

CRITTOGRAFIA

lezione di lunedì 19 ottobre

ore 11:15

CIFRARI PERPETTI



CIFRARI PERETTI

Shannon 1949

informolente:

"un cifrario è perfetto se la sicurezza è garantita
qualsiasi sia l'informazione corrente del canale"

MSG: spazio dei messaggi

CRITO: spazio dei cointogrammi

M : v.a. che descrive il comportamento del mittente, assume
valori in MSG

C : v.a. che descrive il processo di comunicazione del canale
assume valori in CRITO

$P(M=m)$: probabilità che il messaggio spedito
è il messaggio m

$$\forall m \in MSG \quad \forall c \in CRITO$$

$P(M=m | C=c)$: probabilità condizionata che il messaggio
invio è m , posto che del canale
transita il citoogramma c

Scenari: il crittoanalista conosce tutto del sistema, tranne
le chiavi; conosce:

- distribuzione di probabilità con cui vengono inviati i messaggi
- cifrario utilizzato
- lo spazio delle chiavi (key)

Un cifrario è perfetto se:

$$\forall m \in MSG, \forall c \in CRITO$$

$$P(M=m | C=c) = P(M=m)$$

□

ESEMPIO

$$P(M = \bar{m}) = p > 0$$

$\exists \bar{m} :$

$$0 < p < 1$$

Cifrari non perfetti

es.

$$\exists \bar{c} : P(M = \bar{m} \mid C = \bar{c}) = 1 \quad \} \rightarrow \text{sono } \neq$$

\hookrightarrow se passa sul canale \bar{c} , allora il messaggio
è sicuramente \bar{m}

$\exists \bar{c}$

$$P(M = \bar{m} \mid C = \bar{c}) = 0$$

se passa \bar{c} , allora non è stato spedito \bar{m}

\rightsquigarrow

In un cifrario perfetto, la conoscenza complessiva
del crittanalista non cambia dopo che è stato
osservato un cattogramma in triste

\hookrightarrow m e c sono dati nello stesso
momento nessuna informazione può filtrare dal
cattogramma c

TEOREMA DI STEANON

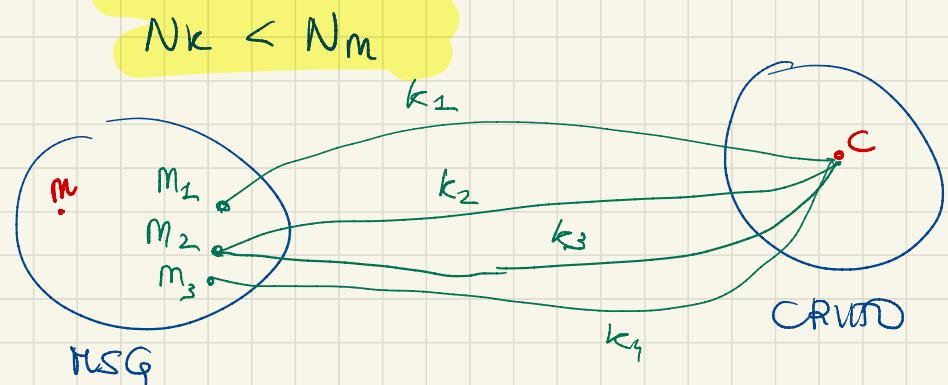
In un cifario perfetto il numero delle chiavi deve essere maggiore o uguale al numero dei messaggi possibili.

DIM

$$\text{#} \quad N_m = \# \text{ dei messaggi possibili} \\ m \in \text{MSG} \quad t.c. \quad P(M=m) > 0$$

$$N_k = \# \text{ delle chiavi}$$

Per assurdo:



$$P(C=c) > 0$$

↓
a c possono corrispondere S messaggi

$$S \leq N_k$$

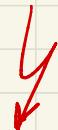
$$S \leq N_k < N_m \Rightarrow S < N_m$$

