UT6: Criptografía y sistemas de identificación

CRIPTOGRAFÍA GENERALIDADES:

- **OBJETIVO:** El objetivo de la criptografía e intercambiar la información para que no nos pille el mensaje.
- **FINALIDAD:** Es la confidencialidad para lo que se han desarrollado técnicas para desarrollar la información.
- **LA INFORMACIÓN Y LAS COMUNICACIONES NECESITAN CIFRADOS:** Para que solo pueda acceder a la información de personas específicas.
- **La clave:** Es indispensable en la criptografía, la clave es una combinación de signos letras etc. Y están expuestas a ataques de fuerza bruta y diccionario de datos.
- **Las características de las claves son:** Longitud, cambio de letras, utilización de todo tipo de caracteres, no utilizar palabras recogidas en el diccionario, las claves y el algoritmo son un punto débil en la criptografía porque son más vulnerables.
- **En general los métodos de criptografía son:** Transposición–que consiste en descolocar las silabas o letras puede ser simple o múltiple. Sustitución–Puede ser sustituir letras por número o al revés. Escenografía–es la que oculta un mensaje detrás de una imagen.
- **Cifrado y descifrado de la información:**

Cifrado/descifrado de la información.

- **Métodos para asegurar la confidencialidad:**
  - **Protección del algoritmo**
  - **Protección de la clave.**
- **Tipos de algoritmos:**
  - **En función de la gestión de la clave:**
    - **Simétrico**
    - **Asimétrico**
    - **Hibrido**
  - **En función del método de cifrado**
    - **En bloque:DES AES,etc**
    - **De flujo: A5,RC4,etc**
- **Criterios de elección**
  - **Algoritmos utilizados en función de la capa OSI:**
    - **Nivel de enlace**
      - **WEP**
      - **WAP/WAP2**
    - **Nivel de red**
      - **IPSEC**
    - **Nivel de transporte**
      - **SSL**
      - **TLS**

- **Nivel de aplicación**
  - **Mensajería**
  - **Comunicación con base de datos**
  - **Etc**

SIMETRICA O CLAVE PRIVADA:

Criptografía simétrica o privada: Utiliza la misma clave para el proceso de cifrado que descifrado.

- **Inconvenientes:** Intercambio de las claves entre el emisor y el receptor. El atacante puede interpretar la clave fácilmente. El número a claves de generar es mucho.
- **Ventajas:** Algoritmos más rápidos, para las aplicaciones para la transmisión de datos, almacenamiento de datos la mayor parte de ataques son para quitar datos.
- **Métodos de criptología:**
  - Transposición: Consiste en cambiar el texto.
    - Simple: Consiste en un único cambio.
    - Doble: Consiste en varios cambios.

Criptografía simétrica o clave privada:

Utiliza la misma clave para cifrar como para descifrar

ASIMETRICA O CLAVE PÚBLICA:

Necesita dos claves una privada y una publica que comparte con el resto de usuarios.

Las claves se complementan una cifra y otra descifra, las claves obtienen mediante algoritmos matemáticos complejos y para cifrar un mensaje el emisor utiliza la clave pública del receptor y el receptor utiliza la clave privada para descifrar.

Ventajas: No necesitas claves seguras, no hay desbordamiento de clave, solo necesitas dos claves.

Desventajas: son pocos fiables porque se le da mucha importancia a la clave, se ralentiza el proceso y el mensaje ocupa mucho espacio.

Hay que proteger la clave privada y para guardarla se guarda en un llavero de claves(**Keyring**), este llavero está protegido mediante cifrado simétrico, es importante hacer copias de seguridad, transportar la clave privada que supone un riesgo–Solución: utilizar tarjetas inteligentes etc.

Este cifrado ofrece: Confidencialidad, autenticación y no repudio

Se usa para la firma digital y para distribución de las claves secretas.

CRIPTOGRAFÍA HIBRIDA

Utiliza un poco de las 2. Cifra con clave privada (o simétrica) para intercambiar el mensaje y utiliza clave pública (o asimétrica) para el intercambio de las claves.

ALGORITMOS QUE SE UTILIZAN EN LAS CRIPTOGRAFÍAS

Algoritmo: transforma texto plano en texto cifrado, este proceso se llama encriptado, el algoritmo se basa en una clave secreta, la fortaleza del cifrado depende de la clave.

Los algoritmos de cifrado se clasifican en:

- Bloque: que divide el texto en bloques o en grupos de tamaño fijo y se cifran de forma independiente.
- Lujo: se realiza bit a bit o byte a byte.

FUNCIÓN RESUMEN O HASH

Asocian un documento a un número, para obtener el valor resumen de ese documento se emplean algoritmos matemáticos, dos documentos no tienen el mismo valor resumen.

FIRMA DIGITAL

Es una de las ventajas de criptografía clave pública o asimétrica, es el resultado de cifrar con clave privada el resumen de los datos a firmar utilizando algoritmos HASH.

Dos documentos distintos firmados por la misma persona tendrán firmas digitales diferentes, con la firma digital se **consigue integridad, autenticación y no repudio.**

Para comprobar la firma digital,esa firma se descifra con clave pública y se obtiene el resumen o hash para obtenerlo se debe emplear el mismo algoritmo.

CERTIFICADO DIGITAL

Archivo que pude emplear un software para firmar digitalmente ficheros hay certificados digitales que identifican personas o organismos estos contienen nombre, dirección, correo electrónico etc.

DNI ELECTRÓNICO

DNI similar al tradicional y cuya principal novedad es que incorpora un pequeño circuito integrado (CHIP), capaz de guardar de forma segura, mediante medidas específicas de seguridad para impedir su falsificación en formato digital.