CriptoTema1.pdf

onafolch

Criptografia i Seguretat

3º Grado en Ingeniería de Datos

Escuela de Ingeniería
Universidad Autónoma de Barcelona

CRIPTOGRAFIA

INTRODUCCIÓ

1. SERVEIS DE SEGURETAT

- **Confidencialitat**: és una propietat que garanteix que la informació no es fa pública a persones no autoritzades.
- **Integritat**: és la propietat que garanteix que la informació no ha estat modificada.
- **Autenticació**: és el procés de reconeixement de la identitat d'un usuari.
- **No-repudi**: és la propietat que garanteix que l'autor d'una determinada acció no pugui negar haver-la realitzat.
- **Anonimat**: on la identitat de l'usuari és desconeguda.
- **Privacitat**: capacitat dels usuaris d'aïllar-se o aïllar informació sobre ells.
- **Consens**: s'utilitza en els sistemes distribuïts, i és un mecanisme de consens que s'utilitza per aconseguir l'acord necessari sobre les decisions en un procés distribuït.
- **Censura**: és el control o la supressió d'allò que es pot accedir, publicar o veure digitalment.

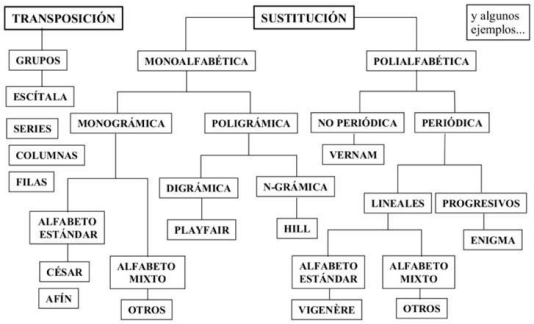
2. CRIPTOSISTEMES CLÀSSICS

Claude Shannon va proposar dos mètodes en els algoritmes de xifra:

- Difusió: per difuminar la redundància del llenguatge. Pretén difondre les característiques del text en clar en tot un text xifrat ocultant la relació entre el text en clar i el text xifrat.
- Confusió: per dificultar la descoberta de la clau utilitzada. Pretén confondre a l'atacant perquè no li sigui fàcil poder establir una relació senzilla entre el text xifrat i la clau emprada.

Tant màquines, artefactes de xifra, com els algoritmes que treballaven matemàticament dins un cos finit n, fan ús de dues tècniques bàsiques orientades a caràcters i que, molts segles després, les proposarà Shannon com a eines per enfortir la xifra.

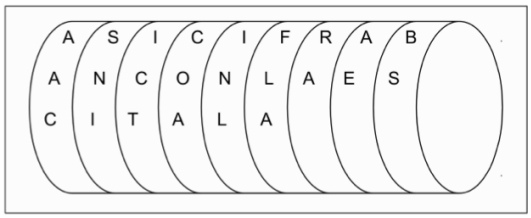
- **Tècniques de substitució**: els caràcters o lletres del missatge en clar es modifiquen o es substitueixen per altres elements o lletres. Per tant, tindrà caràcters diferents als que tenia el missatge en clar.
    - Monoalfabètiques: es caracteritzen per fer servir una substitució de caràcters fixa, on una mateixa lletra del text en clar sempre correspondrà a la mateixa lletra del text xifrat, independentment de la posició que ocupi la lletra en el text en clar.
    - Polialfabètiques: es caracteritzen per fer servir múltiples alfabets de substitució, fent que una mateixa lletra del text en clar pugui quedar xifrada amb diferents lletres, depenent de la posició que aquesta ocupi en el text en clar.
    -
- **Tècniques de transposició o permutació**: els caràcters o lletres del missatge en clar es redistribueixen sense modificar-los i seguint unes regles. El criptograma tindrà els mateixos caràcters del missatge en clar però amb una distribució o localització diferent.



Ona Folch

Escítala

Cirptosistema de **transposició** on la clau de xifrat és una pal d'un determinat gruix. Per a xifrar, s'enrotllava una tira de papir al voltant del pal i s'escrivia el missatge en sentit longitudinal. Després, es desenrotllava, obtenint el missatge xifrat. El gruix del bastó representava la clau compartida.

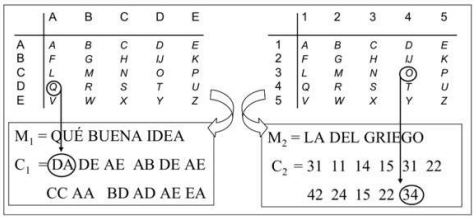


Text en clar: M = ASI CIFRABAN CON LA ESCITALA

Text xifrat o criptograma:
C = ACC SNI ICT COA INL FLA RA AE BS

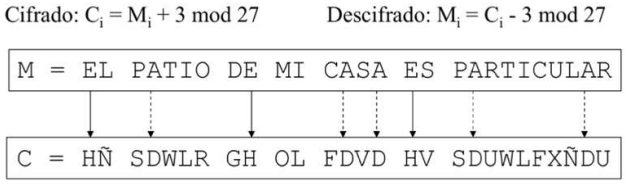
Polybios

Xifrador per **substitució**, on cada lletra es substituirà per dues lletres o números. Duplica la mida del text en clar i per aquesta raó no és bona idea.



