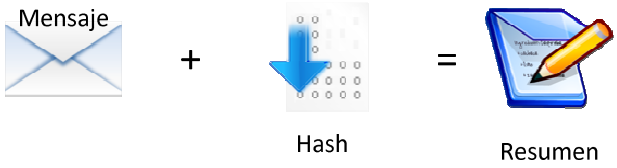
Con el crecimiento de los medios electrónicos de comunicación, también ha crecido la necesidad para crear acuerdos electrónicos donde las partes involucradas tendrán que firmar de conformidad, pero ¿cómo firma un documento electrónico con una pluma? Es aquí donde se utiliza la firma electrónica. La firma electrónica tiene la misma función que la firma autógrafa pero en documentos electrónicos, utilizando diversas tecnologías que permiten al receptor del documento tener la certeza de la identidad de la persona que envía el mensaje y que este no ha sido modificado durante él envió el mismo, donde el mensaje puede ser totalmente legible, es decir que no está cifrado.

La firma digital de un documento no es un password o clave secreta, es el resultado de aplicar un algoritmo matemático, denominado hash (resumen) al contenido del documento, el hash es cifrado con una clave asimétrica (puede ser cualquiera de la dos claves que componen las claves asimétricas) y son enviados tanto el mensaje como el hash cifrado, finalmente el destinatario puede aplicar de nuevo la función al mensaje y compararlo con el hash recibido.

Una firma digital se representa por una extensa e indescifrable cadena de caracteres, esta cadena es en realidad el número obtenido en la función hash.

1. Tenemos una persona A que tiene un mensaje y una clave asimétrica (puede ser la parte pública o la privada) y tiene que enviar el mensaje a la persona B.

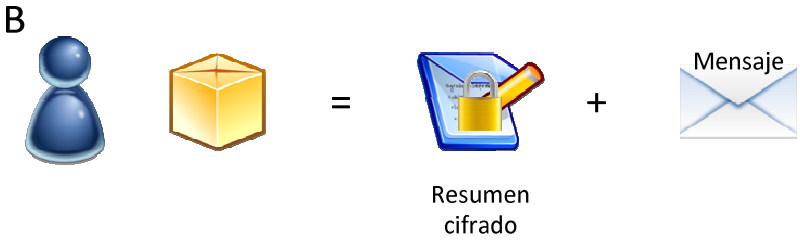
2. Se aplica la función hash al mensaje obteniendo el resumen del mismo.



3. Entonces cifra el resumen del mensaje con la clave asimétrica y obtiene un resumen cifrado.

4. La persona A envía en un solo paquete el mensaje y el resumen cifrado a la persona B.

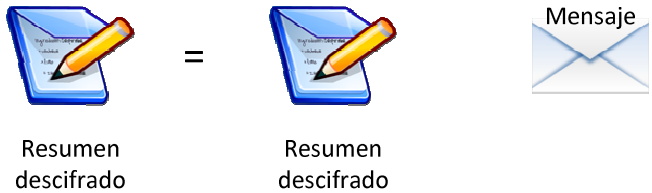
5. La persona B recibe el paquete conteniendo el mensaje y el resumen cifrado, adicionalmente posee la pareja de la clave asimétrica.



6. Descifra el resumen del mensaje con su clave asimétrica (tiene que ser el par de la clave con que se cifró el mensaje, no la misma).

7. Le aplica la misma función hash al mensaje y obtiene el resumen del mensaje recibido.

8. Compara el resumen recibido con el resumen obtenido en el paso anterior, si son iguales, el mensaje es autentificado y se determina que no ha sufrido alteración alguna.



Este tipo de aplicación nos proporciona la certeza que los mensajes recibidos son de las personas que dicen ser y que no han sido modificados e inclusive que no han tenido problemas durante la transmisión del mismo.

Firma de software

Los certificados digitales también pueden ser utilizados para firmar software, permitiendo a la entidad que va a utilizar el software garantizar que es el software original, conocer quién es el creador y, lo más importante, que nadie lo ha modificado; esto garantiza que el software en cuestión no contiene virus y si los contiene, es el propio creador quien los ha incorporado.

Identificación para acceso restringido

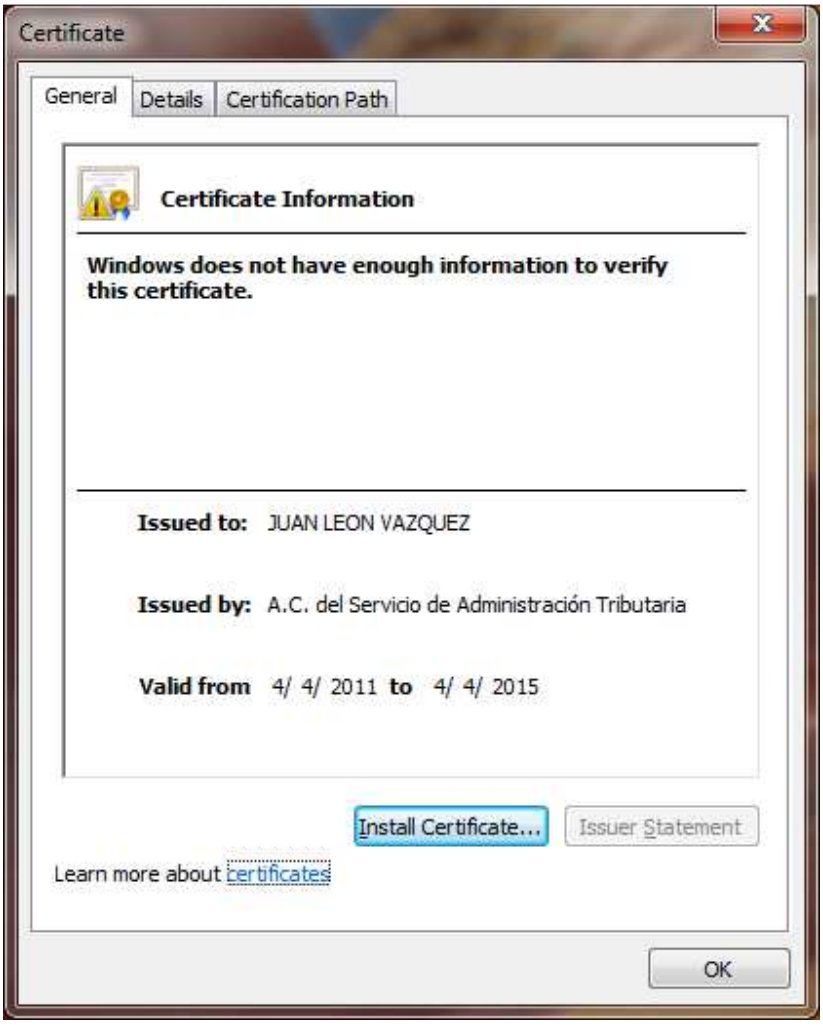
En la actualidad se utiliza la combinación "user" + "password" como el sistema de seguridad más utilizado en los sistemas de información de la mayoría de las empresas llámese intranets, accesos a una red local, a servidores y aplicaciones.

