**Seguridad: Tema 2**

1. Introducción a la criptografía

La **criptografía** es la ciencia de cifrar y descifrar información para que sólo pueda ser interpretada por el receptor. A través de la criptografía se pueden alterar las representaciones lingüísticas para que un mensaje sea confidencial entre las personas autorizadas.

Aspectos de la criptografía:

* La **información original** a proteger se denomina texto plano.
* El **cifrado** convierte el texto plano en un criptograma (texto cifrado o texto ilegible)
  + **Cifrado en bloque**: El texto original se divide en bloques de tamaño fijo que se cifran de manera independiente
  + **Cifrado en flujo**: se cifra bit a bit, byte a byte, carácter a carácter
* **Técnicas más sencillas de cifrado**:
  + **Sustitución**: cambiar el significado de los símbolos o caracteres por otros.
  + **Transposición**: reordenar los elementos del mensaje.
* **Descifrado**: proceso inverso que recupera el texto plano a partir del criptograma

Los objetivos de la criptografía cubren las siguientes necesidades:

* **Privacidad**: la información sólo puede ser interpretada por los usuarios autorizados
* **Integridad:** la información no puede ser alterada en su transmisión
* **Autenticidad**: garantizar que el mensaje proviene de la persona que realmente lo envía
* **No repudio**: no se puede negar la autoría o recepción de un mensaje

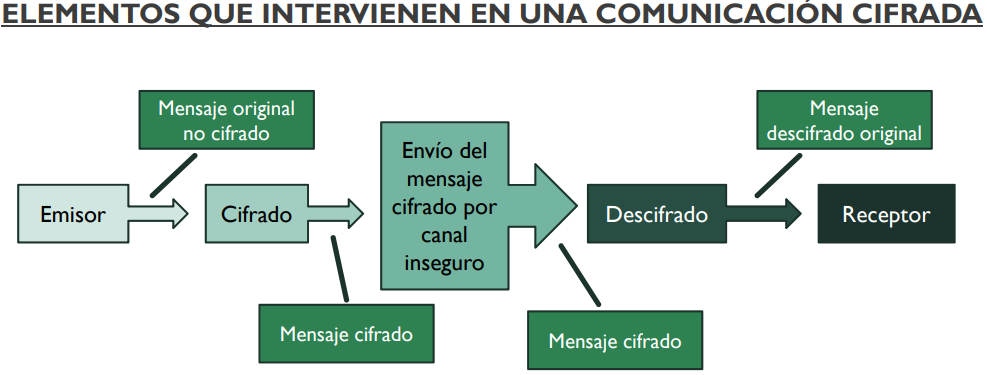
Las claves son combinaciones de símbolos que están expuestas a **ataques de fuerza bruta**. Para evitarlo:

* Utilizar **claves de gran longitud** para que un ordenador necesite muchos recursos para cubrir todo el rango de posibilidades
* **Cambiar regularmente de clave** para limitar el tiempo para comprobar todo el rango de claves
* **Utilizar todos los tipos de caracteres posibles:** una clave con solo números (10 caracteres) es más fácil de adivinar que una con números y letras (36 caracteres).
* **No utilizar palabras fácilmente identificables** como palabras del diccionario, nombres, etc.…
* **Detectar repetidos intentos fallidos** en un periodo corto de tiempo (Por ejemplo, el PIN del móvil)

Las claves no son el único problema de la criptografía. Pueden existir vulnerabilidades en un algoritmo o SO. Todas estas vulnerabilidades las estudia el **criptoanálisis**.

La operación de cifrado se realiza mediante dos métodos:

1. **Utilizando un algoritmo de cifrado que solo conozcan emisor y receptor:** método empleado por los primeros sistemas criptográficos. (Por ejemplo, desplazando las letras del alfabeto)
2. **Haciendo que el algoritmo sea conocido por todos** (algoritmo público) pero se utiliza una clave que regula el comportamiento del algoritmo. Sólo quien conozca la clave es capaz de descifrar el mensaje



1. Sistemas criptográficos

Dos sistemas criptográficos que usan claves son:

**Criptografía simétrica:**

Permite la comunicación segura entre emisor y receptor utilizando una única clave, denominada clave simétrica, ya que la misma es usada por ambos.

