2. CRITTOGRAFIA CLASSICA

Le origini della crittografia classica trovano radici nella ***steganografia***, una tecnica che si prefigge di nascondere la comunicazione tra due interlocutori: veniva utilizzata in tempi antichi, con la complicanza che, una volta scoperto il meccanismo con cui si nascondeva il messaggio, la segretezza della comunicazione era compromessa.

La **crittografia** (dal greco κρυπτός [*kryptós*], "nascosto", e γραφία [*graphía*], "scrittura") è la branca della ***crittologia*** che tratta dei metodi per rendere un messaggio non intelligibile a persone non autorizzate a leggerlo. Questo meccanismo si basa su criteri di ***trasformazione*** e ***segretezza***. Può essere ottenuta in numerosi modi.

- I cifrari **a trasposizione** ottengono, a partire da un messaggio in input, una sua permutazione. Le tecniche di trasposizione, basate su matrici e/o sulla ripetizione di essa, usate da sole sono facili da analizzare: possono essere usate insieme a tecniche con sostituzione.

Basate su matrici

EGGSOESIRMGEOAST

4	1	3	2	5
M	E	S	S	A
G	G	I	O	S
E	G	R	E	T
O				

MESSAGGIO SEGRETO

MSAGOERT
ESGISGEO

MSAGOERTESGISGEO

Ripetizione trasposizione

GSESRAGIOEEGTOMS

4	1	3	2	5
E	G	G	S	O
E	S	I	R	M
G	E	O	A	S
T				

- I cifrari **a sostituzione** ottengono, a partire da un messaggio in input, un altro messaggio sostituendo una o più lettere del messaggio con altre. Il più famoso (ed antico) cifrario a sostituzione è il Cifrario di Cesare, un cifrario **con shift** che ad ogni lettera (con indice *i*) del messaggio assegna la lettera avente indice *i+k* dell'alfabeto corrispondente, con chiave k. I cifrari a sostituzione *monoalfabetica* sostituiscono ogni lettera dell'alfabeto con altre lettere scelte arbitrariamente; i cifrari a sostituzione monoalfabetica *con chiave* utilizzano una frase chiave, inserendo in una riga l'intero alfabeto (con ogni colonna avente una sua lettera) e nella riga sottostante le lettere in ordine della frase chiave (con lunghezza <= 26) senza ripetizioni, riempendo eventualmente inserendo le lettere dell'alfabeto non utilizzate nella frase chiave.

CIFRARIO DI CESARE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

testo in chiaro

X ← M+3 mod 26

OMNIA GALLIA EST DIVISA IN PARTES TRES
RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV

testo cifrato

CIFRARO A SOSTITUZIONE MONOALFABETICA

Alfabeto in chiaro

Alfabeto cifrante

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

testo in chiaro: C A S A
testo cifrato: T O P O

2.1 CRITTOANALISI

Per ***crittoanalisi*** s'intende lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta, solitamente richiesta per effettuare l'operazione. Trattasi della "controparte" della ***crittografia***. Dato un testo cifrato, si provano tutte le possibili chiavi. In epoche passate, ci si basava su frequenza, vicinanza con altre lettere ("q" è sempre seguita da "u", …) e altre regole: il cifrario poteva essere rotto considerando le regolarità del linguaggio.

caratteri	occorrenze
8	33
;	26
4	19
+)	16
*	13
5	12
6	11
! 1	8
0	6
9 2	5
: 3	4
?	3
`	2
- .	1

Assumiamo che 8 corrisponda al carattere e

7 occorrenze di ;48

Per evitare ***analisi statistiche***, si possono utilizzare tecniche:

- ***nulle***, con cui si aggiungono simboli meno frequenti in posizioni tali da non alterare il significato (es.: "QUELQRAMODELQLAGO…");
- ***omofoni***, con cui si utilizzano molti simboli per cifrare singoli caratteri frequenti.

Un'altra tecnica utilizza ***nomenclatori***, dove si usa un insieme di parole in codice in aggiunta all'alfabeto cifrante. Oltre la ***cifratura monoalfabetica***, possono essere usati due approcci:

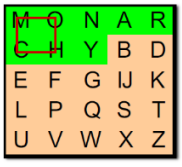
- mediante l'utilizzo di cifrature di più lettere per volta (Playfair, Hill, …);
- mediante l'utilizzo di più alfabeti cifranti (Leon Battista Alberti, Vigenère, …).