$$s < N_m$$

$\Rightarrow \exists m \in \text{MSG} \setminus \{s\}, P(N=m) > 0, \text{ t.c.}$

$$P(N=m \mid C=c) = 0$$

\Rightarrow il avviso non è perfetto



One-Time Pad

1917 MAUBORGNE VERNAM

Alf: $\{0, 1\}^n$

MSG, CRUT, KEY = $\{0, 1\}^n$
 $n \geq 0$
sequenze binarie

C, D: usano lo XOR
 $m \xrightarrow{\text{(Somma mod 2)}} c$

$m \in \{0, 1\}^n$ $k \in \{0, 1\}^n$

$$c = C(m, k) = m \oplus k$$

\oplus : XOR bit a bit

$$n = 5$$

$$m = \overbrace{10110}^{5 \text{ bit}}$$

$$k = \overbrace{01011}^{5 \text{ bit}}$$

$$c = 11101$$

$$\begin{array}{r} 10110 \\ 01011 \\ \hline 11101 \end{array}$$

$x \oplus y \oplus y = x \oplus 0 = x$

Decomposizione

$$m = \bigoplus (c, k) = c \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k)$$

$$= m$$

\curvearrowleft
sequenza di 0

ES: $m = 01010101$

$$\begin{array}{r} k = 10110110 \\ \hline 11100011 \end{array}$$

Chiave non utilizzabile

$$\begin{array}{l} K \\ m' \oplus k = c' \\ m'' \oplus k = c'' \end{array}$$

Ese: $c' \oplus c'' = (m' \oplus k) \oplus (m'' \oplus k) = m' \oplus m'' \oplus (k \oplus k)$

$$= m' \oplus m''$$

$\nearrow 0$

TEOREMA

IPOTESI

1) tutti i messaggi hanno lunghezza n

(padding se più corti di n , divisione in blocchi lunghi n se più lunghi di n)

2) tutte le sequenze di n bit sono messaggi possibili

(prob. molto bassa, ma > 0 , decide per le sequenze prime di significato)

3) chiavi scelte perfettamente cas. per ogni messaggio

$$\left(\frac{1}{2^n}\right)$$

Sotto le ipotesi ①, ② e ③, One-time pad è un cifrario perfetto e impiega un numero minimo di chiavi.

DIM (Perfecto)

$\forall m \in MSG, \forall c \in CRYPTO$

$$P(M=m | C=c) = P(M=m)$$

} tesi
=

$$P(M=m | C=c) = \frac{P(M=m \text{ e } C=c)}{P(C=c)}$$

def.

$$= \frac{P(M=m)P(C=c)}{P(C=c)} = P(M=m)$$

x le proprietà dello XOR,
 fissato m , chiavi diverse producono ciphertext diversi
 $\hookrightarrow \exists !$ chiave k t.c.

$$m \oplus k = c$$

$\forall c \in CRYPTO$

$P(C=c) = P(\text{scoprire l'unica chiave t.c. } m \oplus k = c)$

$$= \frac{1}{2^n}$$

$\{M=m\} \text{ e } \{C=c\}$ sono eventi
INDIPENDENTI

(minimale)

$$N_k \geq N_m$$

One Time PAD

$$n \quad N_k = N_m = N_{\text{CRUT}} = 2^n$$

Quindi chiavi sono sequenze di n bit
(come i messaggi e i cattogrammi)

D

ATTA (CFL)

Attack brute force: non ha senso

ogni chiave fa ricevere un messaggio possibile

Osservazione

Rimuoviamo l'ipotesi che tutte le sequenze di n bit sono messaggi possibili

i messaggi significativi per la ~~inglese~~ lingua inglese
sono circa α^n $\alpha = 1.1$

$$\alpha^n \ll 2^n$$

$$N_m = \alpha^n$$

$$N_k \geq N_m \quad N_k \geq \alpha^n$$

le diverse sono una sequenza di t bit con:

$$t: \quad 2^t \geq \alpha^n$$

$$t \geq \log_2 \alpha^n = n \log_2 \alpha = 0.12 * n$$

è opportuno utilizzare (\rightarrow per confondere l'attacco)

dc coppia $\neq (m, k)$ producono lo stesso ciphertext

$\Rightarrow \# \text{coppie } (m, k) \gg \# \text{ciphertext}$

\sim

$$\alpha^n \cdot 2^t \gg 2^n$$

\sim

messaggi

\downarrow

$$t \gg 0.88 \cdot n$$