UT5: Sistemas de identificación. Criptografía. Parte1

2º Curso CFGM SMR

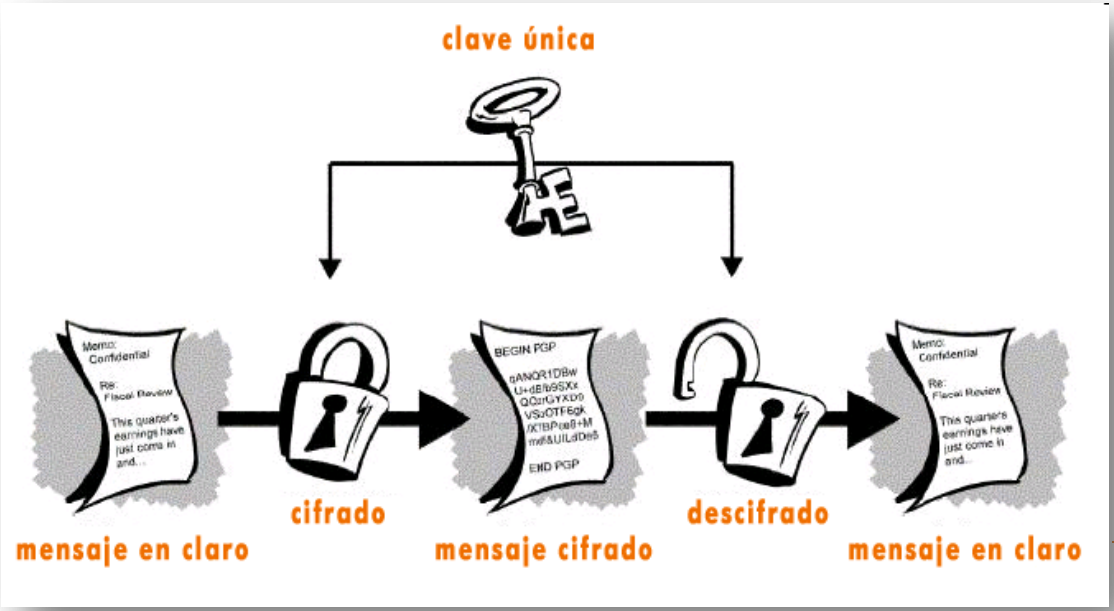
Índice.

5.1 Principios de criptografía.

- La ***criptografía*** (del griego "oculto" y "escribir", literalmente "escritura ocultar") es el arte o la ciencia de **cifrar y descifrar** información.
- Se emplea frecuentemente para permitir el intercambio de mensajes que **sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.**

5.1. Principios de criptografía.

- Conceptos:
  - ✓ **Información original a proteger:** texto en claro **o texto plano**.
  - ✓ **Cifrado** proceso de convertir el *texto plano* en un texto ilegible, o ***texto cifrado*** o *criptograma*. En general, la aplicación concreta del ***algoritmo de cifrado*** existencia de ***clave*** o información secreta que adapta el *algoritmo de cifrado* para cada uso.
- .