Diversas empresas líderes de tecnología están adaptando sus productos a la tecnología de los certificados digitales, donde el poseedor del mismo tendrá acceso a diversos servicios que están delimitados por el perfil que le sea asignado por el administrador del sistema.

Ya existen productos que sirven para que el usuario pueda guardar un certificado digital de forma segura, entre estos dispositivos se encuentran los usb token, dispositivos parecidos a las memorias usb y que están protegidos por algoritmos simétricos y asimétricos incorporados en un chip especial que esta implementado en el dispositivo.

Certificados estándar X.509

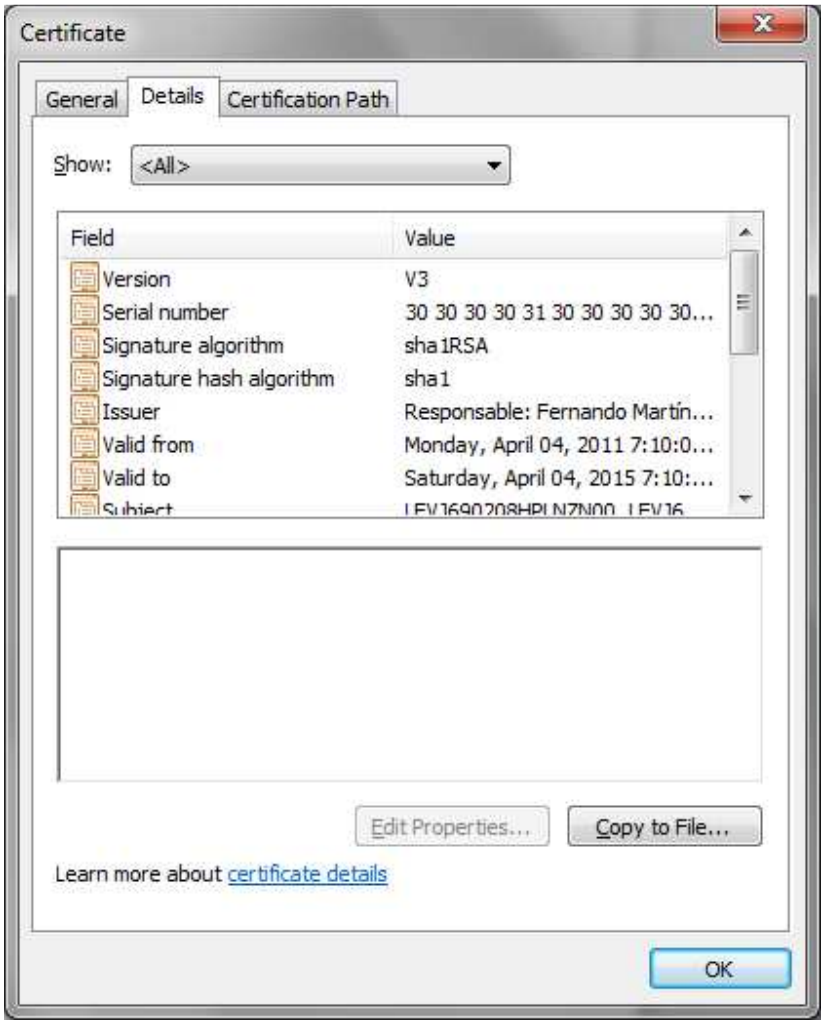
El formato de los certificados X.509 es un estándar creado por ITU-T (Internacional Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IES (International Standards Organización / Internacional Electrotechnical Comisión) publicado por primera vez en 1988.



El estándar se encuentra en la versión 3 y fue publicado en 1996 donde los principales elementos son:

- **Versión:** contiene la versión del certificado utilizado y los valores aceptado son: 1, 2, 3.

- **Número de serie del certificado:** es un número entero y es asignado por la autoridad certificadora que lo expide, el número asignado debe ser único en cada autoridad certificadora, por tal motivo el nombre del emisor y el número de serie identifica a un único certificado.



- **Identificador del algoritmo de firmado:** aquí se identifica el algoritmo empleado para firmar el certificado así como la función de resumen utilizada (md5WithRSAEncryption, sha-1WithRSAEncryption, etc.)

- **Nombre del emisor:** nombre de la autoridad certificadora que ha expedido y firmado el certificado.

- **Periodo de validez:** es el intervalo de tiempo durante el cual el certificado será válido. En este período de tiempo la autoridad certificadora tiene la obligación de informar sobre el estado del certificado.

- **Nombre de usuario o entidad:** identifica la entidad a la que está asociada la llave pública que se encuentra en el campo de información de llave pública del sujeto.

- **Información de llave pública de sujeto:** en este campo se proporciona la llave pública, parámetros y el identificador del algoritmo con el que se emplea la clave (rsaEncryption, dhpublicnumber, etc.).

- **Identificador único del emisor:** es opcional y permite reutilizar nombres del emisor.

