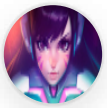


Belen_Dominguez
www.wuolah.com/student/Belen_Dominguez

Apuntes-TAI-Tema-2.pdf

? Apuntes TAI ?

3° Tecnologías Avanzadas de la Información

Grado en Ingeniería Informática - Tecnologías Informáticas

Escuela Técnica Superior de Ingeniería Informática
Universidad de Sevilla

APUNTES TAI

TEMA 2 - CRIPTOGRAFÍA BÁSICA Y VPN

PARTE 1 - CRIPTOGRAFÍA

Funciones HASH:

Funciones que toman como entrada una cadena de bits de cualquier tamaño y devuelven una cadena de bits de un tamaño determinado llamada huella. Tiene las siguientes propiedades:

- F(datos) = HASH
- *Preimage resistance*: dado un HASH no es computable encontrar una cadena de datos tal que F(datos) = HASH
- *2nd preimage resistance*: dados unos datos no es computable encontrar otros datos con el mismo HASH
- *Collision resistance*: Es imposible/improbable encontrar 2 datos con el mismo HASH

Las aplicaciones del HASH incluyen la integridad de datos así como la verificación de estos. Varios ejemplos son el md5, sha1, sha256 o sha512.

`md5("1234")`	`e7df7cd2ca07f4f1ab415d457a6e1c13`
`sha1("1234")`	`1be168ff837f043bde17c0314341c84271047b31`
`sha256("1234")`	`a883dafc480d466ee04e0d6da986bd78eb1fdd2178d04693723da3a8f95d42f4`
`sha512("1234")`	`7985558370f0de86a864e0050afdf45d7029b8798bcd72cddbf781329f99380e3f3b1afdca6765d89fc388b213df8f6a193cfc56d4ff2ef6e0a99bd883a6d98c`

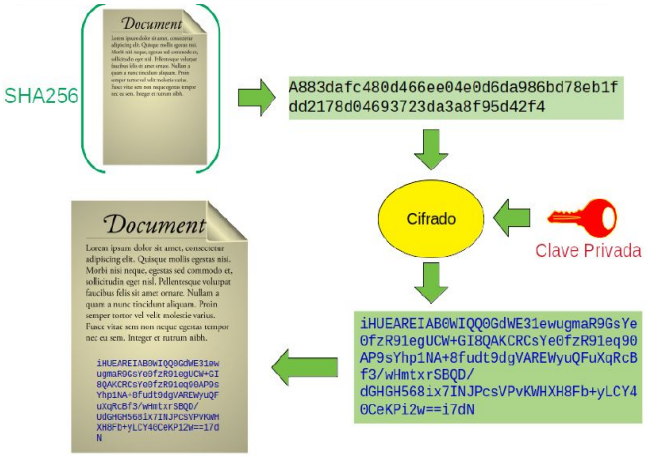
Cifrado simétrico/asimétrico:

- Cifrado simétrico: Emisor y receptor usan la misma clave (se ponen de acuerdo en cual usar). En caso de varios sistemas, todos usan la misma clave. Como puede verse, llega a ser muy vulnerable debido a las claves compartidas. Aunque se conozca el mensaje original y el mensaje cifrado, la clave debe ser difícil de obtener (la dificultad dependerá del algoritmo y de la longitud).

  La ventaja de este cifrado es la alta velocidad de ejecución. Podemos evitar la vulnerabilidad de la clave cambiandola cada cierto tiempo (este debe ser menor que lo que se requiere para adivinarla). Un método de intercambio de claves seguro es el **Algoritmo Diffie-Hellman**.

- Cifrado asimétrico: cada parte tiene dos claves y se basa en los números primos y la factorización. Algunos de los algoritmos más conocidos son **RSA**, Diffie-Hellman o DSA. Al tener dos claves (pública y privada), se elimina el problema de la distribución de claves pues solo se intercambian las públicas, lo que supone en su contra un deterioro del rendimiento respecto del cifrado simétrico. Para asegurar el intercambio de claves aparecen las **autoridades de certificación** (CA) y **certificados digitales**. Todos estos elementos forman la **PKI** (Public Key Infrastructure).

  Para asegurar la identidad de las dos partes, se usa la **firma electrónica**, la cual aplica una clave secreta al HASH sin que el documento original sufra cambios. Esta firma será visible para aquel que tenga la clave pública.



