

CRIPTOGRAFIA

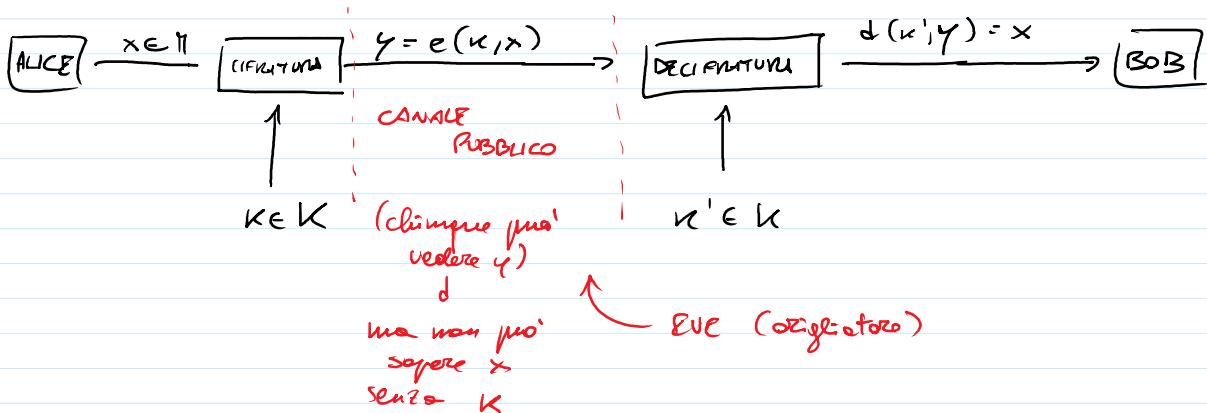
Un sistema crittografico consiste di:

- un alfabeto A insieme finito (e.g. $A = \{A, B, \dots\}$, $A = \mathbb{Z}_n$ o. \mathbb{Z}_{26} $A = \{0, 1, \dots\}$)
- $M \subseteq \bigcup_{n \geq 0} A^n$ possibili messaggi (es. parole nel dizionario) detti PLAIN TEXT
- $C \subseteq \bigcup_{n \geq 0} A^n$ " " CIFRATI (CIPHER TEXT)
- K insieme di chiavi
- $e : K \times M \rightarrow C$ funzione di cifratura (encryption)
- $d : K \times C \rightarrow M$ funzione di decifratura (decryption)

Cifratura $\xrightarrow{\text{chiave}} \text{mess.} \rightarrow \text{mess. cifrato}$

- $S \subseteq K \times K$ insieme di coppie di chiavi (κ, κ') tali che

$$\begin{array}{c} d(\kappa', e(\kappa, x)) = x \\ \downarrow \quad \downarrow \\ \text{decif. con } \kappa' \quad \text{x cifrato con } \kappa \end{array}$$



• Comune con poche certezze/magici

Dos $\forall \kappa \in K \quad e_\kappa = e(\kappa, -) : M \rightarrow C$ è iniettiva (un messaggio ha solo una sua corrispondente cifra)

CIFRARIO DI CESAR

→ no classi di equiv.

$A = M = C = \mathbb{Z}_m$ m>0 spesso \mathbb{Z}_{26} con convenzione $1 \leftrightarrow A, 2 \leftrightarrow B, \dots$
 $\kappa = \mathbb{Z}_m \setminus \{0\} \quad \kappa \in \mathbb{Z}_m, \kappa \neq 0$ (altrimenti non si cifra)

$$e(\kappa, x) = x + \kappa$$

$$d(\kappa, y) = y - \kappa$$

Cesare scrive spesso $\kappa = 3$

$$x = \text{CESAR} = 3 \mid 1 \mid 5 \mid 13 \mid 1 \mid 18 \quad \text{PLAIN TEXT} \quad (\text{messaggio in chiaro})$$

$$\kappa = 3 \quad y = e(3, x) = 6 \mid 4 \mid 8 \mid 22 \mid 4 \mid 18 \mid 21$$

$$n = 3 \quad \gamma = e(3, \times) = 6 | 9 | 8 | 22 | 4 | 18 | 21$$

$$= F | D | 14 | V | D | U \quad \text{cypher text}$$

è un sistema simmetrico (chiave di cifratura = "di decifratura")

$$S = \{(u, u) : u \in K\}$$

Problema:

