Técnico en

DESARROLLO DE SOFTWARE

Seguridad Informática

Instituto Von Neumann

Introducción a la criptografía

Unidad V

1. Introducción a la criptografía

La facilidad con que la información se transmite a través de cualquier medio hace que implícitamente exista la necesidad de restringir la facilidad de obtener la información, esto se logra a través de la criptografía, esto nos permite lograr el objetivo anterior cifrando la información.

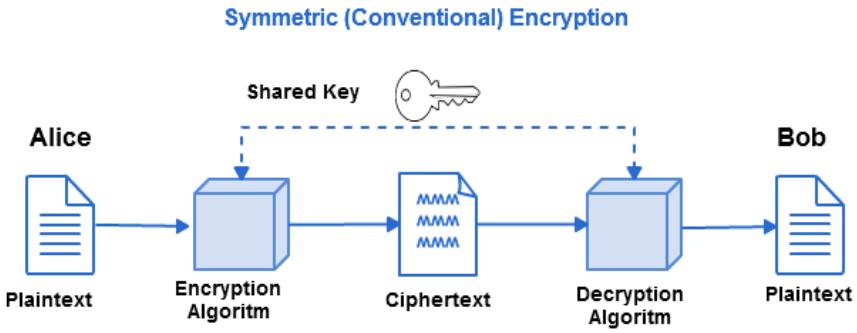
La criptografía nos permite obtener confidencialidad, comprobar integridad y proveer autenticidad, facilitando el convertir texto plano (entrada) en cifrado (salida).

2. Métodos de criptografía

La criptografía se divide en 3 métodos utilizados en la actualidad en diversas aplicaciones y para diferentes objetivos:

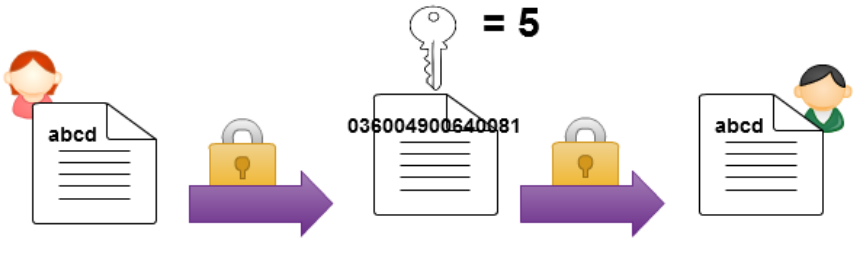
1. Criptografía simétrica.
2. Criptografía asimétrica.
3. Criptografía híbrida.

Criptografía simétrica



La criptografía simétrica utiliza una única clave para cifrar y descifrar la entrada, esto significa que se debe conocer la clave tanto del que cifra como el que descifra, esto a su vez, también representa una vulnerabilidad porque la clave se debe transmitir.

Ejemplo de criptografía simétrica



Donde:

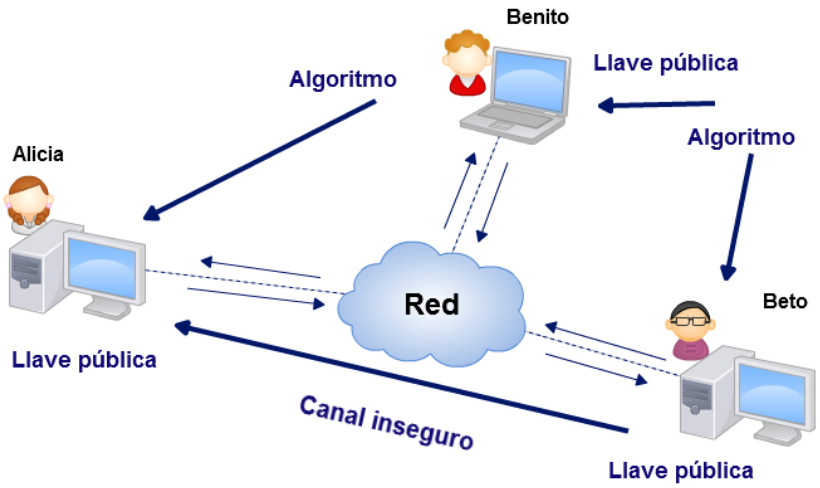
a = 0001
b = 0002
c = 0003
d = 0004
. . . .

a "cifrada" = 0036 = (valor numérico de "a" + clave)^2

0036 "descifrado" = a = $\sqrt{\text{valor cifrado}}$ - clave

Criptografía asimétrica

La criptografía asimétrica utiliza dos claves, la primera: la pública, que como su nombre lo indica puede ser difundida libremente, y la privada: que la debe contener únicamente la persona que se desee abra el mensaje.



