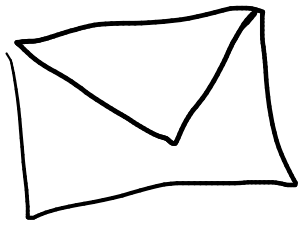
7 26/11

[Breve storia della crittografia, Fermat, crittografia simmetrica e asimmetrica, aritmetica modulare e proprietà, Algoritmo di Diffie-Hellman.

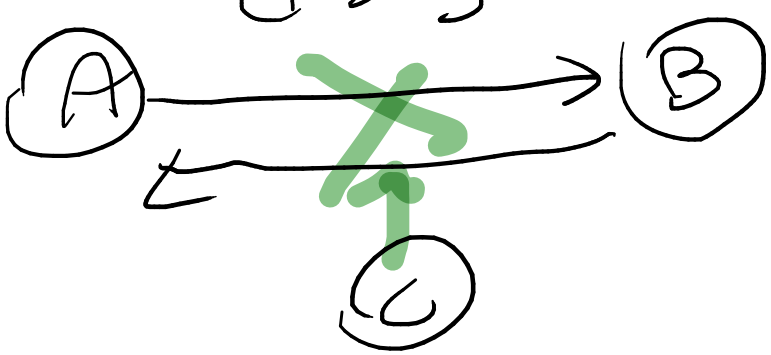
↓

[CRITTOGRAFIA



CONFIDENZIALE
INTEGRA
DISPONIBILE]

[RSA]



MAN
IN
THE
MIDDLE

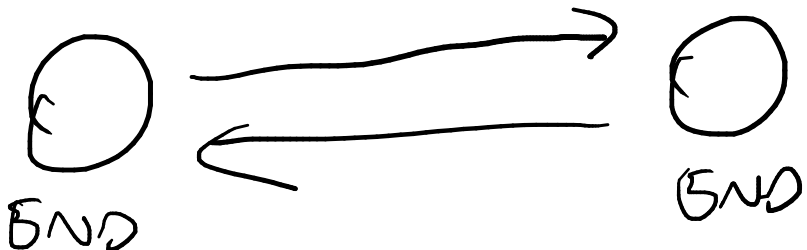
(C)

Tra A e B resta
tutto segreto!

→ (STORIA)

[END - TO - END]

END =
SISTEMA



ALGORITMI

→ RSA [RIVEST SHAMIR ADLEMAN]

[NUMERI PRIMI] → [5 / 5 ; 5 / 1]

DIVISIBILI PER SE STESSO

DIVISIBILI PER 1

↓

ARITMETICA MODULARE

$5 \bmod 2 = [1]$ → RESTO

$(2 * 2) + [1] = 5$ (RESTO)

↳ RIS. DIVISIONE → $5/2 = 2$

$7 \bmod 3 = [1]$ → RESTO

$(3 * 2) + [1] = 7$

↳ RIS. DIVISIONE → $7/3 = 2$

ARITMETICA MODULARE → (WITH) NUMERI PRIMI!

NUMERI PRIMI = NUMERI UNICI → SI POSSONO RAPPRESENTARE SU SÉ STESSI

7 mod 1
8 mod 1
9 mod 1

7/1
8/1
9/1

MULTIPLI (mod "n")

OGNI NUMERO DIVISO PER N (1) DÀ SEMPRE IL N. STESSO

ES.

314 / 24 = 13

314 = (13 · 24) + 2 → resto

→ MODULO (operazione)

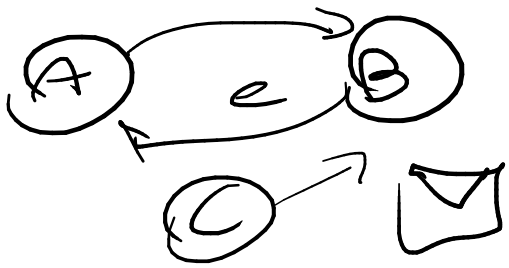
RSA → 2 3

P Q

155873

MOLTO GRANDE! (circa)

CRITTOGRAFIA ⇒



"C" NON LO DEVE CAPIRE!

