Sessioni future:

Gennaio/Febbraio 2023 → gennaio: CS, SAW, SSGS, TAP; febbraio: FIS

Giugno/Luglio 2023 → IOT, EC, WD, PCAD

Settembre 2023 → APA, TDII

Gennaio/Febbraio 2024

Cryptography

transposition cipher

scramble the letters → infeasible with statistical analisys

substitution ciphers

$1 \leq l \leq 8$ 10.000 p/s

0..127

| | | | | | | |

127^8 password

$127^8 \cdot 127^7 \cdot \ldots \cdot 127^2$ = password possibili

$= \prod_{i=2}^{8} 127^i$

$$\frac{10.000}{\prod_{i=1}^{8} 127^i} = \checkmark$$

2. ***Crittografia***

Un sistema consente all'utente di scegliere una password con una lunghezza minima di un carattere e massima di 8 caratteri. Si assuma che sia possibile testare 10.000 password al secondo. L'amministratore di sistema vuole disabilitare le password non appena si abbia la probabilità 0.1 che sia stata scoperta.

Si determini il tempo medio dopo con cui questa probabilità viene raggiunta nel caso in cui i caratteri con cui sono formate le password siano:

(a) *Caratteri ASCII con codici da 1 to 127, estremi inclusi.*

Soluzione.

(b) *Caratteri alfanumerici (da 'A' a 'Z,' da 'a' a 'z,' e da '0' a '9').*

Soluzione.

(c) *Numeri (da '0' a '9').*

Soluzione.

$$\prod_{i=1}^{8} 62^i$$

$$\prod_{i=1}^{8} 10^i$$

2. **Public-key Cryptography**

(a) Which of the following activities are carried out by a smartcard?

A. take as input a document, compute the hash code of the document and encrypt it with a public key stored in the smart card, and return the result.

B. take as input a document, compute the hash code of the document and encrypt it with a private key stored in the smart card, and return the result.

C. take as input a sequence of bit, encrypt it with a private key stored in the smart card, and return the result.

D. take as input a sequence of bit, encrypt it with a public key stored in the smart card, and return the result.

(b) Alice must send a large file M to Bob in such a way to ensure both the confidentiality and the authenticity of the message. Which of the following procedures is most suited for the task?

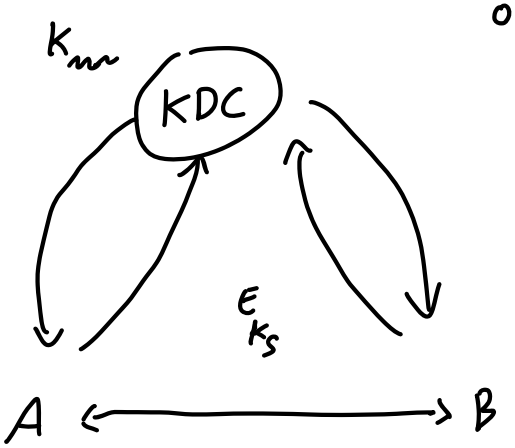
A. Alice computes and sends Bob the ciphertext obtained by encrypting M with Bob's public key.

B. Alice generates a (pseudo)random symmetric key K and sends Bob
- the ciphertext obtained by encrypting M with K and
- the ciphertext obtained by first encrypting K with her own private key and then encrypting the result with with Bob's public key.

C. Alice generates a (pseudo)random symmetric key K and sends Bob
- the ciphertext obtained by encrypting M with K,

$A \to B : E(K, [A, B, T])$

A manda a B $[A, B, time()]$ criptato con E_K



A -> 5 , B -> 8 $\quad q = 11 \quad \alpha = 2$

$Y_A = \alpha^{X_a} \bmod q \qquad 5 = (2^{X_a} \bmod 11)$

$Y_b = \alpha^{X_b} \bmod q \qquad 8 = (2^{X_b} \bmod 11)$

$2^x \bmod 11 = 5 \rightarrow 16 \bmod 11 = 5 \rightarrow X_a = 4 \qquad X_b = 3$