El receptor que desea recibir un mensaje debe enviar la clave pública la cual está relacionada con nuestra clave privada y así el emisor cifra el mensaje utilizando la clave pública, obviamente como la clave pública fue generada por la privada solo esta última podrá tener acceso al mensaje.

Criptografía híbrida

La criptografía híbrida únicamente utiliza las ventajas de la simétrica y asimétrica para sacar el máximo provecho de ambos métodos.

1. El receptor: crea su clave pública y privada.
2. El emisor: cifra el archivo (simétrica).
3. El receptor: envía la clave pública.
4. El emisor: cifra la clave que ha sido usada para cifrar el archivo con la clave pública que envía el receptor.
5. El emisor envía el archivo y envía la clave simétrica cifrada con la clave asimétrica pública que envió el receptor para que este pueda obtener acceso al archivo de forma más rápida y a la vez segura.

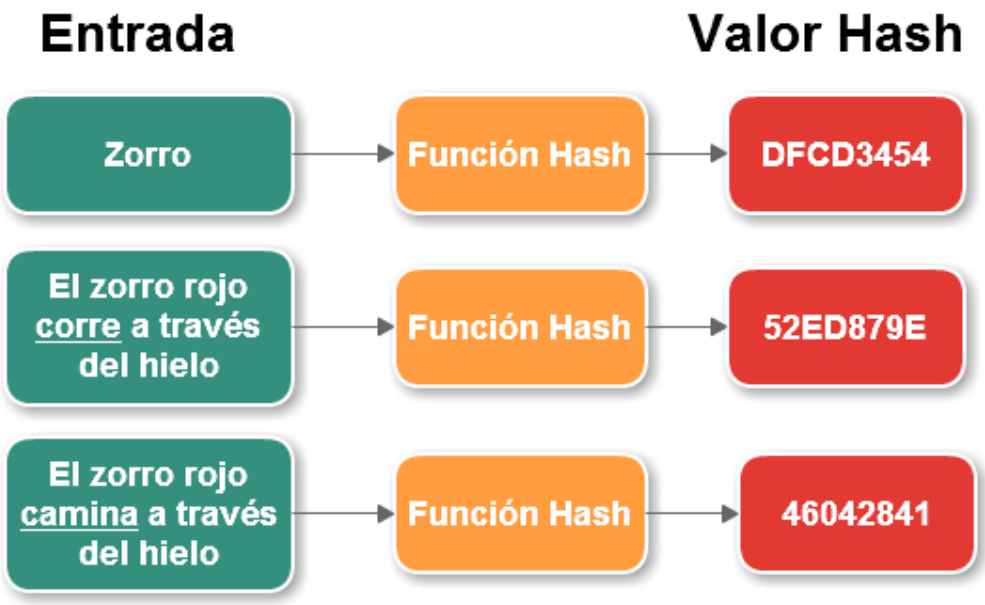
Funciones Hash

En criptografía una función hash es un algoritmo que crea a partir de una entrada una salida alfanumérica de longitud constante dependiendo del algoritmo.

1. Su longitud según su algoritmo es constante, sin importar el tamaño de la entrada.
2. Son funciones unidireccionales, es decir solo pueden cifrar la entrada, pero no se puede descifrar.
3. Representan colisiones, es decir una entrada podría producir la misma salida que otra entrada totalmente distinta.

Para poder usar las funciones Hash primero debemos saber que para poder comprobar la información utilizaremos la misma técnica, es decir cifraremos nuestro texto con el mismo algoritmo para saber si la información que ya poseemos coincide con la nuestra.

Las funciones Hash se utilizan para comprobar contraseñas ya que una vez implementado el usuario es quien va a demostrar que la contraseña que el provee es la misma que la contraseña que se encuentra almacenada.



Las funciones hash proveen una característica que puede ser aprovechada, debido a que una entrada determinada provee una salida única, cualquier alteración en la entrada repercutiría en la salida, esto sirve para saber si la información enviada es exactamente la misma que la recibida. Por lo cual permiten crear firmas digitales para los documentos electrónicos.