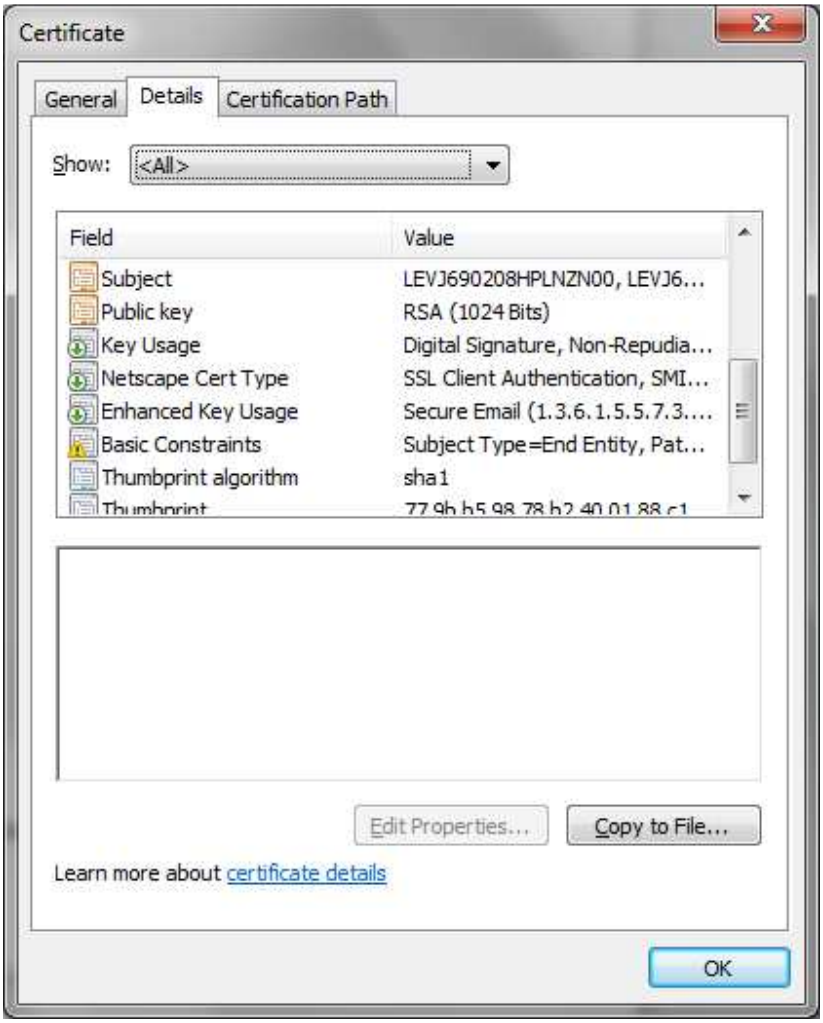
- **Identificador único del usuario o entidad:** es opcional y permite reutilizar nombres del usuario o entidad.

- **Extensiones:** las extensiones proporcionan una manera de asociar información a los usuario o entidades, claves públicas, etc. Un campo de extensión tiene 3 componentes:

    - **Tipo de extensión:** es un identificador de objeto y proporciona el tipo de información (texto, fecha u otra estructura de datos) para el valor de la extensión.

    - **Valor de la extensión:** dato que tiene la extensión.

- **Indicador de la importancia:** es una bandera que indica a una aplicación si es seguro ignorar el campo de la extensión si no reconoce el tipo.



Las extensiones permiten que se puedan crear e implementar aplicaciones que trabajen bajo un entorno seguro utilizando certificados y que pueden evolucionar conforme se agreguen más extensiones. Dentro de las extensiones la ITU y el ISO/IEC han desarrollado y publicado un conjunto de extensiones estándar:

- **Limitaciones básicas:** indica si el usuario o entidad del certificado es una autoridad certificadora y el máximo nivel de profundidad de un camino de certificación a través de la autoridad certificadora.

- **Políticas de certificación:** indica las condiciones bajo las cuales la autoridad certificadora emitió el certificado y el propósito del certificado.

- **Uso de la clave:** se restringe el propósito de la clave pública certificada, indicando el uso que se le debe dar a la misma, por ejemplo: si es para firmar documentos, para la encriptación de datos, etc. Este campo suele marcarse como importante ya que delimita el uso apropiado de la clave pública y cualquier otro uso no estaría validado por el certificado.

Protocolos de certificación o seguridad

Independientemente de los diferentes métodos que existen para cifrar o para obtener resúmenes de documentos, también se han hecho esfuerzos para implementar protocolos de certificación.

Los protocolos de certificación se pueden definir como el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad criptográfica, algunos de estos protocolos de certificación son:

- **SET:** El protocolo fue desarrollado por VISA Y MÁSTERCARD con el apoyo de grandes empresas como IBM, Microsoft, Netscape y otras. El protocolo SET (Secure Electronic Transaction) fue creado con el propósito de asegurar y autentificar la identidad de los participante en las compras efectuadas con tarjetas de crédito en cualquier tipo de red en línea incluyendo Internet, se espera que con este protocolo Internet sea un lugar seguro para efectuar negocios, lo que incrementara paulatinamente

la confianza de los consumidores para realizar compras a través de este medio.

El objetivo primordial del protocolo SET es mantener estrictamente la confidencialidad de la información, garantizar la integridad del mensaje y autentificar la legitimidad de las personas o entidades que participan en una transacción, por lo tanto el protocolo debe:

- Proporcionar la autentificación necesaria entre compradores, comerciantes e instituciones financieras y para conseguir este fin se expiden certificados digitales y se generan firmas digitales para cada uno de los participantes.
- Garantizar la confidencialidad de la información sensible (número de tarjeta de crédito o cuenta, fecha de caducidad, nombre del titular, etc.), lo cual se logra cifrando toda la información.
- Preservar la integridad del mensaje que contiene la información tanto del pedido como de las instrucciones de pago y para tal fin utiliza firmas digitales.
- Definir los algoritmos criptográficos para los servicios anteriores

Los pasos que sigue el protocolo SET para las transacciones son:

- Cuando se va a cerrar el pedido, el cliente recibe la firma digital de la tienda y verifica su validez.
- El cliente envía al comerciante la siguiente información firmada digitalmente:
    - Los datos del pedido: identificación del comerciante, importe y fecha

        - La orden de pago con una encriptación que sólo puede leer el banco.

        - La relación entre el pedido y la orden de pago que los liga indisolublemente.

    - El comercio recibe el pedido y verifica la validez de la firma digital.

