26/11

SISTEMI. Compito scritto in classe su foglio protocollo.
Argomenti del compito:
Breve storia della crittografia, Fermat, crittografia simmetrica e asimmetrica, aritmetica modulare e proprietà, Algoritmo di Diffie-Hellman.

CRITTOGRAFIA = A e B

CONFIDENTIALITY = A e B SI CAPISCONO SOLO LORO

INTEGRA = IL PACCHETTO ARRIVA TUTTO

DISPONIBILITÀ = A e B HANNO UN CANALE SOLIDO

END-TO-END

END = OSTACOLO

END END

STORIA → ALGORITMI → RSA, DIFFIE-HELLMAN, AES

(CIFRARI USATI)

CRITTOGRAFIA

SIMMETRICA

A ⇄ B

↑

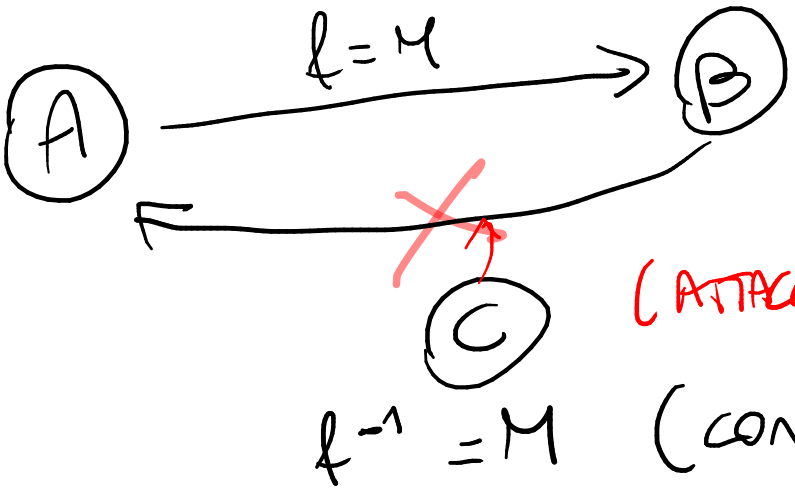
ALGORITMO
(CAES / RSA / DH ...)

ASIMMETRICA

A ⇄ B

ALGORITMO
+
CHIAVI
(PRIVATA / PUBBLICA)

