M9 – UF1
Introducción Criptografía

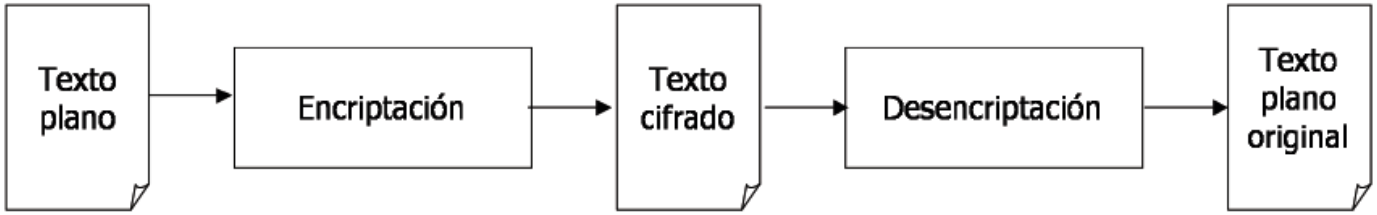
Eduard Lara

INDICE

1. INTRODUCCION

Definició:

És un conjunt de tècniques que ens permeten enviar un missatge des d'un emissor a un receptor sense que ningú que intercepti el missatge en el camí pugui interpretar-ho.



Nota: Xifrat vs Encriptat:

Xifrat (Ciphertext): Està sent representat per un altre sistema de codificació. Encriptat: No es pot accedir a ell

2. APLICACIONS DE LA CRIPTOGRAFIA

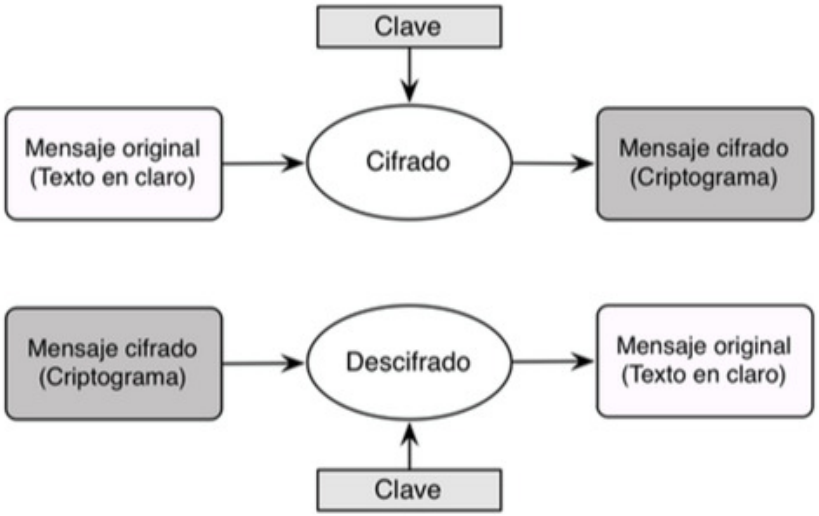
- Identificació i autentificació. Identificar a un individu o validar l'accés a un servidor.
- Certificació. Esquema mitjançant el qual agents fiables validen la identitat d'agents desconeguts (com usuaris reals).
- Seguretat de les comunicacions: Permet establir canals segurs per aplicacions que operen sobre xarxes que no són segures.
- Comerç electrònic: Utilitzar canals segurs i mecanismes d'identificació possibilita permetre a les empreses i als usuaris que tinguin garanties de que les operacions no seran espiades ni modificades

3. CARACTERISTIQUES SERVEIS SEGURETAT

- Confidencialitat : es tracta d'assegurar que la comunicació només pugui ser vista pels usuaris autoritzats, evitant que cap altre pugui llegir el missatge.
- Integritat de la informació: es tracta d'assegurar que el missatge no hagi sigut modificat de cap mode per altres persones durant la seva transmissió.
- Autenticació: es tracta d'assegurar l'origen, la autoria i la propietat de la informació de qui envia el missatge.
- No repudi: Es tracta d'evitar que la perona que envia el missatge o realitza una acció, negui haber-ho fet entre tercers.

4. ESTRUCTURA D'UN SISTEMA SECRET

- Un sistema secret actual es troba definit per dos funcions:
  - Funció de xifrat.
  - Funció de desxifrat.
- La clau és el paràmetre que especifica una transformació concreta dins de totes les possibles substitucions que es podrien realitzar amb la funció de xifrat.