  El funcionamiento de la firma electrónica es, una vez cifrado el texto el texto original, se encripta añadiendo la clave privada. De esta forma obtenemos un documento nuevo que solo aquel con la clave pública puede descifrar.

  Los **certificados digitales** no son más que un archivo firmado con la clave privada de una CA para así evitar la suplantación (ambas partes confían en la autoridad y su clave pública es conocida por todos). Otro de los cometidos de una CA es el listado de certificados revocados (**CRL**). Aparte de lo anterior, los certificados pueden tener campos adicionales.

Ejemplos de aplicaciones:

- Autenticación: Almacenes de contraseñas de distintas aplicaciones que implementan el uso de HASH para mejorar la seguridad de las claves de usuarios (no todos lo consiguen, se necesita un algoritmo bueno para no conseguir las contraseñas por fuerza bruta o inyecciones).
- SSL (Secure Sockets Layer): Protocolo para dar seguridad a la capa de transporte.
- TLS: nueva versión de SSL más fácil de usar a nivel de programación.
- Firma electrónica: Usada por Apps stores (Google Play, Apple) o Ubuntu (aplicación GPG para el encriptado digital).
- Blockchain: Base de datos compuesta de bloques de tamaño fijo o variable. En cada bloque se almacena: una cantidad de registros, información referente a ese bloque y su vinculación con el bloque anterior y el bloque siguiente a través del hash de cada bloque.

- Bitcoin: Tanto para las transacciones como para la minería de estas.

PARTE 2 - VIRTUAL PRIVATE NETWORK (VPN)

Una VPN (Virtual Private Network) es una red de datos privada con el objetivo de ofrecer una interconexión segura de equipos de forma que aunque los datos sean visibles, no puedan descifrarse. Para garantizar una VPN, se debe requerir **Privacidad** (sólo los equipos autorizados están conectados), **Integridad** (lo que se intercambien no debe alterarse) y **Disponibilidad** (la conexión debe estar disponible cuando se requiera). La privacidad se consigue mediante la criptografía.

Túneles:

Definimos como túnel el canal de comunicación usado encapsulando un protocolo en otro de manera que los paquete que se envíen se **encapsulen** (empaquetar una trama como datos en otra trama de nivel superior) dentro de otro paquete cifrado y este solo tiene como visible el origen y el destino.

Esta envoltura produce una sobrecarga en el tráfico, siendo una de las desventajas más importantes de los túneles. Un túnel puede ser hecho en diferentes capas del modelo OSI.

VPN en varias capas :

- VPN en OSI capa 2: (*No profundizaré mucho ya que nunca se ha preguntado en el examen anteriormente*) permite transferir protocolos no-IP dentro del protocolo IP. Varias tecnologías son: Point to Point (PPTP), Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), Layer 2 Security Protocol (L2Sec).

- VPN en OSI capa 3: **IPsec** (conjunto de protocolos cuya función es la de asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.) Funciona en modo túnel y suele ser muy complejo. Otras tecnologías que veremos más adelante son OpenVPN y TINC.

- VPN en OSI capa 4: establecer un túnel VPN en el nivel de aplicación: SSL y TLS. Es la solución más simple para el usuario

Privacidad:

Como dijimos anteriormente, la privacidad se consigue mediante el cifrado tanto simétrico (IPsec cambia las claves cada cierto tiempo) como asimétrico (TINC usa clave pública/privada sin firma digital y OpenVPN usa PKI con certificados digitales).

OpenVPN:

Es una solución basada en SSL / TLS que implementa conexiones en la capa 2 o capa 3. No siempre podrá implementarse pero si se puede, el despliegue sería rápido y de bajo coste.

Se recomienda el uso de una clave asimétrica como **RSA** (algoritmo criptográfico basado en una clave pública y privada. La pública se usará para cifrar los datos y es visible para cualquier usuario y la clave privada se empleará para descifrar por lo que deberá estar protegida)

Los tipos de túneles que utiliza son: Túnel IP (tráfico IP punto-a-punto sin broadcast y fácil de configurar) y Puente ethernet (encapsular tanto protocolos IP como no-IP).

TINC:

Se configuran puntos de entradas (nodos) que indican quienes tienen permitidos conectarse a ellos usando TCP (intercambio de metadatos) o UDP (intercambio de datos).