2.2 CIFRATURA MULTILETTERA DI PLAYFAIR

La ***cifratura multilettera di Playfair*** cifra due simboli insieme, utilizzando una matrice 5x5 costruita a partire da una parola chiave per facilità di memorizzazione (con IJ poste in un'unica cella), dove non devono esserci lettere consecutive (si inserisce una lettera fittizia tra le due, nel caso); si individuano le due lettere nella matrice:

- se individuano un rettangolo, allora ciascuna lettera viene sostituita dalla lettera che si trova nella stessa riga del rettangolo;
- se individuano una colonna, allora ciascuna lettera viene sostituita dalla seguente nella colonna;
- se individuano una riga, allora ciascuna lettera viene sostituita dalla seguente nella riga.

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



testo in chiaro: AT TA CX CO
testo cifrato: RS SR BU HM

2.3 CIFRATURA MULTILETTERA DI HILL

La ***cifratura multilettera di Hill*** cifra insiemi di lettere di volta in volta: ***m*** lettere in chiaro successive, ***m*** lettere di testo cifrato, con sostituzione usando algebra lineare; per m=3, la cifratura delle lettere $p_1p_2p_3$ è:

- $c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26$;
- $c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26$;
- $c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26$.

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{12} & k_{22} & k_{23} \\ k_{13} & k_{32} & k_{33} \end{bmatrix} \times \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \bmod 26$$

La chiave K è la matrice dei coefficienti k

La chiave k è la matrice dei coefficienti k, per la decifratura si usa la ***matrice inversa*** (quindi la matrice k deve essere invertibile).
Queste due decifrature nascondono le frequenze delle singole lettere; se si conoscono *m* coppie testo in chiaro/cifrato, allora si riesce a recuperare la chiave.

Es. P = PAYMOREMONEY

Chiave $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$

m=3, primi 3 caratteri

- PAY = (15, 0, 24)

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \times \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \bmod 26$$

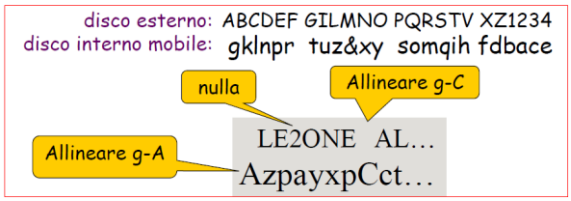
- Testo cifrato: (11,13,18) = LNS

Testo cifrato completo: LNSHDLEWMTRW

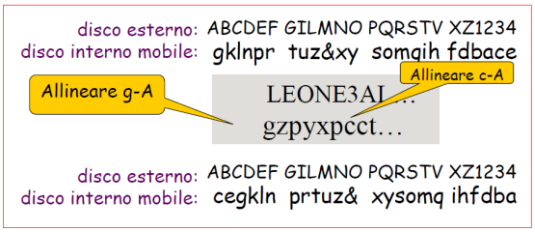
2.4 CIFRARIO DI ALBERTI

Il ***cifrario di Alberti*** usa più alfabeti cifranti (con due dischi uno interno all'altro contenenti due alfabeti, le cui celle sono della stessa dimensione fisica ed il disco interno è mobile) e li sostituisce durante la cifratura, utilizzando due metodi: a ***indice mobile*** e a ***indice fisso***.

INDICE MOBILE



INDICE FISSO

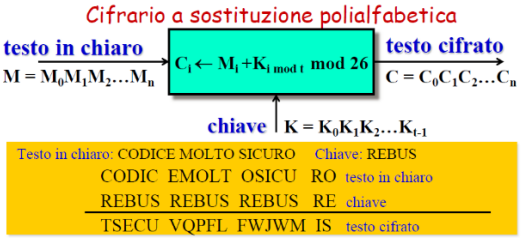


2.5 CIFRARIO DI VIGENÉRE

Il ***cifrario di Vigenère*** funziona come segue: riceve in input il testo in chiaro $M = M_0M_1M_2…M_n$ e la chiave $K = K_0K_1K_2…K_{t-1}$, restituendo il testo cifrato $C=C_0C_1C_2…C_n$, dove $C_i \leftarrow M_i + K_{i \bmod t} \bmod 26$. Ad esempio, abbiamo un testo in chiaro "CODICE MOLTO SICURO" e, usando una chiave "REBUS", si ottiene il testo cifrato "TSECU VQPFL FWJWM IS" in questo modo:

1. si suddivide il testo in chiaro di t in t lettere (dove t è la dimensione della chiave), incolonnando il testo e la chiave (CODIC-REBUS, EMOLT-REBUS, OSICU-REBUS, RO-RE);
2. si esegue la somma con la formula precedentemente scritta.