* Sólo quien conoce la clave es capaz de descifrar el mensaje por lo que se garantiza la confidencialidad mientras la clave solo la conozcan el emisor y el receptor.
* La simetría es el proceso por el cual se utiliza la misma clave para cifrar y descifrar
* El sistema de cifrado simétrico queda comprometido si alguien externo conoce la clave por lo que la robustez del sistema depende en la seguridad con la que se envía la clave.
* Los algoritmos más utilizados son: DES, 3DES, AES, Blowfish e IDEA

Problemas de la criptografía simétrica

* El intercambio de claves: es importante que el emisor y receptor se intercambien las claves a través de un canal de comunicación seguro
* El número de claves que se necesitan: Para un numero “n” de personas es necesario un numero “n/2” de claves ya que estas deben ser únicas

Cifrado de Vernam:

* Cifrado en flujo por bits a través de la operación XOR con la clave
* Claude Shannon demostró que cuando la clave es realmente aleatoria y se usa una vez el algoritmo es matemáticamente irrompible
* El problema de este algoritmo es que la clave es tan larga como el mensaje

Ejemplos de algoritmo

* Algoritmo de cifrado DES usa una clave de 56 bits, actualmente muy fácil de descifrar para un ordenador
* Algoritmo de cifrado 3DES, Blowfish, Twoofishc o IDEA: usan 128 bits
* Algoritmo RC5 y AES (Rijndael) los cuales se están desarrollando actualmente.

**Criptografía asimétrica:**

La criptografía asimétrica utiliza dos claves diferentes pero relacionadas entre sí. Cada usuario posee dos claves:

* Clave pública: conocida por todos los usuarios
* Clave privada: sólo conocida por el propietario

La criptografía asimétrica se utiliza en la firma digital ya que es más robusta que la criptografía simétrica.

Esta también tiene desventajas:

* Es necesario mayor tiempo de proceso
* Las claves son de mayor tamaño
* El mensaje cifrado ocupa más espacio que el original

El mensaje se envía con la clave pública del receptor y este lo desencripta con su clave privada

Se recomienda usar claves públicas de 1024 bits

**Funciones Hash**

Las funciones hash transforman un conjunto de datos en un código de tamaño fijo, sin importar la cantidad de datos que se utilice.

Existen varias funciones hash, la más conocida es la SHA-2

**Diffie-Hellman**

No es un algoritmo asimétrico como tal, este genera una clave simétrica en ambos extremos.

El problema de este algoritmo es que no comprueba la autenticación, no puede validad la identidad de los usuarios, si alguien escucha el mensaje y las claves podría descifrar el mensaje

**RSA**

* Sistema de clave pública más usado
* Seguridad basada en la factorización de números enteros grandes
* Los mensajes enviados se representan mediante números
* Su funcionamiento se basa en el producto de dos números primos
* El algoritmo se basa en la pareja: clave pública, clave privada

Ventajas

* Resuelve el problema de distribución de llaves
* Se puede utilizar para firmas digitales

Desventajas

* La seguridad depende de la eficiencia de los ordenadores
* Es más lento que los algoritmos de cifrado simétrico
* La clave privada se tiene que cifrar con un algoritmo simétrico

**Criptografía híbrida**

Para reducir el coste computacional de los algoritmos asimétricos, la criptografía híbrida permite cifrar el mensaje con un algoritmo simétrico y la clave utilizada mediante un algoritmo asimétrico.

Este sistema garantiza la confidencialidad (ya que sólo quien tiene las claves puede leer el mensaje) y la integridad (ya que si el mensaje se modifica no se podrá descifrar) pero no garantiza la autenticidad ni el no repudio del mensaje.