    - El comerciante pasa al banco la orden de pago (que él no ha podido leer) con su firma digital.

    - El banco autoriza la transacción y devuelve dos confirmaciones: una para el comerciante y otra para el titular de la tarjeta.

  Con los beneficios y niveles de seguridad que nos proporciona este protocolo, es posible que se extienda su uso en las transacciones por Internet y que evolucione es pos de brindar mejores prestaciones a los participantes.

- **PGP:** Pretty Good Privacy (PGP) desarrollado por Philip Zimermann es uno de los sistemas para encriptación de comunicaciones por Internet más utilizado en el mundo permitiendo el intercambio de mensajes y archivos con confidencialidad y autentificación.

  Combina la funcionalidad de los sistemas de llave pública (RSA) con la velocidad de la criptografía convencional, resúmenes de mensajes para firmas digitales, compresión de datos antes de cifrar, así como una completa gestión de claves, además de ser el protocolo de certificación que mejor implementa las funciones clave pública y que lo convierte en el protocolo más rápido que utiliza cifrado asimétrico.

- **PEM:** (Privacy Enhaced Mail) es un estándar oficial dentro de Internet, proporciona privacidad y autentificación para los sistemas de correo.

  Los mensajes enviados usando PEM son inicialmente convertidos a una forma normalizada, es decir que tengan las mismas características sobre el uso de un espacio en blanco, tabuladores, el uso de retornos de carro y avance de línea

- **SSL:** Secure Socket Layer es un sistema de protocolos de uso general, se basa en la aplicación o uso de criptografía simétrica, criptografía asimétrica, certificados digitales y firmas digitales para conseguir canales o medios de comunicación seguros a través de Internet. Usa la criptografía simétrica como motor principal en la encriptación de los datos transferidos durante la comunicación, aprovechando la rapidez de estos algoritmos, utiliza los algoritmos de criptografía asimétrica para realizar el intercambio seguro de las claves simétricas, logrando la confidencialidad de la información durante la transmisión de la misma. La clave de encriptación simétrica es única y diferente para cada sesión, de tal forma que si una comunicación falla, se debe establecer una nueva sesión SSL y una nueva clave simétrica se generará para la nueva sesión.

  Es el estándar de comunicación más seguro en los navegadores web más importantes como Internet Explorer o Netscape (Protocolo SHTTP), los navegadores implementan un protocolo de negociación para establecer una comunicación segura a nivel socket (nombre de máquina más puerto) de forma transparente para el usuario y a las aplicaciones que las usan.

  La identidad de servidor seguro se consigue mediante el certificado digital, del cual se comprueba su validez antes de iniciar el intercambio de datos sensibles. La integridad de la información se garantiza con la firma electrónica, se crean resúmenes con funciones hash y con la

comprobación de los todos los resúmenes todos los datos enviado y recibidos.

En los modelos de referencia OSI y TCP/IP, SSL se introduce como una especie de nivel o capa adicional, situada entre la capa de aplicación y la capa de transporte proporciona servicios de seguridad a la pila de protocolos, cifrando los datos salientes de la capa de aplicación antes que estos sean segmentados en la capa de transporte, encapsulados y enviados.

Durante el proceso de comunicación segura SSL existen 2 estados fundamentales: el estado se sesión y el estado se conexión. A cada sesión se le asigna un número de identificación arbitrario asignado por el servidor, un método de compresión de datos, una serie de algoritmos de encriptación y funciones hash y una clave secreta maestra de 48 bites. Cada conexión incluye un número secreto para al cliente y otro para el servidor, usados para calcular los MAC de sus mensajes, una clave secreta de encriptación particular para el cliente y otra para el servidor, unos vectores iniciales en el caso de cifrado de datos en bloque y unos números de secuencia asociados a cada mensaje

Certificados de uso comercial

Queda claro que los certificados digitales pueden tener diversos usos, por tal motivo existe una gran cantidad de empresas que tienen el rol de agencias certificadoras en donde se puede tramitar un certificado digital de uso específico. Alguno de estos usos se describen a continuación:

Certificados de Servidor (SSL - Secure Socket Layer

SSL es un protocolo desarrollado por Netscape en 1996, que muy pronto se convirtió en el método más utilizado para asegurar las transacciones de datos por Internet, SSL es una parte integral de la mayoría de los exploradores y servidores Web.

Para establecer una conexión SSL, el protocolo SSL requiere que el servidor tenga instalado un certificado digital que autentifique al servidor antes de establecer la sesión SSL y donde, gracias al certificado, toda la comunicación entre el cliente y el servidor permanece segura cifrando la información que se envían ambas partes.

El certificado digital del servidor permite la "Autentificación Fuerte", donde el servidor puede exigir certificados digitales personales de navegación a los usuarios para acceder a determinados servicios, lo que afecta directamente en la seguridad y la comodidad por la ausencia de un login y password para la identificación de los usuarios.

Certificados digitales personales (correo y navegación)

Los certificados digitales personales proporcionan a su poseedor una herramienta útil para navegar, comprar y enviar/recibir correo a través de Internet de una manera segura. Además otorgan seguridad y confiabilidad a los correos electrónicos basados en el estándar S/MIME ya que con el certificado se puede cifrar y firmar un mensaje de correo electrónico para tener la certeza de que sólo el destinatario del mismo será la única persona capaz de leerlo.

Esto incrementa la seguridad entre un cliente y un servidor de correo ya que ambas partes deben autentificarse para poder comenzar la comunicación conocida como "Autentificación Fuerte".

La "Autentificación Fuerte" puede utilizarse por las empresas para personalizar los contenidos a nivel individual de cada colaborador y así establecer diversos niveles de seguridad.

Certificado para sellado de tiempo

Se utilizan cuando un documento debe tener la hora exacta de su creación, para este fin se utilizan servidores de "Timestamp", estos servidores deben tener una fuente confiable de tiempo, obtenida de servidores de "tiempo" llamados "Stratum".