- il destinatario deve sapere a priori la chiave

- può forzare il sistema ponendo a forza vari SHIFT

(oss soggetto ad attacco di forza bruta)

ci sono soltanto $m - 1$ possibili chiavi
(non ho lo zero)

CRIPTOSISTEMA RSA (RIVEST, SHAMIR, ADLEMAN, 1978)

E' un sistema a chiave pubblica: non è possibile ottenere (in tempo ragionevole) la chiave di decifratura conoscendo quella di cifratura.

$p, q \in \mathbb{Z}$ primi "grandi" ($e.g. p, q \sim 2^{512} \sim 10^{150}$), $n = p \cdot q$

$$C = m \in \mathbb{Z}_n, \quad k = \mathbb{Z}$$

$$\begin{matrix} E & : & \mathbb{Z} \times \mathbb{Z}_n & \rightarrow & \mathbb{Z}_n \\ (e, m) & \mapsto & m^e & & \end{matrix}$$

$$\begin{matrix} D & : & \mathbb{Z} \times \mathbb{Z}_n & \rightarrow & \mathbb{Z}_n \\ (d, c) & \mapsto & c^d & & \end{matrix}$$

$$S = \{ (e, d) \in \mathbb{Z} \times \mathbb{Z} \mid e \cdot d \equiv 1 \pmod{\varphi(n)} \}$$

$$\varphi(n) = \varphi(p \cdot q) = (p-1) \cdot (q-1)$$

insieme di chiavi
chiave di cifratura chiave di decifratura

Verifica di correttezza

$$(e, d) \in S$$

$$D(d, E(e, m)) = D(d, m^e) = m^{ed} \quad \text{in } \mathbb{Z}_n \quad \forall m \in \mathbb{Z}_n$$

$$e \cdot d \equiv 1 \pmod{\varphi(n)} \rightarrow ed = 1 + t \cdot \varphi(n) \quad t \in \mathbb{Z}$$

multiplo di $\varphi(n)$

$$m^{ed} = m^1 \cdot m^{t \cdot \varphi(n)} = m \cdot (m^{\varphi(n)})^t \quad \underline{\text{EULERO}} \quad m \cdot 1 = m \quad \text{in } \mathbb{Z}_n$$

PUBBLICO: $n, e \rightarrow \text{Alice}$

SEGRETTO: $p, q, \varphi(n), d \rightarrow \text{Bob}$

voule mandare un messaggio a

(ognuno ha le sue chiavi)

ES Bob sceglie $p = 101$ e $q = 113$ (più grandi = più sicurezza)

- Calcola $n = p \cdot q = 11413$
- Calcola $\varphi(n) = (100) \cdot (112) = 11200$
- Sceglie $e = 3533$ (vuole $b \in \mathbb{Z}$ t.c. $\text{gcd}(e, \varphi(n)) = 1$) "e" invertibile
- Bob calcola $d = e^{-1} = 6557 \pmod{\varphi(n)}$
- Bob pubblica la sua chiave $(n, e) = (11413, 3533)$, il resto è segreto
- Alice vuole mandare il messaggio $m = 3726 \in \mathbb{Z}_m = \mathbb{Z}_{11413}$
- Alice calcola $c = m^e = 3726^{3533} = 5761 \in \mathbb{Z}_{11413}$ e lo manda a Bob
- Bob calcola $c^d = 5761^{6557} = \underline{3726} \in \mathbb{Z}_{11413}$

Eve conosce n, e, c e vuole trovare m (o d)

→ Eve non conosce p e q e non sa come calcolare $\varphi(n)$ e quindi
 $d = e^{-1} \pmod{\varphi(n)}$

