Crittografia → Confidenzialità (fino agli anni '70).

ALICE BOB

m

$c = E(m)$ ⟼ c

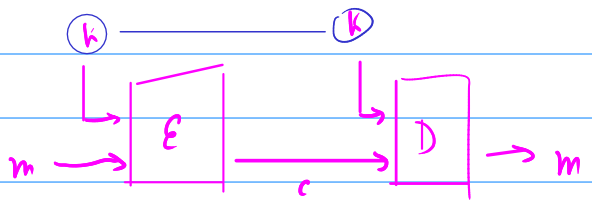
$D(c) = m$

Eve

c

$Pr(m' = m \mid c) = Pr(m' = m)$.

- → NON RIPUDIABILITÀ
- → Autenticazione
- → Firma digitale
- → Anonimità
- → Integrità delle informazioni
  - crittografia
  - teoria dei codici
- → homomorphic encryption → elaborare messaggi criptati senza decodificarli



$\forall k \in K \; \exists k' \in K \; \forall m; D(E(m,k),k') = m$

$k = k'$ → CRITTOGRAFIA SIMMETRICA / A CHIAVE PRIVATA

$k \neq k'$ (è difficile ricavare k' da k)

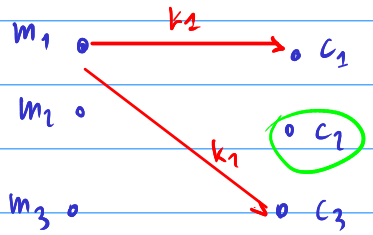
→ CRITTOGRAFIA ASIMMETRICA / A CHIAVE PUBBLICA

Sicurezza nell'ambito della confidenzialità.

EVE vuole ricavare m visto c

1) Non condizionata → EVE può solo scoprire la lunghezza del messaggio.
Non esiste modo per distinguere la codifica $E_{k_2}(m_2)$ dalla codifica $E_{k_1}(m_2)$.

c → Abbiamo visto che l'insieme delle chiavi in questo caso deve avere almeno la stessa cardinalità di quello dei messaggi



2) Sicurezza Dimostrabile

$$Pr(m'=m|c) - Pr(m'=m) < \varepsilon$$

Si dimostra indipendentemente dal modello computazionale selezionato la quantità di informazione che EVE può ricavare da c su m.

3) Sicurezza basata sulla teoria della complessità.

→ Supposto un modello di computazione (Macchina di Turing classica; Macchina di Turing probabilistica; QC; etc. etc.)

ricavare m da c non è possibile in tempo/spazio polinomiale

$O(n^2)$ → $10^{-3} \cdot n^2 + n + 1$

$10^{27} n^2 + 10^{32}$

NP

$p, q \simeq 2^{2024}$ $\quad n = pq$

4) Sicurezza computazionale → Non esistono algoritmi che permettano di risolvere il problema assegnato in tempi brevi/utili

Esempio $\quad n = pq \quad S = \log_2 n \quad p+q \quad O(\sqrt{n}) \quad O(e^{\frac{S}{2}})$

N.B: Si parla di algoritmi lineari se il numero di operazioni è del tipo $ax + \beta$ con x = numero di bit.

$p, q \simeq 2^{512}$

Resistenza con 2^{256} → ALGORITMI A FORZA BRUTA / RICERCA ESAUSTIVA

Tecniche crittoanalitiche che consentono di ridurre lo spazio del problema.

$2^{256} \rightarrow 2^{230}$

AES

5) Sicurezza "ad hoc" → No!!

Principio di Kerckhoff → 1) crittosistema deve essere analizzabile

→ 2) deve essere stato analizzato.

3) bisogna sempre avere un

margine di sicurezza.

N.B La sicurezza computazionale ha una "data di scadenza"

DES 56 bit

AES 128, 196, 256

→ servono protocolli per la sostituzione/revoca/generazione delle chiavi

Strategie di attacco.

1) Known ciphertext → Eve conosce c (e basta).

→ RICERCA DI DISTINGUITORI

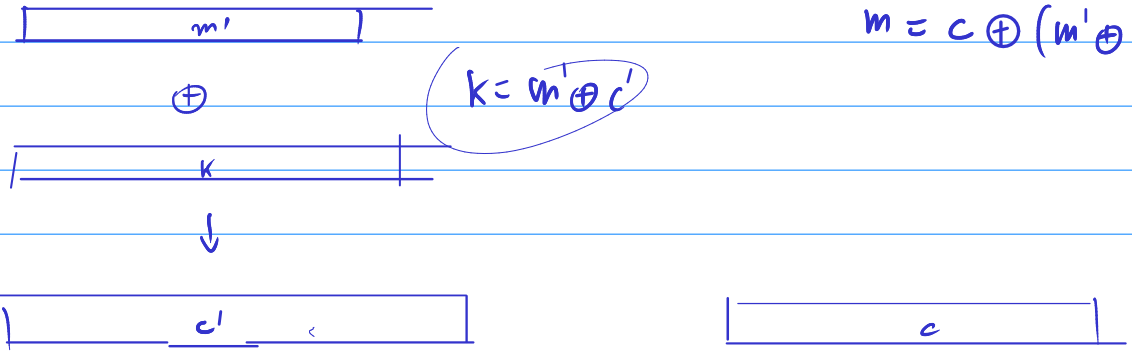
$f(c) = g(m)$ se $m = E_k(c)$ per qualche k