César

Xifrador per **substitució monoalfabètic monogràmic**, el qual xifra cada lletra de l'alfabet en clar per la lletra que es troba tres posicions després de l'alfabet (k=3). Per codificar un text en clar amb César, necessitem n (número d'elements de l'alfabet). Per xifrar farem C = M + k mod n, i per desxifrar M = C - k mod n. Cada lletra sempre es xifrarà igual, cosa que fa que el sistema sigui molt vulnerable i fàcil d'atacar utilitzant les estadístiques del llenguatge.



Podem desencriptar el text xifrat sense saber la k, assignant la lletra més freqüent del criptograma amb la lletra més freqüent de l'alfabet.

Exemple:

C = LZAHL ZBTHW YBLIH XBLKL IL YOH ZLYCH ROKH Freqüències: L(7), H(6), B(3), etc

És possible que la lletra E del llenguatge sigui xifrada per una L, i la A per la H. Ho comprovem:

$$L = E + k \bmod 27 \rightarrow k = L - E \bmod 27 \rightarrow k = 11\text{-}4 \bmod 27 = 7$$
$$H = A + k \bmod 27 \rightarrow k = H - A \bmod 27 \rightarrow k = 7\text{-}0 \bmod 27 = 7$$

M = ESTO ES UNA PRUEBA QUE DEBERIA SER VALIDA

César afí: És el mateix que el César, però tenim una nova variable. Per xifrar farem que C = a*M + b mod n, i per desxifrar M = (C – b)*a^{-1} mod n, on a^{-1} és inv(a, 27). Per tant, el factor de multiplicació ha de ser primer amb 'n' per tal que existeixi inversa, i el factor de desplaçament pot ser qualsevol entre 0 i 26 (inclosos). Atacar aquest sistema també és molt fàcil.

Ona Folch

Vigènre

Xifrador per **substitució polialfabètic periòdic**. Soluciona la debilitat del xifrat de César en que una lletra es xifra sempre igual. S'utilitza una clau K de longitud L i es xifra caràcter a caràcter sumant mòdul n en el text en clar amb els elements de la clau. `C = M + K mod 27.`

Si K = CIFRA i M = HOLA AMIGOS

M	=	H	O	L	A	A	M	I	G	O	S
K	=	C	I	F	R	A	C	I	F	R	A
C	=	J	W	P	R	A	Ñ	P	L	G	S

El problema és que si observes el text xifrat es poden observar cadenes repetides, i amb això pots saber la llargada de la clau (Kasiski). També podem aconseguir la clau sabent quines són les lletres més repetides en l'alfabet.

Amb la regla AEO mirem les posicions relatives de les tres lletres, i sabem que la A està a la posició 0, la E a quatre espais de la A (m+4 mod 27), i la O està 15 espais a la dreta de la A, i 11 de la E. Per tant, s'han de buscar les tres lletres més freqüents i que compleixin amb la distribució de 0, +4, +11 mod 27. Si tenim 4 textos xifrats amb la mateixa clau, busco aquesta distribució en els 4, i obtenint la primera lletra de cada un (de les 3 lletres que segueixen la distribució) puc saber la clau. (mirar pàgina 19).

Playfair

Xifrador de **substitució monoalfabètic poligramic**. Els anteriors es feien caràcter a caràcter (monogràmicos). Per augmentar la seguretat de la xifra i trencar estadístiques, podem xifrar per poligramas, és a dir, blocs de caràcters. Playfair treballa amb una matriu de 5x5 lletres, xifrant per diagrames. Si el text en clar té un número impar d'elements, s'omple amb una lletra preestablerta, com per exemple la X.

- Si M_1 i M_2 estan a la mateixa fila, C_1 i C_2 seran els 2 caràcters de la dreta.
- Si M_1 i M_2 estan a la mateixa columna, C_1 i C_2 seran els 2 caràcters de abaix.
- Si M_1 i M_2 estan en diferents files i columnes, C_1 i C_2 seran els 2 caràcters de la diagonal, desde la fila de M_1.

A	B	C	D	E
F	G	H	I/J	K
L	M	N/Ñ	O	P
Q	R	S	T	U
V	W	X	Y	Z

Exemple:

Si la clau és K = BEATLES i el missatge és M = WITH A LITTLE HELP FROM MY FRIENDS, primer de tot crearem la matriu introduint primer de tot la clau seqüencialment. Si el caràcter ja es troba a la matriu, no es posa i es passa al següent.