Il sistema è rotto se Eve riuscirà a calcolare $n = p \cdot q$ e quindi può calcolare

$$\varphi(n) = (p-1)(q-1)$$

? Conoscere $\varphi(n)$ permette di fattorizzare n

$$\varphi(n) = (p-1)(q-1) = \cancel{p} \cancel{q} - p - q + 1 = n$$

possiamo calcolare

$$\rightarrow p + q = n + 1 - \varphi(n)$$

summa prodotto

Calcoliamo p e q come radici di $x^2 - (p+q)x + n = 0$.

Teorema dei numeri primi

$$\pi(x) = \#\{p \text{ primo} \mid p \leq x\}$$

$$\pi(2) = 2 \quad \pi(10) = 4 \dots$$

$$\pi(x) \sim \frac{x}{\log x}$$

distruzione = sintetica

Fissato A - "alfabeto" un insieme

$$S = S_A = \bigcup_{n \in \mathbb{N}} A^n \quad \text{gli elementi di } S \text{ si chiamano STRINGHE}$$

$$\alpha \in S \rightarrow \alpha \in A^n \text{ per qualche } n \in \mathbb{N}$$

$\alpha = (a_1, \dots, a_n)$
esempio ordinato
 \downarrow
 a_1, \dots, a_n

$$n=0 \quad \alpha \in A^0 \text{ definiamo } \alpha = () \quad \text{STRINGA VUOTA}$$

$$\text{dato } \alpha \in S \quad l(\alpha) = n \text{ se } \alpha \in A^n \quad \text{LUNGHEZZA DELLA STRINGA}$$

$$l: S \rightarrow \mathbb{N}$$

Def $\alpha = (a_1, \dots, a_n), \beta = (b_1, \dots, b_m) \in S_A$

$$\alpha @ \beta = (a_1, \dots, a_n, b_1, \dots, b_m) \quad \text{CONCERNENZA DI } \alpha \text{ e } \beta$$

$$\alpha @ () = () @ \alpha = \alpha \quad \text{la stringa } \alpha \text{ rimane invariata}$$

$@: S \times S \rightarrow S$ OPERAZIONE BINARIA ASSOCIAUTIVA e non commutativa (tranne per casi particolari)
e con elemento neutro la stringa vuota

$$(S_A, @, ())$$

TRONO DELLE STRINGHE SU A
(TRONO LIBERO SU A)

Oss Ci sono elementi invertibili? A parte le stringhe vuote non ve ne sono altri.

$$\alpha \in S, \alpha @ () \quad \alpha = (a_1, \dots, a_n) \rightsquigarrow \exists \beta \text{ t.c. } \beta @ \alpha = () \quad \text{No}$$

Def β è un **prefisso** di α (\Rightarrow una testa di α) se $\exists \gamma \in S$ t.c. $\alpha = \beta @ \gamma$

cioè d' inizia con β

β è un **suffisso** di α (\Rightarrow una coda di α) se $\exists \gamma \in S$ t.c. $\alpha = \varepsilon @ \beta$

β è una **sottostringa** di α se $\exists \varepsilon, \eta \in S$ t.c. $\alpha = \varepsilon @ \beta @ \eta$

lo vale anche $()$

N.B. α è una sottostringa di se stessa

Def Definiamo una relazione d'ordine su S_A

$$\alpha \Delta \beta \iff \exists \gamma \in S_A \quad \gamma @ \alpha = \beta \quad \alpha \text{ coda di } \beta$$

Verifichiamo:

$$1) \Delta \text{ riflessiva} \quad \alpha \Delta \alpha \text{ vero, perché } \alpha = () @ \alpha$$

Proprietà:

1) Δ riflessiva $\alpha \Delta \alpha$ vero, perché $\alpha = () @ \alpha$

2) Δ antisimmetrica $\alpha \Delta \beta \wedge \beta \Delta \alpha \stackrel{?}{\rightarrow} \alpha = \beta$