5. XIFRAT PER SUBSTITUCIÓ

- El xifrat per substitució consisteix a reemplaçar cada caràcter del text pla per un altre caràcter en el text xifrat, i per desxifrar se segueix el procés invers.
- Exemple Xifrat Cèsar:

Texto plano ——————> H U Y E

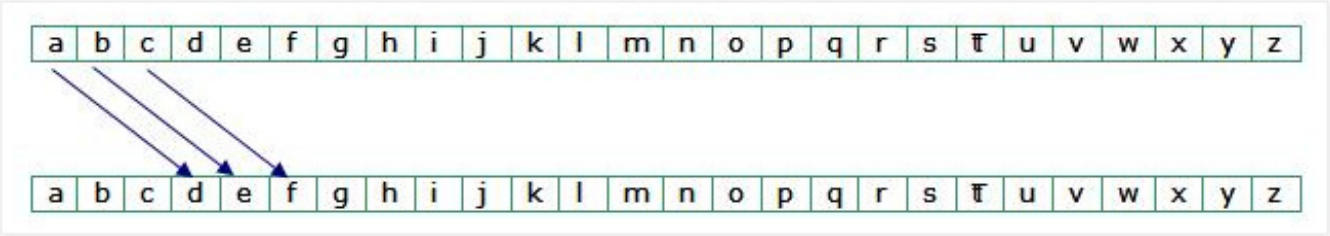
Texto cifrado ——————> K X B H

Xifrat

Texto cifrado ——————> K X B H

Texto plano ——————> H U Y E

Desxifrat



6. XIFRAT PER TRANSPOSICIO

- Els xifradors per transposició simplement canvien l'ordre de les lletres.
- Exemple: Per columnes

Texto plano: NOS ATACAN CON CARBUNCO

```
N O S _ A
T A C A N
_ C O N _
C A R B U
N C O _ _
```

Texto cifrado: NT CN OACACSCORO ANB AN U

PRACTICA 1

Institut Joan d'Àustria

Xifrat per substitució

Realitza les següents funcions en java:

- cifradoCesar (cadena, N) : ha de xifrar un missatge fent servir la tècnica de substitució. Cada caràcter s'ha de substuir amb el N caracter més endavant en el llistat especificat.
- descifradoCesar (cadena, N) : ha de desxifrar un missatge xifrat amb substitució, substituint cada caràcter amb el N caràcter més endarrerit en el llistat especificat.
- NOTA: La llista especificada potser:
  - El simple codi ascii
  - Un llistat format amb el nostre abecedari (sense incloure la ñ ni accents), seguit dels 10 dígits (0-9).

PRACTICA 1

Institut Joan d'Àustria

Xifrat per substitució

```
public static void main(String arg[]) {
    Scanner sc = new Scanner(System.in);
    System.out.print("Introduce un texto: ");
    String texto = sc.nextLine();
    System.out.print("Introduce numero: ");
    int N = sc.nextInt();
    String cifrado = cifradoCesar(texto,N);
    System.out.println("Cifrado " + cifrado);
    String descifrado = descifradoCesar(cifrado,N);
    System.out.println("Descifrado " + descifrado);
}
```

```
public static String descifradoCesar(String entrada,int N) {
    String salida="";
    for (int i = 0; i < entrada.length(); i++) {



    }
    return salida;
}
```

```
public static String cifradoCesar(String entrada, int N) {
    String salida="";
    for (int i = 0; i < entrada.length(); i++) {



    }
    return salida;
}
```

PRACTICA 2

Institut Joan d'Àustria

Xifrat per transposició

Realitza les següents funcions en java:

- cifradoTrans (cadena, N) : ha de xifrar un missatge fent servir la tècnica de transposició per columnes. Ha de posar el missatge en una matriu de N columnes per files i llegir el resultat per columnes.
- descifradoTrans (cadena, N) : ha de desxifrar un missatge fent servir la tècnica de transposició per columnes. Ha de posar el missatge en una matriu de N columnes per files i llegir el resultat per columnes.

PRACTICA 2

Xifrat per transposició

```java
public static void main(String[] args) {
    Scanner sc = new Scanner(System.in);
    System.out.print("Introduce un texto: ");
    String texto = sc.nextLine();
    System.out.print("Introduce numero columnas: ");
    int N = sc.nextInt();
    String cifrado = cifradoTrans(texto,N);
    System.out.println("Cifrado " + cifrado);
    String descifrado = descifradoTrans(cifrado,N);
    System.out.println("Descifrado " + descifrado);
}
```

```java
public static String cifradoTrans(String entrada, int N) {
    String salida="";



    return salida;
}
```

```java
public static String descifradoTrans(String entrada,int N) {
    String salida="";



    return salida;
}
```