= NUMERI PRIMI

[GARANTISCONO
UNICITÀ
E NON
INTERCETTABILITÀ DA PARTE DI C"]

[DIFFIE - HELLMAN]

① A e B conoscono "g" e "p" numeri pubblici

② A conosce un num. segreto "a"

③ B conosce un num. segreto "b"

(4)

A calcola $A = g^a \bmod p$ e lo comunica a B
B calcola $B = g^b \bmod p$ e lo comunica a A
A calcola $K = B^a \bmod p$
B calcola $K = A^b \bmod p$
Ma:

$$K = B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ba} \bmod p$$
$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$$

PASSAGGI VARI ...

A e B concordano un segreto (numero K) senza comunicarlo!

DIVISIONI E MOLTIPLIC.

⇓

K calcolabile solo conoscendo ["a" e "b"] = numeri segreti!

SIMMETRICA

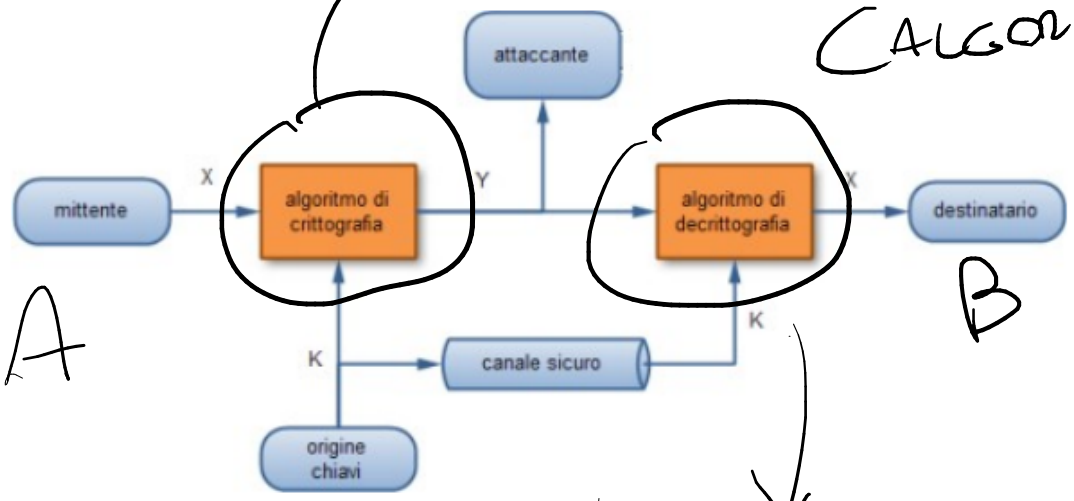
A ⟷ B

(ALGORITMO)

(A e B) → li conoscono!

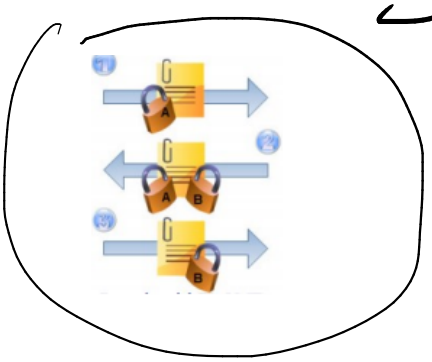
A e B usano lo stesso algoritmo!

RSA / DIFFIE-HELLMAN ...
(ALGORITMI)



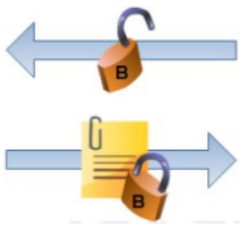
DECODIFICA

[TRASMISSIONE CHIAVE]



CHIAVE = "CAPIAMOCI"!

(ALICE) A B (BOB)

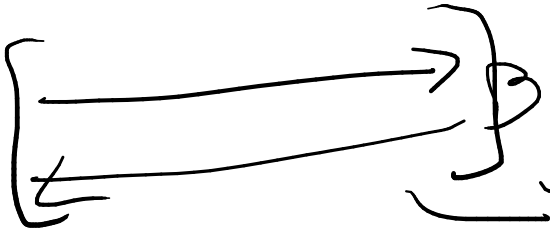
A  B]

