

# **RESUM-FORMULARI TEMA 7**

Informació i Seguretat (Universitat Autònoma de Barcelona)

# <u>RESUM – FORMULARI</u> <u>TEMA 7 CRIPTOGRAFIA I SEGURETAT</u>

## MÈTODES BÀSICS

## **SUBSTITUCIÓ SIMPLE**

Consisteix en substituir cada una de les paraules del nostre missatge per una altra paraula del alfabet utilitzat. Per un alfabet A, tenim |A|! claus (K) possibles.

PER XIFRAR:

 $y = x + k \mod m$ 

PER DESXIFRAR:

 $x = y - k \mod m$ 

y: missatge xifrat, x: missatge original, k: clau, m: longitud del nostre alfabet.

## TRANSPOSICIÓ SIMPLE

Consisteix en reordenar les paraules del nostre missatge. Hi ha d! claus possibles (d: longitud del missatge).

#### **EXEMPLE:**

Si agafem d = 3 i prenem la permutació  $\sigma(1)=2$ ,  $\sigma(2)=3$ ,  $\sigma(3)=1$ , aleshores,

el missatge **m = CRIPTOGRAFIA** queda xifrat com:

 $E_{\sigma}$  (m) = ICROPTAGRAFI

# CRIPTOSISTEMES SIMÈTRICS / CLAU PRIVADA CLAU XIFRATGE = CLAU DESXIFRATGE

## XIFRATGE MATRICIAL O HILT

La clau és una matriu K<sub>r x r</sub>, que ha de ser **INVERTIBLE**.

PER XIFRAR:

 $C = K \cdot M$ 

PER DESXIFRAR:

 $M = K^{-1} \cdot C$ 

Serà invertible si el mcd(det(K), m) = 1.

On m és la longitud del alfabet que estem utilitzant.

$$K^{-1} = \frac{1}{\det(K)} \cdot A_k^T$$

## <u>XIFRATGE AFÍ</u>

**PER XIFRAR:** 

 $f(x)=a\cdot x + b \pmod{m}$ 

on la clau és k=(a, b) i a i b formen part del nostre alfabet.

PER DESXIFRAR:

 $f^{-1}(c) = a^{-1} \cdot (c - b)$ 

c: missatge xifrat

# MÈTODE VIGÈNERE de longitud r

Clau:  $k = (k_0, k_1, ..., k_{r-1})$ 

**PER XIFRAR:** 

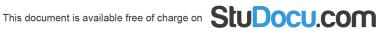
 $C_i = m_i + k_i \pmod{m}$ 

M es divideix en blocs de longitud r.

PER DESXIFRAR:

 $m_i = c_i - k_i$ 

**XAVIER MOLINA** 



### **DES**

 $C = DES_k(m)$ 

Utilitza **claus de 56 bits**, per esbrinar la clau hauríem de provar 2<sup>56</sup> combinacions.

#### **DOBLE DES**

 $C = DES_{k2} (DES_{k1} (m))$ 

No soposa una millora respecte el DES simple, per tant, no s'utilitza.

#### TRIPLE DES

 $C = DES_{k1} (DES_{k2} (DES_{k1} (m)))$ 

Assoleix una **seguretat de 112 bits**, per tant, suposa una millora respecte el DES.

En els tres casos el procés de desxifratge és exactament el mateix que el procés de xifratge.

## **ESTÀNDARD AES**

La clau i els blocs poden ser de 128, 192 o 256 bits.

L'algorisme de desxifrat no és el mateix que el de xifrat, per tant no és adequat per sistemes amb poca capacitat de càlcul.

### **MODES DE XIFRATGE**

- ECB
- CBC
- CFB

# CRIPTOSISTEMES ASIMÈTRICS / CLAU PÚBLICA CLAU XIFRATGE # CLAU DESXIFRATGE

#### **XIFRATGE RSA**

 $\mathbf{n} = \mathbf{p} \cdot \mathbf{q}$  on p i q són nombres primers.

 $\Phi = (p-1) \cdot (q-1)$ 

Clau pública: [n,e]

Clau privada:  $d = e^{-1} \mod \Phi$ 

e ha de ser INVERTIBLE, mcd(e, Φ)=1

**EXEMPLE**: Si volem enviar un missatge xifrat d'A a B:  $C = m^{e_b} \mod n_b$ , utilitzarem per tant la clau pública de <u>B</u> (destí).

**XAVIER MOLINA**