

CIFRARI STORICI

Sono tutti quelli antecedenti a Enigma

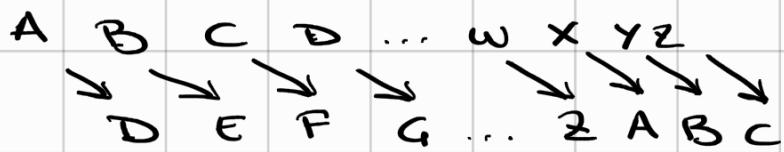
Alfabeto: 26 lettere

Si fa riferimento ai principi di Bacon:

- 1) C, D facili da calcolare
- 2) L'impossibile ricavare D se C non e' nota
- 3) $c = C_{\text{real}}$ deve apparire "innocente" (sembrare un messaggio senza senso compiuto)

CIFRARIO DI CESARE

Il criptogramma c e' costruito dal messaggio in chiaro m sostituendo ogni lettera con quella 3 posizioni più avanti nell'alfabeto (in modo circolare)



- Non ha una chiave
- La segretezza dipende dal metodo

CIFRARIO DI CESARE GENERALIZZATO

Si introduce $1 \leq k \leq 25$; si rota la lettera di k posizioni antiche di 3.

$$\text{pos} : \{A, B, C, \dots, X, Y, Z\} \rightarrow \{0, 1, 2, \dots, 24, 25\}$$

$\text{pos}(x)$ è la posizione di x nell'alfabeto
partendo da 0.

k chiave $\in \mathbb{N}$, $1 \leq k \leq 25$

Cifratura: y : lettera $\leftarrow \text{pos}(y) = (\text{pos}(x) + k) \bmod 26$

Decifratura: $\text{pos}(x) = (\text{pos}(y) - k) \bmod 26$

Crittoanalisi: Si possono provare in breve tempo le 26 chiavi possibili oppure applicare tecniche di crittoanalisi statistiche

es. - Grade di proprietà commutativa

- Date due chiavi k_1, k_2 e una sequenza s vale che

$$C(C(s, k_2), k_1) = C(s, k_1 + k_2)$$

$$D(D(s, k_2), k_1) = D(s, k_1 + k_2)$$

Esistono due tipi di cifrari storici:

CIFRARI A SOSTITUZIONE Si sostituisce ogni lettera del messaggio con una o più lettere secondo una regola prefissata

A TRASPOSIZIONE Si permutano le lettere del messaggio secondo una regola prefissa

CIFRARI A SOSTITUZIONE possono essere di due tipi:

(1) SOSTITUZIONE MONOALFABETICA Alla stessa lettera del

messaggio corrisponde sempre

la stessa lettera nel

cifrogramma

(2)

POLIALFABETICA

Alla stessa lettera del

messaggio corrisponde una lettera

seelta in un insieme I

lettere possibili

(1) Impiegando funzioni C,D piu' complesse lo spazio delle chiavi

e' piu' ampio, la sicurezza e' comunque molto modesta.

CIFRARIO AFFINE

Come Cesare generalizzato, ma:

$$K = (a, b)$$

$$\text{pos}(y) = (a \cdot \text{pos}(x) + b) \bmod 26$$

$$\text{pos}(x) = a^{-1} \cdot (\text{pos}(y) - b) \bmod 26$$

con a^{-1} inverso modulare di a

Vincolo: $\text{MCD}(a, 26) = 1$ per avere chiavente e

unicita' di a^{-1}

(necessario per avere C iniektiva)

e.g. $K = (13, 0)$:

- tutte le lettere in posizioni pari

vengono mappate in $K (\text{pos}(A)=0)$;

- .

dispari

$N (\text{pos}(N)=13)$.

- Quante sono le chiavi possibili?

- $a, 26$ Copioni

$\Rightarrow a$ puo' essere un qualsiasi numero dispari tra 1 e 25

tranne 13

$$\# a = \phi(26) = 12$$

con $\phi(\cdot)$ phi di Eulero

- b puo' assumere 26 valori

$$\Rightarrow 12 \cdot 26 = 312 \text{ chiavi}$$

La coppia $(1, 0)$ non altera il messaggio

$\Rightarrow 311$ possibili chiavi.