Il ricevente utilizza una tabella 26x26 dove: la prima riga è costituita da tutte le lettere dell'alfabeto, la seconda riga è costituita dalla prima riga +1, la terza è costituita dalla precedente +1, e così via; effettua l'inverso della formula precedente per riottenere il testo in chiaro.

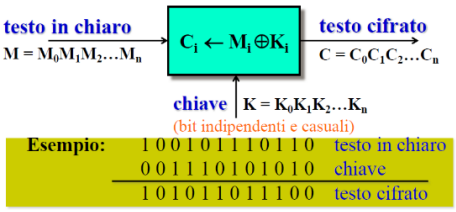


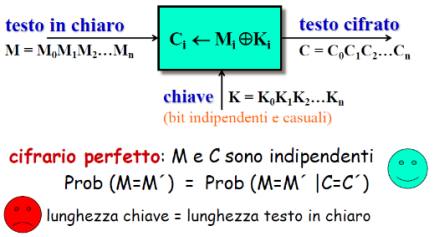
Questo cifrario ha un numero possibile di chiavi pari a 26^t, per cui è stato considerato inviolabile per molto tempo (più è grande la chiave, più è inviolabile la cifratura). Inoltre, resiste all'analisi delle frequenze, in quanto una lettera cifrata corrisponde a più simboli in chiaro. Babbage (1834) e Kasiski (1863) furono i primi a cimentarsi nella crittoanalisi, studiando le ripetizioni ed analizzando le frequenze.

2.6 CIFRARIO PERFETTO (ONE-TIME PAD)

Un cifrario "perfetto" è l'**one-time pad**, creato da Gilbert Vernam nel 1917. Il meccanismo è lo stesso del cifrario di Vigenère, dove invece la chiave ha la stessa dimensione del testo in chiaro ed è scelta casualmente: viene effettuato lo XOR per cifrare il messaggio, ed il ricevente effettua lo XOR con la stessa chiave per ottenere il testo in chiaro.

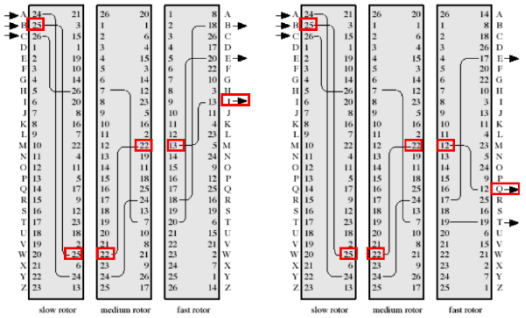
Questo cifrario è praticamente impossibile da violare, in quanto esaminando tutte le chiavi possibili otteniamo anche tutti i messaggi possibili (questo grazie alla casualità della chiave). Un vantaggio risiede nel fatto che M e C sono indipendenti, cioè la probabilità P(M=M') = P(M=M' | C=C'). Tuttavia, lo svantaggio principale risiede nel fatto che la lunghezza della chiave è uguale alla lunghezza del testo in chiaro.





2.7 MACCHINE CIFRANTI

Le **macchine cifranti** erano macchine utili a rendere più efficaci la cifratura e la decifratura.
Il ***cilindro di Thomas Jefferson*** (circa 1800) usava un cilindro di 15cm e 36 dischi di legno che potevano ruotare; i dischi, all'esterno, avevano le varie lettere dell'alfabeto. Il numero dei possibili ordinamenti dei dischi era pari a 36!. Tale cifratura veniva utilizzata in questo modo: si cifravano 36 caratteri per volta, ponendoli sulla stessa riga, in modo tale che il testo cifrato corrispondesse (ad esempio) alla riga di 10 posizioni in basso (quindi, la chiave corrispondeva alla disposizione ordinata dei dischi), si decifrava eseguendo l'operazione inversa.



Le ***macchine a rotori*** (a partire dal 1918) avevano due dischi fatti di materiale isolante, con dei buchi in cui passavano dei fili di rame. In quella di Hebern, ogni cilindro opera una sostituzione monoalfabetica: è facile mettere più cilindri in cascata. I cilindri ruotano: quello più a destra ad ogni lettera cifrata, il secondo dopo 26 rotazioni del primo, il terzo dopo 26 rotazioni del secondo, e così via… Con tre rotori, si hanno $26^3 = 17576$ diversi alfabeti cifranti.

Un altro esempio di macchina a rotori, che ebbe molta diffusione durante la WWII, è la macchina ***Enigma***.