$\alpha \Delta \beta \wedge \beta \Delta \alpha \rightarrow \exists s, s' \in S \text{ t.c. } \beta = s @ \alpha \wedge \alpha = s' @ \beta \parallel \alpha = s' @ s @ \alpha$

$\rightarrow s @ s = ()$ per aver verificato l'uguaglianza

$\rightarrow s' = s = () \rightarrow \beta = s @ \alpha = () @ \alpha = \alpha \quad \beta = \alpha$

3) Δ transitiva $\alpha \Delta \beta, \beta \Delta \gamma \stackrel{?}{\rightarrow} \alpha \Delta \gamma$

$\alpha \Delta \beta \rightarrow \beta = s @ \alpha$

$\beta \Delta \gamma \rightarrow \gamma = s' @ \beta \quad s, s' \in S \parallel \gamma = s' @ s @ \alpha = \gamma @ \alpha$

$\exists \eta \rightsquigarrow \gamma$

Oss. Δ non è un ordine totale (o meno di $A = 1$ (simbolo)) $A = \{1, 2, 3, 4\}$

$\alpha = (1, 2) \quad \beta = (3, 4, 1) \quad \nexists s \in S_A \text{ t.c. } \beta = s @ \alpha$

α e β non sono confrontabili

$\nexists s \in S_A \text{ d.c. } \alpha = s' @ \beta$

Oss. Esiste il minimo di (S_A, Δ) è la stringa vuota $()$

$() \Delta \alpha \quad \forall \alpha \in S_A$

N.B. $S_\Delta = \bigcup_{n \in \mathbb{N}} A^n = A^0 \cup A^1 \cup A^2 \cup \dots$ quindi $() \in S_A$ è un elemento di S_A

Cardinalità di S_A ?

Se A è un insieme finito o numerabile allora $S_A = \mathbb{N}_0$ perché viene numerabile di insiemi finiti o numerabili

Oss. Il poset (S_A, Δ) è BEN CONDOTTO ogni sottoinsieme non vuoto ha un elemento minimo

$\forall \alpha \in S_A, \alpha \neq \emptyset \rightarrow \exists \alpha' \in S$

$\alpha = (z_1, \dots, z_n)$ quali sono gli elementi che precedono α ?

$(\Delta(z_n), \Delta(z_{n-1}, z_n), \dots, \Delta(z_2, \dots, z_n), \Delta(z_1, \dots, z_n)) \Delta(z_1, \dots, z_n) = \alpha$

ma tutti questi elementi stanno necessariamente in S .

Prendo il più piccolo degli elementi della catena precedente che sta in S .

Questo sarà un elemento minimo di S

Ps (S_A non è ben ordinato)

$$A = \{1, 2, 3, 4\} \quad S = \{\alpha, \beta\} \quad \alpha = \{1, 2\} \quad \beta = \{3, 4, 1\}$$

S non ha minimo, $\Delta(\alpha) \Delta (\beta) = \alpha$

ma le due elementi $\Delta(\alpha) \Delta (\beta) = \beta$

minimali $\alpha \cdot \beta$

non sono confrontabili

es

Definiamo cons: $A \times S_A \rightarrow S_A$

$$(\alpha, \alpha) \mapsto (\alpha, \alpha) = (\alpha, \alpha_1, \alpha_2, \dots, \alpha_n) \Rightarrow \alpha = (\alpha_1, \dots, \alpha_n)$$

Proprietà'

- cons è iniezione
- $(\) \notin \text{cons}(A \times S_A)$ (non è immagine), ho sempre un elemento α

• PRINCIPIO DI INDUZIONE STRUTTURALE

Se $X \subseteq S_A$ tale che

1) $() \in X$ aggiungi un elemento x a X caso base

2) $\forall x \in A, \forall \alpha \in X \rightarrow \text{cons}(x, \alpha) \in X$ caso induutivo

Allora $X = S_A$ X contiene tutte le possibili stringhe