(prima erano 25)

Quando la segretezza dipende solo dalla chiave allora il numero delle chiavi deve essere sufficientemente grande da rendere impossibile la forza bruta.

Si puo' espandere lo spazio delle chiavi:

CIFRARIO COMPLETO

Si cifra ogni lettera i del messaggio trasformandola in una lettera scelta in posizione i di una permutatione circolare prefissata.

Lo spazio delle chiavi diventa

$$26! \approx 4 \cdot 10^{26} \text{ chiavi}$$

↳ si scarta la permutazione identica

Il cifrario non e' perciò sicuro, si puo' attaccare sfruttando:

- struttura logica dei messaggi in chiaro;
- occorrenza statistica delle lettere.

Si introducono dunque: CIFRARI A SOSTITUZIONE POLIALFABETICA

CIFRARIO DI AUGUSTO

- I documenti erano scritti in numeri
- Scriveva i documenti in greco, metteva in corrispondenza ogni lettera i del documento con il numero che indicava la distanza nell'alfabeto greco di i con quella in posizione i nel primo libro dell'Eliade

e.g. α in posizione i nel documento

ϵ

nell'Eliade

4

nel ciphogramma

DISCO & LEON BATTISTA ALBERTI

Alfabeto esterno: formato da lettere (alcune) e numeri
per formulare il messaggio

interno: più ricco, disposto in modo arbitrario
e diverso per ogni coppia di utenti

La chiave cambia ogni volta che si incontra un carattere speciale.
inserendone molti e in posizioni irregolari il cifrario diventa difficile
da attaccare e rende inutili gli attacchi basati sulla frequenza
dei caratteri.

Ved. Metodo indice mobile (slide 17)

CIFRARIO DI VIGENÈRE

Sequenza di cifrari + Cesare generalizzati con shift differenti

eg C H I A V E chiave
2 7 8 0 24 4 traslasi
N O N F I | D A R T I | D I E V E messaggi
+ + + + + + + + + +
2 7 8 0 24 2 7 8 0 24 ---
P V V F G H C Y B I . . . crittogramma

La sicurezza dipende dalla lunghezza delle chiavi

poiché lettere uguali in posizioni uguali modulo k
sono cifrate nella stessa lettera

(funzionando dunque come un cifrario monoalfabetico)

ONE-TIME PAD

Si estende il metodo di Vigenere scegliendo una chiave k lunga quanto tutto il testo da cifrare e monouso.

CIFRARI A TRASPOSIZIONE:

PERMUTAZIONE SEMPLICE

Chiave : intero h ;

permutazione π degli interi $\{1, 2, \dots, h\}$

Cifratura : si suddivide in in blocchi di h lettere
di permutano secondo π

oss. Se lsl non è divisibile per h ,

si aggiungono alla fine lettere qualsiasi
(si parla di "padding")

eg $h=9$

$$\pi = \{1 2 5 3 7 6 4 9 8\}$$



Numero delle chiavi : $h! - 1$

Maggiore è h , più forte bruta
diventa difficile

• CIFRARIO A PERMUTAZIONE DI COLONNE

$$K = (c, r, \pi)$$

c, r colonne e righe di T : tabella di lavor.

π : permutazione degli indici $\{1, 2, \dots, c\}$

si decomponga in blocchi di $c \times r$ caratteri

I caratteri sono distribuiti tra le celle di T
scrivendoli in modo regolare

Numero di chiavi: esponentiale in m^m

eg $K = \{6, 3, \{2 \ 1 \ 5 \ 3 \ 4 \ 6\}\}$

$m = \text{NON SONO IL COLPEVOLI}$

N O N S O N

O I L C O L

P E V O L E

O N O N S N

I O O L C L

E P L V C E

C = O I E N O P O O I N L V S C O N L E

• CIFRARIO A GRIGLIA

Griglia $q \times q$ t.c. $\text{par}(q)$

$S = q^2/4$ celle della griglia trasparenti, le altre opache

Si scrivono i primi s caratteri di m nelle posizioni

trasparenti, si ruota di 90 gradi e si ripete

(eg slide 28)