1. Operaciones criptográficas básicas

**Firma digital**

Una de las ventajas de la criptografía de clave pública es que ofrece un método para realizar firmas digitales para que el receptor pueda verificar la autenticidad del mensaje. A través de la firma digital se consigue:

* Autenticación: la firma digital es equivalente a la firma física de un documento
* Integridad: el mensaje no puede ser modificado
* No repudio en origen: el emisor no puede negar haber enviado el mensaje

**Certificación digital**

Los certificados digitales asocian una clave pública con la identidad de su propietario. El formato estándar de estos certificados es el X.509 y se puede distribuir de dos maneras:

* Con clave privada, más seguro y con el fin de realizar copias de seguridad
* Con clave pública, menos seguro y con el fin de verificar la identidad de los archivos firmados

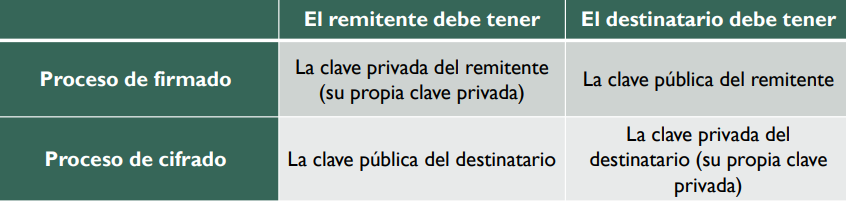
Dos usuarios pueden confiar entre sí, si una tercera parte tiene una relación con ambos y esta da fiabilidad a ambos. Esta tercera parte deberá usar su firma digital para avalar el certificado

Las infraestructuras de clave pública (ICP o PKI) está formada por:

* Autoridad de certificación (CA): emite y elimina los certificados digitales (ayuntamientos)
* Autoridad de registro (RA): controla la generación de los certificados, comprobando la identidad de los usuarios
* Autoridades de repositorio: almacena los certificados emitidos y eliminados
* Software para utilizar los certificados
* Política de seguridad relacionada con la gestión de certificados

El DNIe acredita la identidad y los datos personales que aparecen en él. Para utilizar el DNIe es necesario un Hardware específico (lector de tarjetas) y un Software específico

* Acredita electrónicamente la identidad de la persona
* Firma digitalmente documentos electrónicos con la misma validez que la firma manuscrita



En el certificado digital se puede incluir también la clave privada (como por ejemplo en el momento en el que se generan las claves y se le asignan a una persona). En estos casos la clave privada se protege utilizando una contraseña o un PIN

1. Infraestructura de clave pública, PKI

El PKI es el conjunto de elementos (HW y SW) necesarios para crear un sistema de certificación. El PKI se compone de una o varias autoridades de certificación, registro etc.… podemos diferenciar autoridades de dos clases:

* Autoridades raíz: No dependen de nadie, firman por ellas mismas
* Autoridades subordinadas: Dependen de la autoridad superior, firman en el nombre de la autoridad que dependen.

El Software PKI se puede instalar en un Windows server donde hay dos tipos de oficinas de certificación:

* Oficina independiente: servidores que no están relacionados con un Directorio Activo
* Oficina empresarial: Necesita un Directorio activo el cual realiza las tareas de gestión de la oficina

1. Otras operaciones criptográficas

**Protocolo SSL/ TSL**

El protocolo SSL (o su evolución a TSL) es un protocolo de encriptación usado por las páginas web para cifrar la información personal de los usuarios. Utiliza las funciones hash para cifrar la información entre cliente y servidor. Garantiza la confidencialidad y integridad de la información.

Este es el protocolo que otorga la “s” en “https”. Se puede utilizar este protocolo comprando el certificado.

**Protocolo SSH**

SSH (Secure Shell) es una colección de protocolos que permiten conectarnos a un dispositivo de manera remota de forma segura. A diferencia del Telnet, este protocolo cifra el canal (túnel) de comunicación entre ambos equipos

**Diferencias entre SSL y SSH**

* El protocolo SSL se utiliza en páginas Web mientras que el protocolo SSH se utiliza en aplicaciones de control remoto de quipos.
* El protocolo SSL encripta la información sensible que se envía a la página, mientras que el protocolo SSH encripta el canal de comunicación entero.