B	E	A	T	L
S	C	D	F	G
H	I/J	K	M	N
O	P	Q	R	U
V	W	X	Y	Z

M = WI TH AL IT TL EH EL PF RO MX MY FR IE ND SX

(Es trenca la doble M afegint una X, igual que al final)

C = EP BM TB ME LB BI AB RC UP KY RT MY PC KG DV

Ona Folch

Hill

Xifrador de **substitució monoalfabètic poligramic** utilitzant matrius com a clau, xifrant Ngrames de forma que

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ .. \\ C_N \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} & \dots & k_{1N} \\ k_{21} & k_{22} & k_{23} & \dots & k_{2N} \\ k_{31} & k_{32} & k_{33} & \dots & k_{3N} \\ .. & .. & .. & & .. \\ k_{N1} & k_{N2} & k_{N3} & \dots & k_{NN} \end{pmatrix} \text{X} \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ .. \\ M_N \end{pmatrix}$$

La matriu clau K ha de tenir inversa en el cos n. Després, com que K^{-1}= $T_{ADJ(K)}$/ |K| mod n, on ADJ(K) és la matriu adjunta, T és la transposada i |K| el determinant, aquest darrer valor |K| no podrà ser zero ni tenir factors en comú amb n ja que està al denominador (concepte d'invers ja vist). Si el text clar no és múltiple del bloc N, s'emplena amb caràcters predeterminats, per exemple la lletra X o la Z.

Exemple:

Si M = AMIGO CONDUCTOR i la clau K = PELIGROSO:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 16 & 4 & 11 \\ 8 & 6 & 18 \\ 15 & 19 & 15 \end{pmatrix} \text{X} \begin{pmatrix} 0 \\ 12 \\ 8 \end{pmatrix} \text{ mod } 27$$

M = **AMI** GOC OND UCT ORZ (AMI serà 0 12 8)
C1 = (16*0)+(4*12)+(11*8)mod 27 = 1 = B
C2 = A, C3 = X
C = BAX PMA BJE XAF EUM

Per desxifrar tenim que K^{-1}=inv(K, 27) = $T_{ADJ(K)}$/ |K| mod 27, on |K| = 4. Obtenim:

$$(M) = (K^{-1}) \text{ x } (C) \text{ mod n} \quad \text{y} \quad K^{-1} = \begin{pmatrix} 18 & 26 & 15 \\ 24 & 6 & 13 \\ 11 & 24 & 10 \end{pmatrix}$$

Atac a Hill per Gauss Jordan: si escrivim una matriu amb els elements del text en clar i els elements del criptograma, i fem Gauss Jordan (multiplicant i restar files entre si). En el primer pas vull deixar tota la columna en zeros menys el primer valor; agafo la primera fila i la multiplico per l'invers del primer valor (en aquest exemple, l'invers de 4, que és 7). Finalment, la part de la dreta de la matriu correspondrà amb la clau.

$$\left(\begin{array}{ccc|ccc} 4 & 13 & 21 & 23 & 22 & 24 \\ 13 & 11 & 21 & 8 & 3 & 17 \\ 6 & 0 & 18 & 3 & 3 & 15 \\ 3 & 4 & 11 & 8 & 20 & 17 \\ 0 & 12 & 0 & 9 & 6 & 15 \\ 13 & 2 & 7 & 6 & 9 & 8 \\ 0 & 3 & 4 & 25 & 12 & 6 \\ 2 & 21 & 25 & 5 & 22 & 2 \\ 15 & 13 & 15 & 21 & 14 & 20 \end{array}\right) \rightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 5 & 7 \\ 0 & 1 & 0 & 3 & 5 & 8 \\ 0 & 0 & 1 & 4 & 6 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Vernam

Xifrat de **substitució polialfabètica** binària amb claus d'un sol ús (one-time-pad). L'operació de xifra és la funció XOR, i utilitza una seqüència binaria i aleatòria S que s'obté a partir d'una clau secreta K compartida per l'emissor i el receptor. És l'únic xifrador matemàticament segur, i impossible de criptoanalitzar, ja que la clau K només s'utilitza una vegada, és aleatòria i és tant o més llarga que el missatge.

M = BYTES
K = VERNAM
Solución:
B⊕V = 11001⊕11110 = 00111 = U
Y⊕E = 10101⊕00001 = 10100 = H
T⊕R = 10000⊕01010 = 11010 = G
E⊕N = 00001⊕01100 = 01101 = F
S⊕A = 00101⊕00011 = 00110 = I
C = UHGFI

Enigma

Enigma era el nom d'una màquina de rotors que permetien utilitzar-la tant per xifrar com per desxifrar missatges. Va ser un dispositiu electromecànic que utilitzava una combinació de partes mecàniques y elèctriques.

Ona Folch