3. Algoritmos de criptografía

Algoritmos de criptografía simétrica

DES: Este algoritmo es muy utilizado en varios tipos de entorno aplicativos, tanto así que paso a ser un estándar para cifrar la información del gobierno de los Estados Unidos en 1976. Este algoritmo utiliza el cifrado por bloques, la entrada que se provee en una determinada longitud y cantidad de bits determinada para producir una salida cifrada también con la misma longitud.

AES: A diferencia de DES este algoritmo no es un prototipo del cifrado por bloques sino una implementación plena y mejorada del mismo. Es uno de los algoritmos de este tipo de criptografía más popular y ampliamente utilizado. El funcionamiento de DES motivo a la investigación y mejoramiento de este algoritmo que rápidamente fue tomado como nuevo estándar debido a su efectividad. AES puede trabajar en bloques de 128, 192 o 256 bits, este es un dato muy importante a la hora de llevarlo a la implementación ya que esto no hará pensar en los siguientes factores: efectividad, complejidad y demora en el proceso.

RC4: Este algoritmo es utilizado por los protocolos de redes TLS/SSL y sirve para encriptar las conexiones, además de eso se puede utilizar como un algoritmo efectivo. Existen los algoritmos RC2, RC5 y RC6, estos dos últimos como versiones mejoradas. Es un algoritmo que inicialmente estaba registrado para su uso privado, pero a raíz de una filtración paso a ser conocido públicamente.

IDEA: Es un algoritmo altamente efectivo para pensar en su posible implementación debido a su alta seguridad, esto dado a que se debe probar 10^38 claves para poder encontrar una clave, pero esto es imposible en la práctica debido a la capacidad de los ordenadores actuales.

Blowfish: Este algoritmo de codificación es muy poco utilizado en sí, pero es utilizado como combinación con otras implementaciones de algoritmos ya sea para mejorar la velocidad o la eficiencia.

Algoritmos de criptografía asimétrica

RSA: Este es el algoritmo más utilizado de este tipo. Cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

Algoritmos de función Hash

MD5: Es uno de los algoritmos más populares para poder comprobar integridad y para contraseñas, sin embargo, se conocen algunas colisiones por lo que a la hora de implementar este algoritmo no se toma en cuenta en las aplicaciones que requieren un mayor nivel de seguridad.

SHA-512: Debido a su flexibilidad como un algoritmo de reducción en cuanto a su variabilidad de tamaño debido a su implementación lo convierte en un algoritmo muy viable en aplicaciones que requieren un nivel elevado de seguridad.

Tiger: Por su previsión de eficiencia para plataformas de 64 bits se debería de pensar mucho en implementar esta función Hash en aplicaciones para aprovechar su diseño, también debemos recordar que tiene las versiones de 128 y 169 bits independiente a la versión original que es de 192 bits.

Whirlpool: Este algoritmo se debe implementar pensando en que es parte del estándar ISO y que cuenta con varias versiones.

RIPEMD: Es un algoritmo poco popular desarrollado abiertamente, esto no es malo del todo debido a que al no ser tan popular puede ser utilizado como una ventaja.

Referencias y contenido adicional para revisar

- https://docs.oracle.com/cd/E24842_01/html/E23286/secov-4.html
- http://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des
- http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
- http://es.ccm.net/contents/criptografia-1747462277
- http://es.ccm.net/contents/126-criptografia-de-clave-privada-o-clave-secreta
- http://es.ccm.net/contents/127-sistemas-de-clave-publica
- http://es.ccm.net/contents/130-introduccion-al-cifrado-mediante-des
- http://es.ccm.net/contents/134-cifrado-por-medio-de-rsa
- Hodeghatta Rao, U., & Nayak, U. (2014). *The InfoSec Handbook*. New York: ApressOpen.

Descargo de responsabilidad

La información contenida en este documento descargable en formato PDF o PPT es un reflejo del material virtual presentado en la versión online del curso. Por lo tanto, su contenido, gráficos, links de consulta, acotaciones y comentarios son responsabilidad exclusiva de su(s) respectivo(s) autor(es) por lo que su contenido no compromete al área de e-Learning del Departamento GES o al programa académico al que pertenece.

El área de e-Learning no asume ninguna responsabilidad por la actualidad, exactitud, obligaciones de derechos de autor, integridad o calidad de los contenidos proporcionados y se aclara que la utilización de este descargable se encuentra limitada de manera expresa para los propósitos educacionales del curso.