SIMMETRICA = USIAMO LO STESSO ALGORITMO

SE NOI AMBIAMO LA CHIAVE →

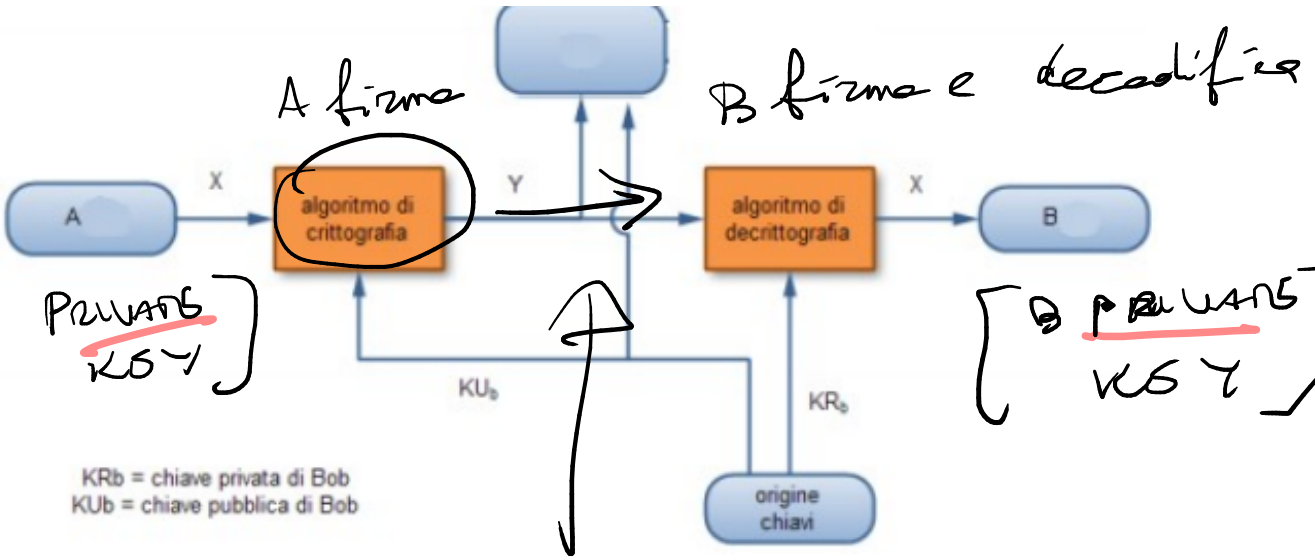
$C=F(M)$	facile	→ LOGARITMO
$M=F^{-1}(C)$	difficile se non si conosce la chiave	DIFFICILE TRANNE INDIETRO

CIFRARE PER A e B)

A  B

FUNZIONE DIFFICILE

ASIMMETRICA → CHIAVE PRIVATA
CHIAVE PUBBLICA



[A PRIVATE KEY]

[B PRIVATE KEY]

(A) CHIAVE PUBBLICA (B)

A → CHIAVE PRIVATA / CHIAVE PUBBLICA

B → CHIAVE PRIVATA / CHIAVE PUBBLICA

↓

ASIMMETRICA

La crittografia asimmetrica evita il problema classico della crittografia simmetrica connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura. → PROBLEMA

Il meccanismo della crittografia asimmetrica si basa invece sulle seguenti assunzioni:

- la chiave privata non è ricavabile dalla chiave pubblica (o almeno non è facilmente ricavabile)
- se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.

RSA → 2 NUMERI PRIMI E OPERAZIONI DIFFICILI DALL'ESAMO!

- Scegliere **due numeri primi** **p e q**
- Calcolare **n = pq**
- Occorre sapere **quanti sono i numeri compresi tra 1 e n che siano coprimi con n** per sceglierne uno
- La φ(n) di Eulero serve a tale scopo e Il risultato è **f = φ (n) = (p – 1)(q – 1) = n – p – q + 1**.
- Scegliere **e** **1 <= e < (p-1) (q-1)** *con **e** coprimo con* φ(n)
- Calcolare **d** tale che **de ≡ 1 mod (p-1) (q-1)** che sarà compreso tra 1 e φ(n)
- La coppia **(n, e)** *è la **chiave pubblica di Bob***
- La coppia **(n, d)** *è la **chiave privata di Bob***
- Non è possibile risalire facilmente dalla chiave pubblica a quella privata (e viceversa), in quanto servirebbe conoscere il numero (p-1)(q-1), e questo implica fattorizzare n nei suoi fattori p e q (problema difficile)