Cuando queremos sellar un documento, lo primero que tenemos que hacer es aplicar el algoritmo hash, posteriormente enviamos el resumen a un servidor de "Timestamp" que nos devuelve el resumen sellado y firmado. Los servidores de "Timestamp" mantienen actualizadas y accesibles las listas de todos los sellos que emiten para que cualquier persona pueda consultarlas y así garantizar que nadie modifique el sello de tiempo. En las listas solo aparecen los hash de los documentos y es responsabilidad de la entidad que está validando el documento, el aplicar el algoritmo hash para compararlo con el publicado en los servidores de "Timestamp".

Certificados para firmar código (Software)

Los certificados de código sirven para que los desarrolladores o empresas de software puedan firmar su software y distribuirlos de forma segura.

La firma del software por parte de sus creadores debe ser el requisito mínimo de seguridad que deben recibir los usuarios, para confiar y tener la seguridad de que el software que reciben o descargan de Internet, proviene exclusivamente de una empresa determinada. Esto previene los problemas causados por la suplantación de personalidad y la distribución de objetos dañinos o perjudiciales. Cualquier modificación sobre el software original lo invalidará y con ésta información el usuario tendrá los elementos necesarios para rechazar el producto.

Certificados de VPN (Virtual Private Network)

Se utilizan principalmente para que las empresas implementen esquemas de seguridad al proporcionar credenciales electrónicas para autentificar servidores remotos, empleados, socios y clientes, asegurando que el contenido al que tienen acceso es el deseado por la empresa y dejando un claro registro de la actividad que se realizó con el certificado.

Agencias Certificadoras

Es una organización fiable que acepta solicitudes de certificados de entidades o personas valida la identidad, genera certificados y mantiene la información del estado del certificado.

Las labores básicas de las agencias certificadoras son:

- **Admisión de solicitudes:** La agencia certificadora recibe solicitudes de usuarios. La solicitud es una estructura de datos firmada por la agencia certificadora que contiene fecha y hora de publicación y nombre de la entidad donde demandan un certificado digital. La generación de las llaves pública y privada son responsabilidad del usuario o de un software asociado a la agencia registradora.

- **Autentificación del usuario:** Antes de proporcionar el certificado la agencia certificadora debe verificar la identidad del usuario, donde dependiendo del nivel de seguridad deseado, será la documentación solicitada para validar la identidad.

- **Generación de Certificados:** Después de admitir una solicitud y de validar la identidad del usuario solicitante, la agencia registradora genera el certificado digital correspondiente y lo firma con su clave privada, posteriormente es enviado al solicitante.

- **Distribución de certificados**: La entidad certificadora proporciona servicios de distribución de certificados donde diversas aplicaciones tienen acceso y pueden obtener los certificados de sus suscriptores.

- **Anulación de certificados:** El procedimiento es igual al de la admisión de la solicitud, la agencia valida la identidad del solicitante y una vez concluida la validación procede a anular el certificado.

- **Lista de anulación de certificados (Certification Revocation Lists - CRL):** es un mecanismo mediante el cual la agencia registradora pública y distribuye información de los certificados anulados que aún no han expirado a las aplicaciones que lo soliciten.

Agencias certificadoras internacionales

Actualmente existen empresas internacionales que gozan de un gran prestigio como agencias certificados, que se consideran agencias certificadoras raíz y su certificado está avalado por ellos mismos (auto certificado), tales como:

- Verising
- RSA Security Inc.
- Thawte
- beTRUSTed
- VISA

Algunas agencias certificadoras en nuestro país con conexión a la Infraestructura Extendida de Seguridad (IES) son:

- BANXICO
- SECOBAN
- SAT
- INDEVAL
- SECRETARIA DE ECONOMIA

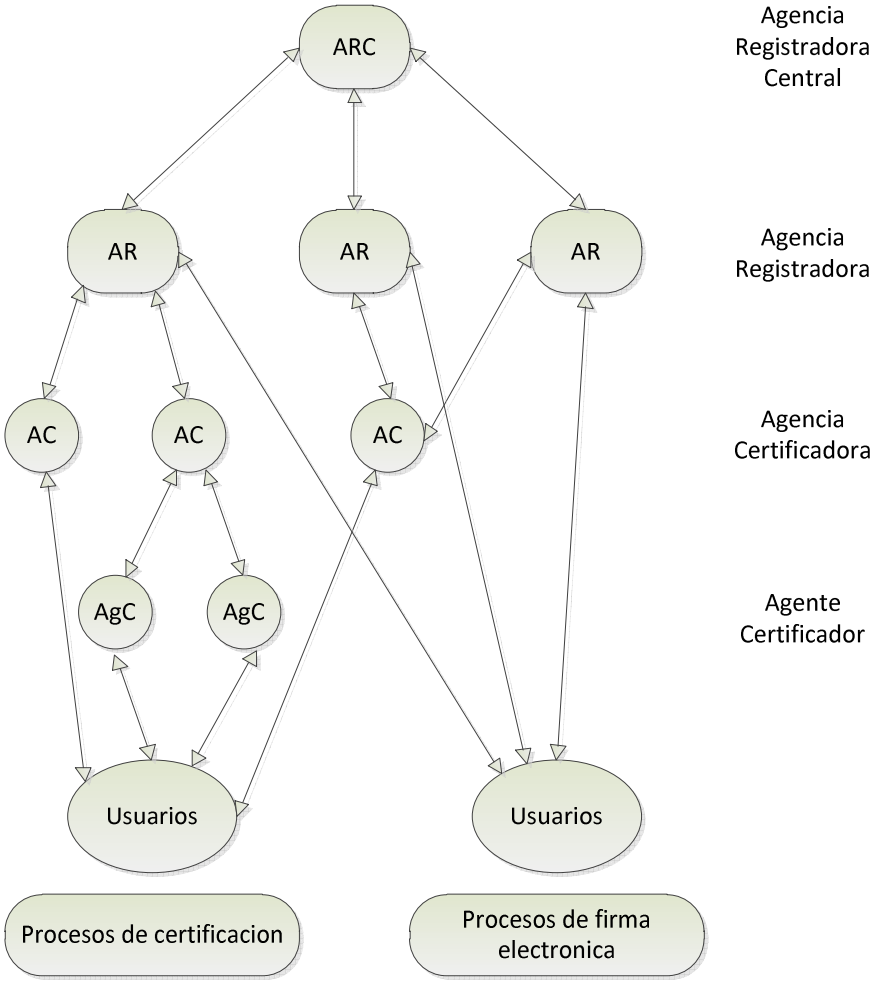
En nuestro país se ha comenzado a hacer esfuerzos para la implementación y uso de los certificados digitales, siendo el Banco de México el principal propulsor.