$2^x \bmod 11 = 8 \rightarrow 8 \bmod 11 = 8$

$K = Y_b^{X_a} \bmod q = 8^4 \bmod 11 = 4096 \bmod 11 = 4$

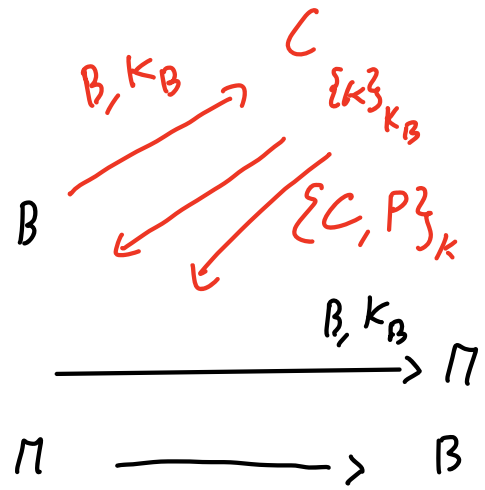
$= Y_a^{X_b} \bmod q = 5^3 \bmod 11 = 125 \bmod 11 = 4$

$4096 \mid 11$
$79 \quad 372$
26
4

① $B \rightarrow M : B, K_B$ — Confidenzialità di K

② $M \rightarrow B : \{K\}_{K_B}$ — non garantisce non-ripudio

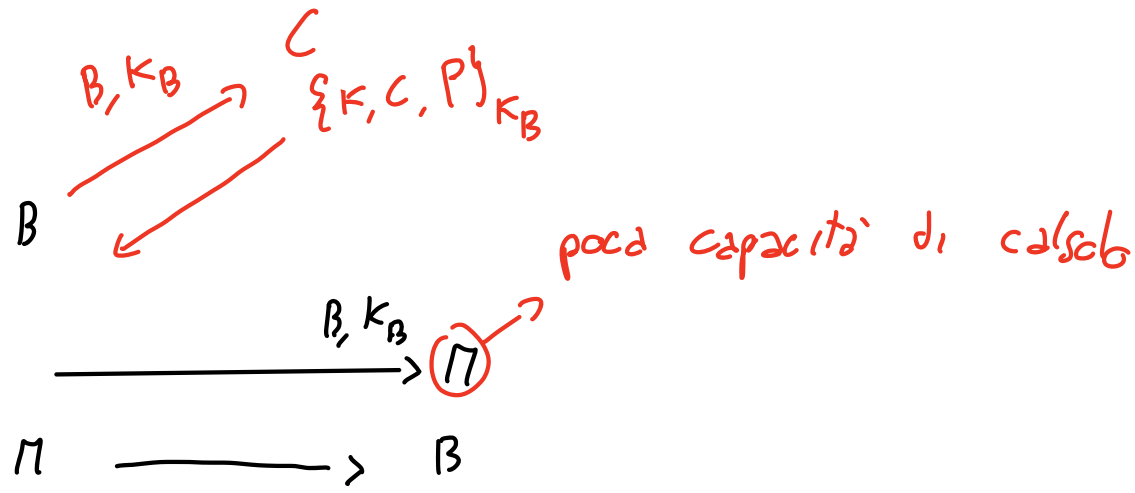
③ $M \rightarrow B : \{M, P\}_K$ — confidenzialità P



M ⟶

B -> M : B, K_B

M -> B : $\{K, M, P\}_{K_B}$



1. conf. di K e P
2. auth di M per B

garantita auth da B -> M
confid. di K_B

- B cert. = $\{B, K_B\}_{K_C^{-1}}$
- M conosce K_C

② B -> M : $\{B, K_B\}_{K_C^{-1}}$

② M -> B : $\{K\}_{K_B}$

③ M -> B : $\{M, P\}_K$

Bisogna autenticare M

- $\{M, K\}_{K_B}$

N, $\{B, K_B\}_{K_C^{-1}}$

$\{K\}_{K_B}$

$\{N, M, P\}_K$

② secret ② top-secret (No read up)

se payload (top secret) ② payload (secret) => W

② secret ③ confidential (No write down)

