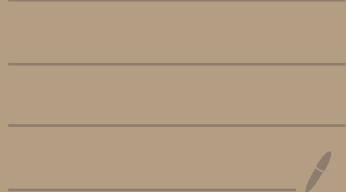


Lezione di
giovedì 14 ottobre '21

CIFRARI PERFETTI
ONE-TIME PAD



Cifron' a sicurezza incondizionata

Cifron' a sicurezza computazionale

} nascondono l'informazione
con certa assoluta

} nascondono l'informazione se
il crittanalista ha accesso a
risorse computazionali limitate
(\rightarrow polinomiali)

P \neq NP

↑

CIFRARI PERFETTI

(Shannon, 1949)

idea intuitiva: "un cifrario è perfetto se la sua sicurezza è garantita qualunque sia l'informazione catturata dal crittanalista sul canale"

MSG : spazio dei messaggi

CRITO : spazio dei campioni

M: visibile obiettivo da descrive il comportamento del mittente, e assume valori in MSG

C: ~~descri~~ visibile obiettivo da descrive la comunicazione sul canale, e assume valori in CRITO

$P(M = m)$: probabilità che il mittente voglia inviare $m \in MSG$

$P(M = m | C = c)$: probabilità condizionale che il messaggio inviato sia $m \in MSG$, posto che all'uscita trasmessa il cointegramma $c \in CRTO$

Un cointegramma è perfetto se

$$\forall m \in MSG, \quad \forall c \in CRTO$$

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

Scenari

il cointegramma comune:

- la distribuzione di probabilità con cui il mittente invia i messaggi
- cointegramma che il mittente invia
- lo spazio delle chiavi

ESEMPIO

$\bar{m} \in \text{RSG}$

1) $P(H = \bar{m}) = p > 0$ $0 < p < 1$

$\exists \bar{c} \text{ t.c. } P(H = \bar{m} \mid C = \bar{c}) = 1$

2) $P(H = \bar{m}) = p \geq 0$ $0 < p \leq 1$

$\exists \bar{c} \text{ t.c. } P(H = \bar{m} \mid C = \bar{c}) = 0$

Teorema di Shannon

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

$m \in MSG$ è un
messaggio possibile
 $\& P(N=m) > 0$

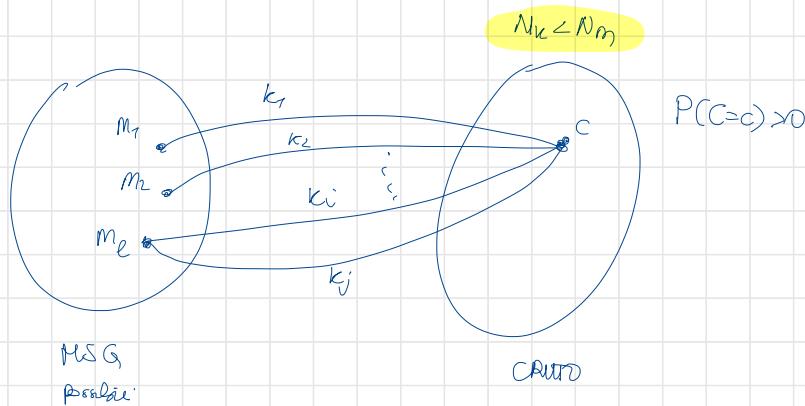
Dim

$N_k = \#$ delle chiavi

$N_m = \#$ dei messaggi possibili

per assurdo si

$$N_m > N_k$$



$S = \#$ messaggi che possono corrispondere al codice parziale c

$$S \leq N_k < N_m$$

$\Rightarrow \exists m^1 \in \text{MSG possibili, che non puo' corrispondere a } c$

$$\underline{P(N = m^1)} = \underline{P} \geq 0$$

$$P(N = m^1 \cap C = c) = 0$$

One-Time Pad

1917 MAUBORGNE - VERNAM

MSG, CRYPTO, KEY = $\{0,1\}^n$

key = spazio delle
chiavi

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

$$C = m \oplus k \quad \oplus : \text{xor bit by bit}$$

CRIPTAZIONE

$$\begin{cases} m = m_1 m_2 \dots m_n \\ k = k_1 k_2 \dots k_i \dots k_n \\ C = C_1 C_2 \dots C_i \dots C_n \end{cases}$$

$$C_i = m_i \oplus k_i \quad 1 \leq i \leq n$$

DECRIPTAZIONE

$$m = c \oplus k \quad \text{bit by bit}$$

$$\forall i, \quad 1 \leq i \leq n$$

$$C_i \oplus k_i = (\underbrace{m_i \oplus k_i}_{\text{ }}) \oplus k_i = m_i \oplus \underbrace{(k_i \oplus k_i)}_0 = m_i \oplus 0 = m_i$$

$$m = 1010101010101010$$

$$k = 100101110001011011$$

$$c = 001111011011110001$$

$$100101110001011011$$

$$101010101010101010$$

$$m_1 \xrightarrow{k}$$

$$c_1 = m_1 \oplus k$$

$$m_2 \xrightarrow{k}$$

$$c_2 = m_2 \oplus k$$

$$\begin{aligned} c_1 \oplus c_2 &= (m_1 \oplus k) \oplus (m_2 \oplus k) = \\ &= (m_1 \oplus m_2) \oplus (k \oplus k) = \\ &= (m_1 \oplus m_2) \oplus 0 = m_1 \oplus m_2 \end{aligned}$$

I POTESI

- ① Tutti i messaggi hanno lunghezza n
(padding se $|m| < n$, ciphatura a blocchi lunghi n se $|m| > n$)
- ② tutte le sequenze di n bit sono messaggi possibili
(si assegna una probabilità molto bassa, $m \gg 0$ ~~ai messaggi~~
alle sequenze binarie prive di significato)
- ③ chiavi scelte perfettamente a caso per ogni messaggio

TEOREMA

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

DIM

1) MINIMETÀ

Righe immediatamente del fatto che

$$N_m = N_k = 2^n$$

2) Cifrario perfetto

$$\left\{ \begin{array}{l} \forall m \in MSG, \forall c \in CRTO \\ \text{tesi} \quad P(M=m | C=c) = P(M=m) \end{array} \right.$$

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

fisso m , chiavi \neq ~~modificare~~: producono ciphertexti \neq

$\exists !$ chiave k che porta un messaggio m fisso in un certo ciphertextone C

$P(C=c)$ = probabilità di scegliere c con l'unica chiesa
che porta m voci c

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

Non dipende da m

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

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



DISCUSSIONE

Proviamo a rimuovere l'ipotesi ②, e considerare solo messaggi significativi.

Perché utilizzare i messaggi significativi? Per $\sim \alpha^n$

$$2^n \rightarrow 1 \cdot 1^n$$

$$\alpha = 1.1$$

$$\underbrace{N_k \geq N_m}_{\text{per}} = \alpha^n < 2^n$$

Possò descrivere le chiavi con t bit, con t . t.c.

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

$$t \geq n \log_2 \alpha \approx 0.12 * n$$

$$n \rightarrow t$$



per confondere il cattivo esiste è opportuno fare i n messaggi
di molte coppie \neq (messaggio, chiave) perché così lo stesso cattivissimo

coppie (messaggio, chiave)

>>

cattivissimo

$N_{\text{cattivissimo}} = 2^n$

chiavi di t bit casuali

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

$$n \log_2 \alpha + t \gg n$$

$$t \gg n - n \log_2 \alpha = n(1 - 0.12)$$
$$\Rightarrow$$

$$t \gg 0.88n$$