Objetivos de la criptografia  
Agregar listas de revocacion  
Crear certificados con la entidad certificadora  
Crear certificados con IIS  
Analiar aspectos de un crtificado  
¿Que hace que un certificado sea valido?  
Pasos para generar un certificado  
Objetivos de un certificado

Objetivos de la criptografía

Es curioso como casi todos los elementos en los que se basa en internet se crearon de una manera más o menos insegura en la que cada elemento viajaba por la red si ningún tipo de protección, libres para que cualquiera pudiera leer su contenido. Esto fue así, hasta que entro en juego la **criptografía**.

Muchas veces la gente no es consciente de la información personal, privada y secreta que viaja a través de sus computadoras o celular, o si lo es no le da importancia requerida. El tema es que es realmente importancia limitar el acceso a nuestra información, porque nunca sabemos que consecuencia podría tener que un extraño acceda a nuestro teléfono, nuestras fotos o mensajes, lo que para nosotros es inofensivo para otras personas abren posibilidades de extorsión o estafas en contra nuestra.

La criptografía garantica que solo nosotros (u otras personas autorizas) puedan acceder a nuestra información, de forma que sepamos que lo que sale de nuestros dispositivos, está debidamente protegida, y es confidencial.

La criptografía es un conjunto de técnicas y métodos en que los que un mensaje origen (o en claro) con información confidencial, se convierte en otro sin aparente significado y que puede viajar por medios no seguros, con la tranquilidad de que el mensaje original no podrá ser descubierto, sin aplicar los correspondiente métodos criptográficos sobre el mensaje original.

La criptografía existe desde hace muchos siglos, siempre asociada al envió de mensaje secretos entre dos partes. Algunos sistema de criptografía antiguos, se basan en la ocultación del método criptográfico. En los sistemas criptográficos modernos, el método de inscripción es público (o podría serlo sin comprometer la seguridad) y al mismo tiempo poseen una clave de encripción que debe ser secreta, y que si la cual aunque tengamos el algoritmo y el mensaje cifrado, no conseguiremos tener el mensaje original.

Las herramientas y métodos involucrados en la criptografía se usan en los siguientes aspectos:

Integridad

Garantiza que la información no ha sido alternada y es tal cual se genero. Este proceso se hace realizando una serie de operaciones matemáticas sobre la información, dando como resultado un numero, casi único, al que solo se puede llegar, realizando los mismos cálculos sobre la misma información. El número resultado de estas operaciones se le conoce como “resumen” o mas comúnmente como “hash”, cuanto mayor sea este numero, mas seguridad ofrece.

Algunos algoritmos de integridad son:

CRC, CRC32, MD5: Algoritmos actualmente obsoletos que no debiera usarse actualmente

Familia de algoritmos SHA: Conjunto de algotimos de hash, que poseen con subfamilias SHA1, SHA2, SHA3, con las siguientes características:

SHA1: Genera un numero de 160 bits, actualmente considerado no seguro:

SHA256 y SHA512: Genera un numero de 256 y 512 bits respectivamente, considerados seguros actualmente.

Uno de los problemas de problemas de estos algortimos, son las colisiones, esto el hecho que se puedan genera dos hash iguales para distinta información, lo cual permite “adulterar” la información que se desea transmitir. El otro problema es que se pueda llegar a la información original a través del hash, lo cual puede ser un fallo de seguridad importante en el caso que la información original sea un password, o un clave simetrica de encriptación.

Confidencialidad:

Es la posibilidad de enviar información desde el punto A al punto B garantizando que solo el emisor y el receptor puedan acceder a ella. En un ambiente inseguro desde su concepción como internet, es fundamental poder disponser de herramientas que nos permitan enviar información privada de forma segura. Considerese que nuestra información confidencial tal como datos biométricos y de salud, datos personales como nuestra direcciones, contactos y realizacon o datos económicos como nuestras tarjetas de crédito están constantemente viajando por internet. Generalmente se garantiza la confiderencialidad mediante la encriptación, la cual se realiza a través de la una seria de transforamcion de la información, usando una llave de determinados tamaño.

Algoritmos que confidencialidad son:

AES: Usando tamaños de llave de 128, 192 o 256 bits. Se usa la misma llave para encriptar y para desencriptar.

RSA: Usando tamaño de llaves de 1024 (considerado obsoleto), 2048, o 4096. Se usa una llave diferente para encriptar y otra para desencriptar.

Identitidad

Es lo que nos permite garantizar que la persona (o maquina) con la que estamos intarcambiando información es realmente quien dice ser.

En estos caso se usa criptogrifia asimétrica, y principalmente certificados.

La identidad también nos ayuda a implementar el principio de “no repudiación” esto es que la persona o sistema que realiza una operación no puede negar haberla realizado.

**Criptografía simétrica**

Tanto el recepto del mensaje encriptado, como la persona que encripta, usan la misma clave de encripción para realizar sus operaciones. Algoritmos que lo usa son por ejemplo AES (Rijndael).

Las **ventajas** de este método son:

* Es la practica tiene una velocidad aceptable
* Es muy seguro

Las **desventajas**:

* La principal desventaja es que un usuario genera la clave y tiene que pasársela a otro usuario, lo cual podría comprometer la conexión desde un inicio

El hecho que compartan la misma clave, es un problema, el único que tiene este tipo de criptográfica, porque ¿Cómo se hace que el usuario final y destino tengan la misma clave?, solo enviando la clave por un medio que sea seguro, para garantizar que nadie más la tiene, pero precisamente necesito intercambiar la llave porque no tengo un medio seguro para enviar información.