2) Known plaintext → Eve conosce almeno una coppia (m', c') con $c' = E_k(m')$

e vede c

CASA ⟶ DBTB +1 t=1

IPNF → HOME



$m = c \oplus (m' \oplus c')$

3) Chosen ciphertext — EVE HA ACCESSO AD UN ORACOLO CHE

4) Chosen plaintext

a) decodifica ogni messaggio tranne quello che le serve

b) codifica ogni messaggio

ORACOLO (x) { if $c == x \rightarrow$ errore

se $c \neq x \rightarrow D_k(c)$

$$D(2x) = 2D(x)$$

2^{-1} ORACOLO $(2c)$

4) ORACOLO $(x) \rightarrow E_k(x)$

0

5) $(3)+(4)$ ADAPTIVE

ONE TIME PAD → CRITTOSISTEMA PERFETTO

$\mathbb{F}_2 = \{0, 1\}$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

OSS $(\mathbb{F}_2, +, \cdot)$ è un campo

- $(\mathbb{F}_2, +)$ gruppo commutativo
- $(\mathbb{F}_2 \setminus \{0\}, \cdot)$ gruppo commutativo

valgono le prop distributive

$$(a+b)c = ac + bc$$
$$a(b+c) = ab + ac$$

Sia M = spazio dei messaggi $\mathbb{F}_2^n$
k = n delle chiavi ($\mathbb{F}_2^n$)
$[a_1, a_2 \text{ —— } a_n]$

$\bar{m}, \bar{k} \in \mathbb{F}_2^h$ $\quad \mathcal{E}(\bar{m}, \bar{k}) = \bar{m} + \bar{k}$

$$\mathcal{D}(\bar{c}, \bar{k}) = \bar{c} - \bar{k} = \bar{c} + \bar{k}$$

$\text{mod } -1 = 1$

EVE RICEVE
$\bar{c}$

$\forall \bar{m}' \in \mathbb{F}_2^n \ \exists \bar{k}' = \bar{c} + \bar{m}'$ vale che $\bar{m}' + \bar{k}' = \bar{c}$

$$\bar{c} + (\bar{c} + \bar{m}') = (\bar{c} + \bar{c}) + \bar{m}' = \bar{m}' \Rightarrow \bar{c} = \mathcal{E}(\bar{m}', \bar{k}')$$

CRITTOSISTEMA PERFETTO

$\mathbb{K}$ campo $V_n(\mathbb{K})$ s.v. tipo su $\mathbb{K}$ di dimensione n

$$M = K = V_n(\mathbb{K})$$

$$\mathcal{E}(\bar{m}, \bar{k}) = \bar{m} + \bar{k}$$
$$\mathcal{D}(\bar{c}, \bar{k}) = \bar{c} - \bar{k}$$

Known plaintext. Eve sa che $\bar{c}' = \bar{m}' + \bar{K}$

$\Rightarrow$ calcola $\bar{K} = \bar{c}' - \bar{m}'$

vede $\bar{c}$ e calcola poi

$\bar{m} = \bar{c} - \bar{K}$

$$\left.\begin{aligned} \bar{c}_1 &= \bar{m}_1 \oplus \bar{K} \\ \bar{c}_2 &= \bar{m}_1 \oplus \bar{K} \end{aligned}\right] \rightarrow \bar{d} = \bar{c}_1 \oplus \bar{c}_2 = \bar{m}_1 \oplus \bar{m}_2$$

$\downarrow$

DIPENDE SOLO DAI TESTI IN CHIARO

$$d_i = \begin{cases} 0 & \text{se } m_1^i = m_2^i \\ 1 & \text{se } m_1^i \neq m_2^i \end{cases}$$

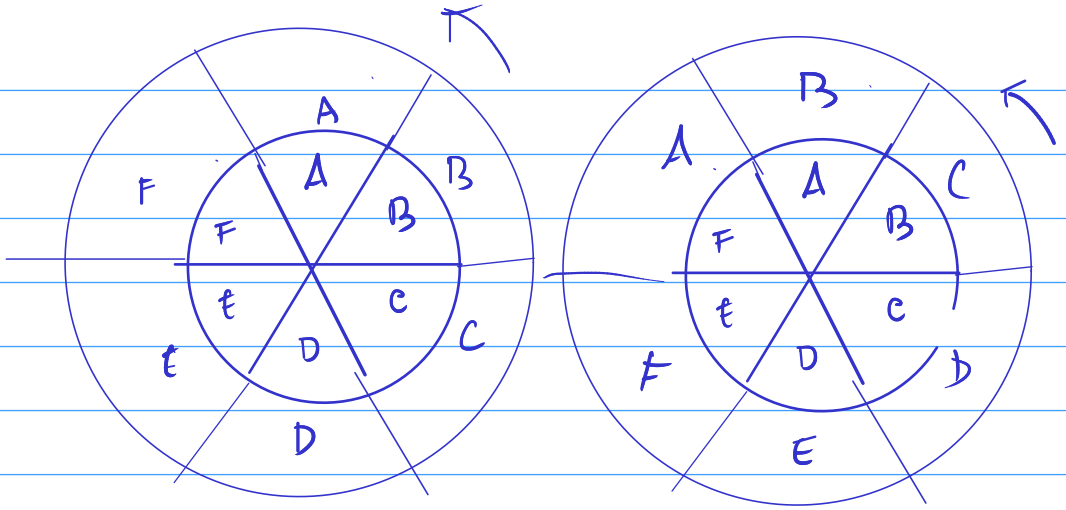
	m_1	m_2
	x	x
	x	x
d_i	0	1

Cercate di indovinare i valori di alcuni m_j^i

$$m_1^1 \oplus c_2^1 = k_1$$

$\{0\ 1 \ldots 25\} = \{A\ B\ C \ldots Z\}$

$$E(\alpha, \beta) = (\alpha + \beta) \% 25$$


A
F
A
B
B
F
E
C
C
D
D
B
A
A
C
F
B
E
D
D
E