Capítulo 4 - Infraestructura Extendida de Seguridad (IES)

Estructura IES

La IES es una estructura organizacional creada y administrada por el Banco de México y está pensada para proporcionar seguridad y confianza a las operaciones financieras que se realizan a través de los medios electrónicos en los medios de pago.

El objetivo de la IES es mantener el control de las claves públicas que se utilizan para la verificación de las firmas digitales mediante la expedición y administración de los certificados digitales.



La estructura de la IES es flexible ya que es independiente del sistema criptográfico que se utilice y puede crecer gradualmente cuando se necesite y permite que la administración de las claves quede distribuida entre diversos participantes. Para lograr la distribución se tienen interconectados varios servidores de certificados digitales para proporcionar de forma ágil los requerimientos de los usuarios.

Las principales funciones que desempeña cada participante en la IES son:

ARC – Agencia Registradora Central

Administrar y establecer las normas que rigen a la IES, aplicando las políticas que establezca el Banco de México.

- Crear su propio certificado digital (Auto certificación).
- Certificar a las Agencias Registradoras (AR) y Agencias Certificadoras (AC).
- Garantizar que las claves públicas sean únicas dentro de la estructura.
- Administrar la base de datos de las claves públicas correspondientes a los certificados que las agencias registradoras tengan en sus bases de datos y mantener una liga con las agencias certificadoras que los expidieron.
- Distribuir a través de Internet en la página del Banco de México, su clave pública y las claves públicas de las Agencias Registradoras y las Agencias Certificadoras.
- Crear y administrar las medidas de seguridad para garantizar el buen funcionamiento del sistema.

AR – Agencia Registradora

- Registrar los certificados digitales una vez que la Agencia Registradora Central ha comprobado la unicidad de las claves públicas.
- Administrar la base de datos de los certificados digitales registrados vigentes e históricos.
- Proporcionar información a los usuarios que soliciten a través de medios electrónicos de información respecto a los certificados digitales.
- Revocar certificados digitales, informar a la Agencia Certificadora que los haya emitido y divulgar dichas revocaciones de conformidad con las reglas emitidas por la Agencia Registradora Central.

AC – Agencia Certificadora

- Emitir certificados digitales a los usuarios solicitantes.
- Emitir certificados digitales de las personas que les presten servicios de Agentes Certificadores y proporcionales la acreditación como tales.
- Solicitar a la Agencia Registradora que corresponda la revocación de los certificados digitales que haya emitido, en los supuestos previstos o cuando un usuario lo solicite directamente o a través de un Agente Certificador.
- Auxiliarse de los Agentes Registradores para la realización de sus funciones.
- Responde por daños y perjuicios, que por motivo de sus actividades incurra en el proceso de certificación.
- De la misma manera también serán responsables por los daños y perjuicios que se deriven de la mala función de sus agentes registradores.

AgC – Agente Certificador

- Auxiliar a las Agencias Certificadoras a realizar sus funciones.
- Verificar la identidad de los usuarios que soliciten un certificado digital con base en la documentación oficial que los usuarios presenten para este fin.
- Recibir y verificar la solicitud de certificado digital elaborada por el usuario solicitante.
- Informar a los usuarios solicitantes de certificados digitales los derechos y obligaciones que adquieren al tener un certificado.
- Firma autógrafa del usuario solicitante en una declaratoria donde manifiesta su conformidad con las reglas sobre el uso de firma electrónica.
- Proporcionar al solicitante de un certificado digital los medios necesarios para la generación de datos de creación y verificación de su firma electrónica.
- Generar un pre certificado y solicitar el respectivo certificado digital a la agencia certificadora correspondiente.
- Entregar al usuario su certificado digital registrado, debiendo solicitar al usuario la firma autógrafa de la carta de aceptación del certificado digital
- Informar a los titulares la revocación de sus certificados digitales.

Usuarios

- Solicitar el certificado digital a una Agencia Certificadora o a un Agente Certificador, entregando su requerimiento digital, la documentación oficial

que se le requiera para su identificación y la carta de solicitud (solo si se le requiere).

- Manifestar su conformidad al ser informado de sus derechos y obligaciones a las disposiciones aplicables a la firma electrónica.
- Establecer su frase de seguridad (en secreto) con la que podrá cifrar su llave privada para protegerla.
- Generar en secreto y en forma individual su par de claves (pública y privada) así como los archivos correspondientes.
- Recibir la carta de aceptación de su certificado digital en la que conste su firma autógrafa y su certificado digital ya registrado.
- Mantener en un lugar seguro su clave privada.
- Recordar su frase de seguridad y mantenerla en secreto.
- Solicitar a las Agencias Registradoras la información de los certificados digitales de aquellos usuarios con los que tiene una relación.
- Tener acceso a un servicio que le permita revocar, en línea, su certificado digital en cualquier momento.
- Ser informado por la Agencia Certificadora de las reglas, procedimientos y características de los servicios de certificación y de los certificados digitales

Puesta en Marcha y funcionamiento de la IES

El inicio de operación de la IES comienza con la generación del certificado para la Agencia Registradora Central, llamado certificado raíz y bajo la responsabilidad exclusiva de Banco de México. A continuación se expiden los certificados de la Agencia Certificadora y de la Agencia Registradora operadas por Banco de México y que fueron registrados en la Agencia Registradora Central.

Las Agencias Certificadoras pueden dar de alta los certificados digitales de los usuarios finales solicitantes, mediante el uso de las herramientas informáticas proporcionadas por la IES. Las Agencias Registradoras los registran de forma automática con la autorización electrónica de la Agencia Certificadora y de la Agencia Registradora Central lo que agiliza el alta de los certificados digitales.