**Criptografía asimétrica**

Consta de dos claves, en lugar de una, llamadas clave privada y clave pública, la clave pública sirve para encriptar, y es de libre acceso, la clave privada para desencriptar y solo la tiene una persona (la que genero las claves). Además la privada sirve para firmar mensajes y garantizar que la persona que la usa es el dueño de la clave.

En la práctica funciona así: Una persona genera (a través de un algoritmo) una clave privada y pública (que se complementan entre sí), se queda para si la clave privada, y distribuye la clave pública (a quien desee), a partir de ese momento, quien desee mandarle un mensaje encriptado, puede hacerlo usando la clave pública, y solo el podrá desencintarlo usando la clave privada. Igualmente si él quiere mandar un comunicado y garantizar su autenticidad, podrá firmarlo con su llave privada, y todo aquel que tenga la llave publica, podrá validar su origen.

Algoritmos que implementan esta tecnología son por ejemplo RSA o DSA.

Las **ventajas** de estos algoritmos son:

* Seguridad en cuanto al custodio de las claves (nunca se difunde la clave privada)
* Seguro en cuanto los mecanismo de inscripción

Las **desventajas:**

* Increíblemente lento

En esta criptografía se resuelve el problema de la llave compartida, puesto que al haber dos llaves, se puede distribuir libremente la llave pública (a cualquier persona) para encriptar, y la permanecer debidamente custodiada la llave privada para desencriptar. Así por ejemplo dos personas (o entes), pueden iniciar una comunicación segura, simplemente intercambiando sus llaves públicas y usando sus llaves privadas para desencriptar.

Debido a que la criptografía asimétrica es realmente lenta, en lugar de encriptar un mensaje completo, se genera una llave simétrica aleatoria, con la que se encripta el mensaje y se envía el mensaje encriptado y adjunto con la llave simétrica encriptada (ahora sí) con la llave asimétrica publica, lo cual garantiza la velocidad y la confidencialidad.

**Certificados digital**

Cuando recibimos un mensaje firmado con una llave privada, podemos validar su autenticidad con nuestra llave pública. Esto quiere decir que podemos garantizar que la persona que tiene la llave privada es la se está comunicado, con nosotros, puesto que debe coincidir con la llave publica que nos proporcionó.

Hay que agregar que la firma es diferente por cada mensajes, por lo que garantiza no solo que el mensaje fue enviado por quien tiene la llave privada, sino además que el mensaje no ha sido modificado en el cambio.

Un detalle importante es que solo garantiza eso, es decir que el mensaje fue firmado con la llave privada, pero no garantiza que esa firma electrónica pertenezca a una persona en particular. La firma podría ser de cualquier persona, y haberse generado en cualquier momento.

Para garantizar además que la firma privada pertenece a una determinada persona o entidad, se usan los certificados, que bien pueden identificar a una persona o a un ente como una empresa o un banco.

Pero, ¿En que consiste exactamente un certificado? Imaginemos que yo quiero comunicarme (a través de una computadora) con otra persona o entidad, por ejemplo una tienda. Con el uso de llaves públicas (y privada) garantizo que la comunicación es confidencial entre ambos, pero de ninguna forma garantizo que esa llave pertenezca a la tienda, pero igualmente imaginemos que existe un tercer elemento, un ente en el que confiamos los dos (la tienda y el usuario), que garantice que esa llave privada pertenece a la tienda, ¿Cómo lo puede hacer? Dando por supuesto que yo confió en el tercero, que se llama entidad certificadora, esta firma (con su propia llave privada), la llave publica y demás información de la tienda, posterior a que valide la identidad de la tienda (mediante documentos, escrituras, registros de empresa, visitas en persona). En este punto ya tenemos un certificado, que contiene la llave pública, y que está firmado por alguien en el que confiamos que ha validado correctamente la identidad de la tienda, de esta forma queda ligada la identidad con la llave pública.

¿Quién son esas entidades certificadoras y por qué confiamos en ella? Son grandes empresas cuyo servicio es precisamente ese garantizar la identidad de entes y personas, y son aceptadas a nivel mundial como VERISIGN, o incluso gobiernos o entidades gubernamentales que realizan dicha función.

## ¿Cuál es proceso para generar un certificado?

1. Se genera un par de llaves (pública y privada)
2. Se realiza una petición de generación de certificado en base a la clave pública, y a los datos de la empresa (y los host que queremos certificar).
3. Se envía la petición a una entidad certificara, que realizara los pasos necesarios para garantizar que somos la empresa para la cual estamos pidiendo los certificados, y una vez garantizado nos expedida dicho certificado.
4. En nuestro servidor podemos unir la llave privada con el certificado, y en base a eso configurar nuestros servidores para que lo usen apropiadamente

Nuestro clientes al conectarse a nuestros servidores descargaran el certificado (con la llave publica), y al estar firmado por la entidad certificadora (en la confiamos), asumiremos que el servidor al que nos estamos conectando es el correcto. Igualmente si no está firmado o lo está por alguien en que no confiamos seremos advertidos de esta situación, y estará en nuestra decisión continuar la comunicación con dicho servidor.