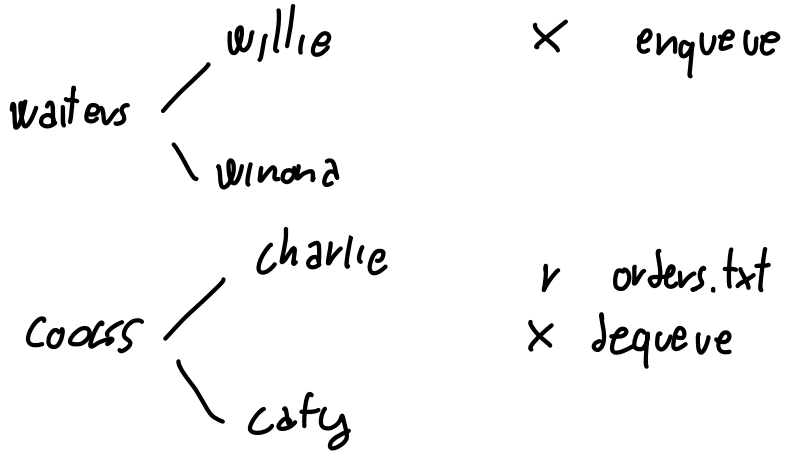
se payload (secret) ③ payload (confidential) => R

secret = secret (② ∪ ②)

{Red, green, blue} > {red, green} => R

{red, green} < {Red, green, blue} => W

{red} = {red} => RW



manu - manu rwx orders.txt

rw- r-- --- manu cooks orders.txt

---s --x --- mario waiters enqueue

---s --x --- mario cooks dequeue

Il bit setuid è importante perchè i programmi leggono e scrivono su orders.txt. Per farlo, servono i permessi di mario

PC A

$PC \rightarrow A : H(M)$

$A \rightarrow PC : \{H(M)\}_{PR_A}$

$PC : \{\{H(M)\}_{PR_A}\}_{PU_A} = H(M)$

n di transposition cipher : $n!$ (n numero d. caratteri nel messaggio)

n di substitution cipher : $|A|!$ ($|A|$ = numero d. caratteri nell'alfabeto)

$4 = 1000 \qquad \frac{3}{10.000} = 0.0003$

0000 -> 9999 A...F 0..5

0...9A...F

0...90...5 0...9

0...9 0...9

1234 3921

$(secret, \{dog, cat, pig\}) = S$

s_1 (top-secret, {dog}) : niente

s_2 (secret, {dog}) : $pay(S) > pay(s_2) \Rightarrow R$

s_3 (secret, {dog, cow}) : niente

s_4 (secret, {moose}) : niente

s_5 (confidential, {dog, pig, cat}) : $pay(S) = pay(s_5) \Rightarrow R$

n $K_1, \dots, K_n$

P_n

K_1
↑
$P_n[1, \dots$

1. $(\{K \oplus P_K\}_{K_C}, P_K)$

se P_K^2 viene modificato, ho $P_K \neq P_K^2$, quindi posso genere un risultato K insabile

→ inteso come "sicuramente compromesso"

2. $(\{K\}_{K_C \oplus P_K}, P_K)$

$P_K \oplus K_C \neq P_K^2 \oplus K_C$ (se $P_K \neq P_K$), quindi genero una chiave insabile perché cripto con una chiave diversa

3. $(\{K\}_{K_c} \oplus P_K, P'_K)$

$P_K \oplus P'_K \oplus \{K\}_{K_c} = \{K\}_{K_c}$ se $P_K = P'_K$

se $P_K \oplus P'_K \oplus \{K\}_{K_c} \neq \{K\}_{K_c}$, significa che $P_K \neq P'_K$, quindi ho un ciphertext diverso da $\{K\}_{K_c}$ (quindi una chiave invalida)

$(\text{Nome}, \text{PU}, \text{Certificatore})[K_{cert.}]$

example.com aruba.it

uid=1000 gid=1000 groups=1003

	1	2	3	4	
alice	r w A	r w A	r	r A	
bob	r	r w A	r	r w A	
charlie	r	r w	r w	r	

Append ./