El Banco de México tiene que garantizar el funcionamiento de la IES en base a una serie de principios de funcionamiento, para asegurar que ésta opere en un entorno confiable y seguro:

- La implementación técnica del sistema de la IES (el diseño y control del código fuente así como de la configuración inicial de las máquinas en las que se ejecuta dicho sistema) es responsabilidad de la Gerencia de Informática de la Dirección de Sistemas Operativos y de Pagos de Banco de México.

- La operación de los componentes de la IES está asignada a áreas distintas. Esto es, el personal encargado del desarrollo y mantenimiento del sistema de la IES tiene bajo su responsabilidad la administración de la Agencia Registradora Central y el personal responsable de la operación de la IES tiene a su cargo el control de los passwords de acceso a los servidores y a las cuentas de usuario de los equipos que albergan el sistema.

- Los equipos de cómputo que albergan los programas de la IES tienen habilitadas únicamente dos cuentas, una para el administrador del sistema y otra, sin privilegios, bajo la cual se ejecutan los programas de la IES.

- Los archivos de bitácora del sistema son revisados periódicamente para detectar intentos de acceso no autorizados y, en su caso, tomar las medidas preventivas y/o correctivas necesarias.

- El área de desarrollo y mantenimiento de la IES, estableció la configuración inicial de las computadoras en las que se ejecutan los programas de la IES, con los servicios de red deshabilitados, a fin de evitar que alguna persona esté en posibilidad de tomar el control de los sistemas desde un lugar remoto de la red y de limitar los accesos no autorizados que pudieran dañar el sistema.

- Toda modificación a la configuración de los equipos de cómputo de la IES, cambio de versión del sistema IES o sistema operativo, debe ser supervisado y certificado conjuntamente por personal de las áreas competentes de Banco de México.

- El proceso de expedición y registro de certificados de las Agencias Certificadoras y Agencias Registradoras es realizado por el área de desarrollo y mantenimiento de la IES y supervisado por el área de operación para verificar que se den de alta sólo aquellas agencias que cumplan con los lineamientos establecidos en las disposiciones aplicables.

- Sólo se realizan conexiones a través de la red de telecomunicaciones con los servidores de la IES que estén debidamente documentadas y se supervisa periódicamente que no existan conexiones no autorizadas.

- Los programas de la IES únicamente pueden crear, abrir o modificar archivos que estén claramente especificados de los cuales se conozca su contenido y esté de acuerdo con la documentación del sistema. Dichos programas son verificados periódicamente para garantizar el cumplimiento de la condición antes referida.

- Se cuenta con una copia de los resúmenes digitales de los programas ejecutables de la IES, con el objeto de verificar en cualquier momento, que las versiones ejecutables en producción no han sido modificadas sin la autorización correspondiente.

- Existen planes de contingencia del sistema de la IES los cuales son probados periódicamente. Dichos planes consisten en mantener un respaldo diario de la información de la base de datos, copiándolo tanto a un servidor alterno, como en una cinta magnética. Así mismo, se mantiene un esquema de cluster de alta disponibilidad con dos nodos para la Agencia Registradora Central, de manera que si se llegara a perder el nodo activo, inmediatamente entraría en operación el nodo alterno. Además todos los servidores de la IES cuentan con arreglos de discos en espejo y notificaciones para que, en caso de falla de alguna parte del equipo se pueda actuar de manera pronta y expedita y no se pierda la información.

- Personal de la Gerencia de Trámite de Operaciones Nacionales de la Dirección de Trámite Operativo y de la Gerencia de Informática de la Dirección de Sistemas Operativos y de Pagos revisa periódicamente los controles de funcionamiento implementados en la IES, descritos en el presente documento.

Con estos principios se logra la seguridad de los equipos de cómputo, la integridad del software, la confidencialidad de la información y la continuidad de la operación en la IES.

Uso de la IES

Para obtener un certificado digital de la IES como puede ser la Firma Electrónica Avanzada (FEA) hay que cumplir primeramente con una serie de requerimientos:

- Tener obligaciones fiscales y estar inscrito en el Registro federal de Contribuyentes.
- Contar con la Clave Única de Registro de Población (CURP).
- Posteriormente se tiene que seguir el siguiente procedimiento.
- Solicitar una cita al centro de atención telefónica del SAT:

  01-800-INFOSAT

  01-800-463-6728

El solicitante puede elegir día, hora y lugar donde realizará el trámite (existen 73 puntos de atención).

- Descargar de la página del SAT, la aplicación de "Solicitud de certificados digitales" llamado SOLCEDI, que generara un archivo de acuerdo a las instrucciones que le proporcionaron cuando solicitó la cita por teléfono.
- Acudir puntualmente a la cita programada con la siguiente documentación (todo en original o copia certificada y copia fotostática):
  - Acta de nacimiento, carta de naturalización o documento migratorio vigente.
  - Identificación oficial.

- Comprobante de domicilio fiscal.
- Llevar en un medio de almacenamiento el archivo con extensión "REQ", el cual se generó junto con la llave privada a través de la aplicación SOLCEDI.
- Llevar debidamente lleno el formato impreso solicitud de certificado de Firma Electrónica Avanzada

Firma Electrónica Avanzada (FIEL)

Podemos definir a la firma electrónica avanzada como un conjunto de datos, los cuales son adjuntados a un mensaje electrónico con el propósito de identificar al emisor del mensaje como el autor legítimo del mismo, es el símil de la firma autógrafa.

La firma electrónica avanzada es una herramienta que proporciona una serie de medidas de seguridad a las transacciones electrónicas que se realicen entre los contribuyentes y el SAT ya que permite:

- Verificar que los mensajes no han sido modificados.
- Identificar el autor del mensaje.

La firma electrónica avanzada se basa en los estándares internacionales de claves públicas, específicamente en el estándar X509v3 para la creación de certificados digitales.

La Firma Electrónica avanzada permite "firmar" o asegurar diversas transacciones que el Servicio de Administración tributaria (SAT) tiene a disposición de los usuarios o que irá liberando gradualmente como son:

- Generación de Factura electrónica.
- Generación de Pedimentos.
- Declaraciones anuales.
- Declaraciones provisionales.
- Dictámenes.
- Avisos al RFC.
- Devoluciones.