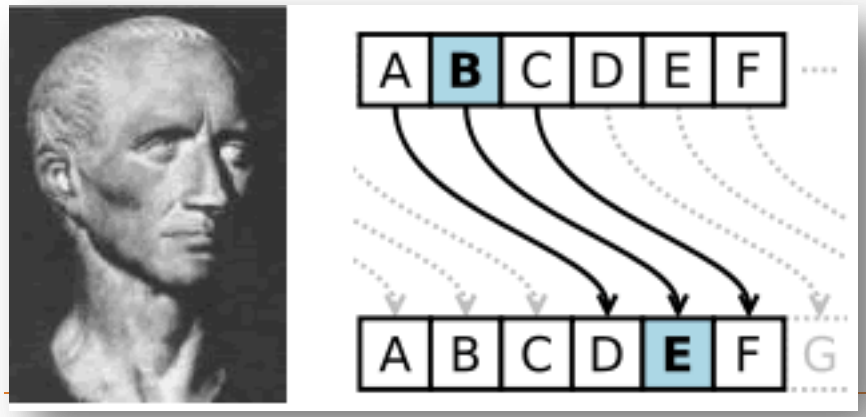


5.1. Principios de criptografía.

- Los **algoritmos de cifrado** se clasifican en dos grandes tipos:
  - **De cifrado en bloque**: dividen el texto origen en bloques de un tamaño fijo, y los cifran de manera independiente.
  - **De cifrado de flujo**: se realiza bit a bit o byte a byte o carácter a carácter.
- Las **dos técnicas más sencillas** de *cifrado*, criptografía clásica, son:
  - **Sustitución**: cambio de significado de los elementos básicos del mensaje, las letras, los dígitos o los símbolos.
  - **Transposición**: reordenación de los mismos, los elementos básicos no se modifican.
- El **descifrado:** proceso inverso recupera el *texto plano* a partir del *criptograma* y la *clave*.

5.2.Tipos de algoritmos de cifrado.

- Ejemplo de clave criptográfica: **Cifrado César.**
- La clave consiste en el *desplazamiento de 3 letras*. De esa manera se cifra el mensajes
- Para descifrarlo se emplea la misma clave.
- Ejemplo que usa la misma clave para cifrar y descifrar el mensaje.



Práctica: Scripts de cifrado.

1. En Ubuntu, crea un archivo con el siguiente texto.

```
Este documento tiene informacion confidencial:
User:angelica
Password:angelica2011
```

1. Utiliza el comando tr. Este comando, a partir de un flujo de datos, permite modificarlos, sustituyendo o borrando caracteres. La forma de usarlo es:
   - tr CONJUNTO1 CONJUNTO2
     - Ejemplo: echo murcielago | tr aeiou AEIOU
     - mUrcIElAgO
2. Ejecuta sobre el archivo anterior usando la clave César.:

```
Try `tr --help` for more information.
root@ubuntu:/home/afernan1# cat documento |tr [a-z] [d-zabc]|tr [A-Z] [D-ZABC] >
documento_cesar
```

3. Haz un cat de documento_cesar. A continuación, desencríptalo.

5.2. Tipos de algoritmos de cifrado.

- Hay dos grandes grupos de algoritmos de cifrado:

✓ **Simétricos o de clave simétrica o privada**: una ***única clave*** en el proceso de *cifrado* como en *descifrado*.

✓ **Asimétricos o de clave asimétrica o pública**: ***dos claves:*** una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Estos forman el núcleo de las técnicas de cifrado modernas: certificados digitales, firma digital, DNIe.

5.2. Tipos de algoritmos de cifrado.

- *Criptografía simétrica:* **Fundamentos.**

- Se usa una misma clave para cifrar y descifrar.
- Las 2 partes que se comunican deben ponerse de acuerdo de antemano: clave a usar.
- Un buen sistema de cifrado toda la seguridad en la clave y ninguna en el algoritmo.
- Importante: que sea muy difícil adivinar.
- El espacio de *posibles de claves* debe ser amplio.
- **Longitud y conjunto de caracteres**.

5.2. Tipos de algoritmos de cifrado.

- *Criptografía simétrica:* **Algoritmos**
- **DES** clave de 56 bits.
- Algoritmos de cifrado **3DES**, **Blowfish, CAST5** e **IDEA** claves de **128 bits**. La mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo 3DES.
- Otros algoritmos de cifrado muy usados: **RC5** y **AES**, Advanced Encryption Standard, conocido como **Rijndael**, estándar de cifrado por el gobierno de los Estados Unidos (sustituyó a DES).

5.2. Tipos de algoritmos de cifrado.

- *Criptografía simétrica:* **Principales problemas.**
- **Principales problemas** de los sistemas de cifrado simétrico no son su seguridad sino:
  - **El intercambio de claves**: ¿qué **canal de comunicación seguro** han usado para transmitirse las claves?
  - **El número de claves que se necesitan**: un número **n** de personas comunicarse entre sí, **n(n-1)/2** claves diferentes para que cada pareja de personas pueda comunicarse de manera segura.

5.2. Tipos de algoritmos de cifrado.

- ***Criptografía simétrica:***

- ✓ Video de intypedia: ***http://www.intypedia.com/***
- ✓ Práctica 1.