- Registro de operaciones financieras

Estas son las dependencias gubernamentales y órganos desconcentrados que utilizan firmas electrónicas para la realización de trámites de forma remota:

- Banco de México
- Secretaría de la Función Pública
- Secretaría de Economía
- Instituto Mexicano del Seguro Social
- Instituto para el depósito de valores

INDEVAL

El instituto para el depósito de valores (INDEVAL) es una institución privada que cuenta con la autorización para operar como el depósito central de valores, proporcionando los siguientes servicios:

Custodia y administración de valores:

Se encarga de administrar todos los instrumentos financieros almacenados en las bóvedas física y electrónica, asume la responsabilidad por los valores en depósito.

- Guarda física de los valores y/o su registro electrónico en instituciones autorizadas para este fin.
- Depósito y retiro físico de documentos de las bóvedas de la institución.
- Inmovilización de documentos.
- Custodia centralizada de todos los valores inscritos en el registro nacional de valores e intermediarios (títulos bancarios, títulos gubernamentales, títulos de deuda privada y acciones) que son negociados en el mercado financiero a través de la BMV o fuera de ella
- Ejercicio de derechos en efectivo: dividendos en efectivo, pago de intereses y amortizaciones
- Ejercicio de derechos en especie: capitalizaciones, canjes, conversiones y splits.
- Ejercicio de derechos mixtos: suscripciones

Operación nacional

- Transferencia electrónica de valores
- Transferencia electrónica de efectivo
- Compensación de operaciones y liquidación
- Liquidación de operaciones (de diversos plazos) para el mercado de dinero (directo y reporto) y mercado de capitales (operaciones pactadas en la bolsa mexicana de valores)
- Administración de colaterales

Operación Internacional

- Liquidación de operaciones en mercados internacionales
- Administración de derechos patrimoniales de emisiones extranjeras
- Administración de impuestos sobre acciones estadounidenses

Servicios de Información

- Asignación de códigos ISIN a emisiones
- Servicios a emisoras

INDEVAL tiene en marcha diversas acciones encaminadas a mejorar los servicios que actualmente presta a los diferentes intermediarios financieros, el principal reto de la institución es la de implementar un nuevo sistema de liquidación basado en

estándares internacionales que le permitan operar de forma transparente con cualquier agente financiero internacional.

Los estándares utilizados para la implementación del nuevo sistema de INDEVAL son básicamente 2:

- Mensajes ISO 15022 como componente principal para la creación de mensajes financieros que pueden ser interpretados por cualquier institución mundial que utilice el estándar, este estándar es usado actualmente por la principal red financiera mundial llamada Swift.

- Uso de certificados digitales para la autenticación de los mensajes, estos certificados son proporcionados por el SAT o Banxico y son comúnmente llamados "Fiel", es decir que utiliza la infraestructura de llave pública de Banxico.

La implementación de la infraestructura de llave publica de Banxico, al nuevo sistema de INDEVAL nos muestra lo importante que estas tecnologías se están volviendo para crear un clima de tranquila para todo el sector financiero, actualmente INDEVAL ha liberado la primera fase de su nuevo sistema, en esta primera fase ya se están firmando digitalmente todas las operaciones bursátiles que se están operando día a día.

Conclusiones

A través de la firma electrónica tanto entidades gubernamentales y empresas privadas podrán agilizar el envío y recepción de documentación, reduciendo el tiempo de los procesos y mejorando los mecanismos de intercambio de información, brindarán protección, integridad y autenticación a los documentos. De igual forma ayudará a la reducción de contaminación ambiental y los costos a las empresas en papel, horas hombre y mensajeros.

A pesar de los grandes beneficios que brinda el uso de la firma electrónica, hoy en día sólo cuatro estados de la República cuentan con un marco jurídico sobre su uso:

- Guanajuato
- Sonora
- Hidalgo
- Querétaro

Es indispensable crear un marco jurídico para todo el país que proporcione un sustento legal a la firma electrónica, tal y como se le otorga a la firma autógrafa, con esta medida se impulsará a que cada vez más empresas privadas y estatales la utilicen para llevar a cabo casi cualquier trámites.

Asimismo eliminar la brecha digital existente para que los medios electrónicos estén al alcance de todas las personas y como última instancia, pero no por eso menos importante, crear confianza y costumbre en el usuario.

Finalmente, este trabajo representa en gran parte mi capacidad para integrarme a la vida laboral, donde las herramientas más importantes han sido la investigación y el análisis, ya que me han permitido abordar temas que no domino o desconozco, y que gracias a mi formación como Matemático Aplicado, puedo elaborar

propuestas de mejoras, soluciones integrales o simplemente dar recomendaciones para diversos escenarios, con el fin de realizar implementaciones más eficaces y eficientes.

Bibliografía

Garfinkel, Simson (1999). Seguridad y comercio en el WEB. McGraw Hill/Interamericana. España

Harrington, Jan l. (2006). Manual práctico de seguridad de redes. Anaya multimedia. Madrid.

Oppliger, rolf (1998). Sistemas de autentificación para redes de seguridad. Alfaomega. Madrid

Reyes Krafft, Alfredo Alejandro (2003). Editorial Porrúa. México

AMECE

http://www.amece.org.mx/amece/fype/content.php?id=20

BANXICO

http://www.banxico.org.mx/tipo/disposiciones/bancos/cir6-2005.htm

http://www.banxico.org.mx/tipo/disposiciones/bancos/cir19-2002_compilado.html

Ciberhabitat

http://ciberhabitat.gob.mx/comercio/factura/index.html

INVEDAL

http://www.indeval.com.mx

ISO/IEC

http://www.standardsinfo.net/isoiec/index.html

ITU

http://www.itu.int

http://www.itu.int/rec/T-REC-X.509/es

SAT

http://www.sat.gob.mx/nuevo.html

http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_6651.html

http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_6622.html

http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_6627.html

http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_6701.html

http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_6626.html

http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_6695.html

http://www.sat.gob.mx/sitio_internet/e_sat/comprobantes_fiscales/15_6542.html

http://www.sat.gob.mx/sitio_internet/e_sat/comprobantes_fiscales/15_6522.html

http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_1472.html

UNAM

http://www.enterate.unam.mx/Articulos/2003/junio/facelec.htm

Wikipedia

http://es.wikipedia.org/wiki/X.509