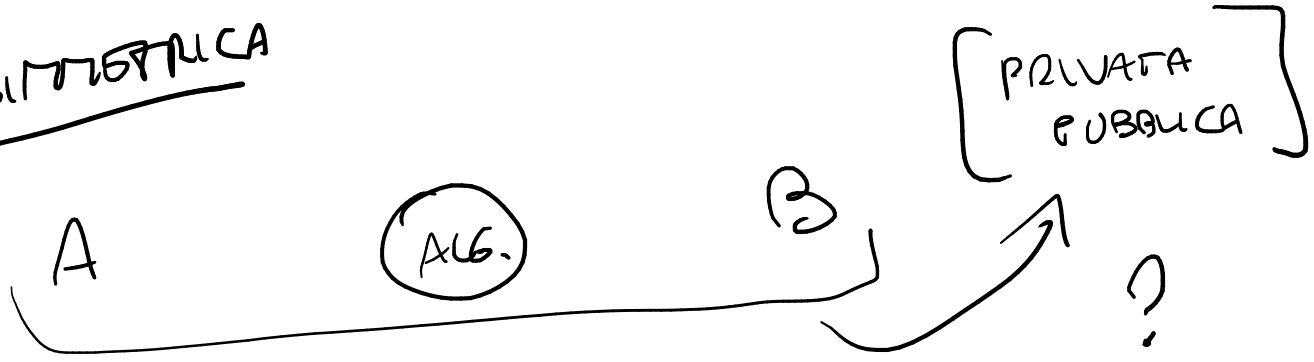
SIMMETRICA

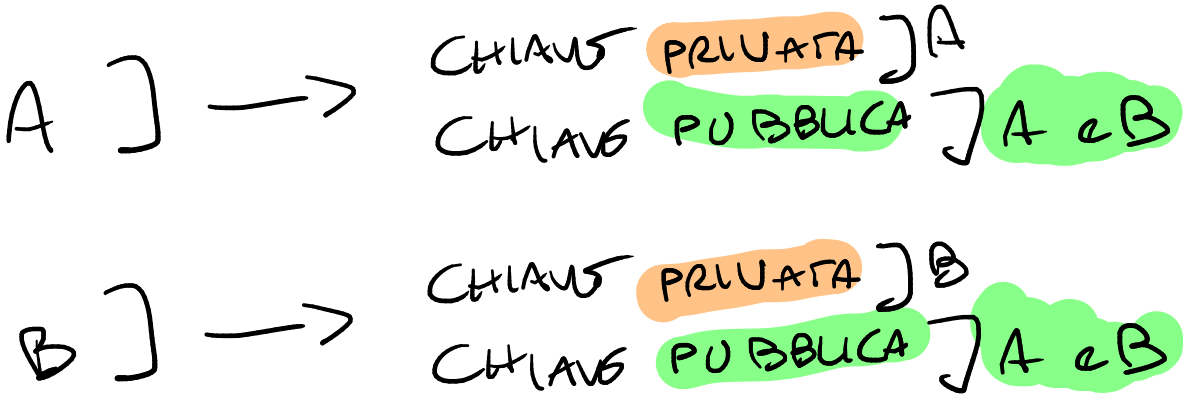


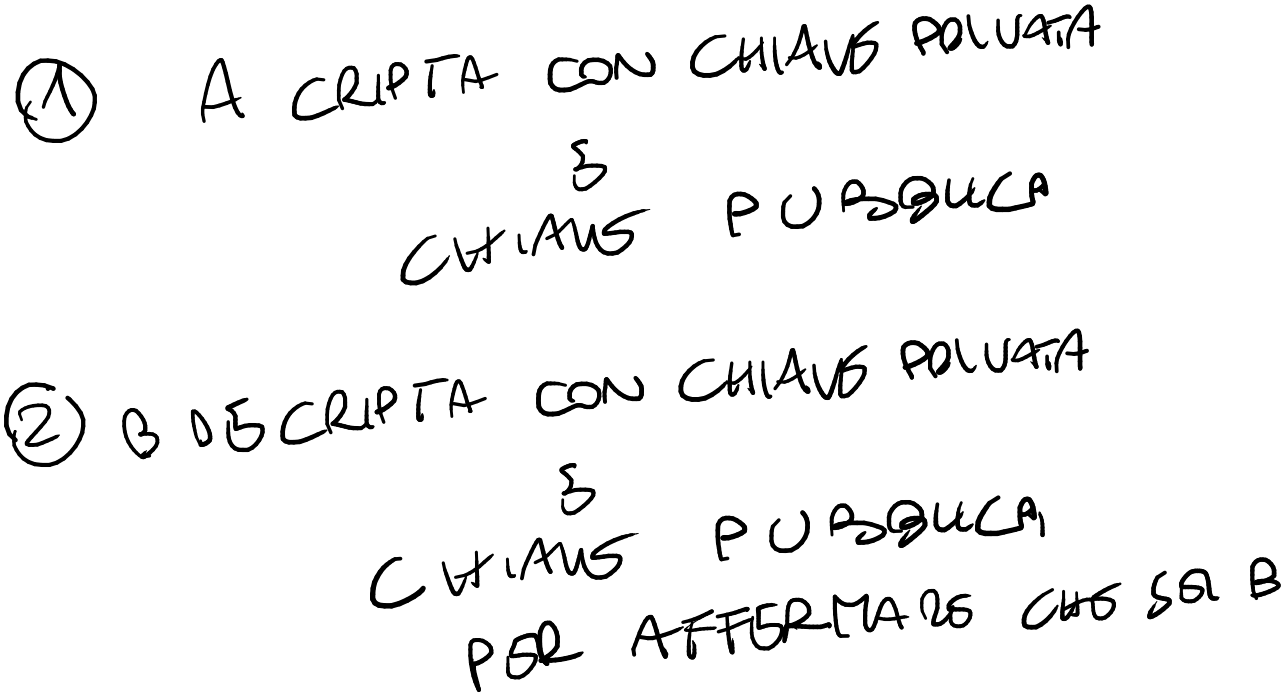
ANDARE "AVANTI" È FACILE
↓
MA, DIFFICILE TORNARE "INDIETRO"

(CONTRARIO = NON CI RIESCO!)

ASIMMETRICA







SIMMETRICA → 1
ASIMMETRICA → 3

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.

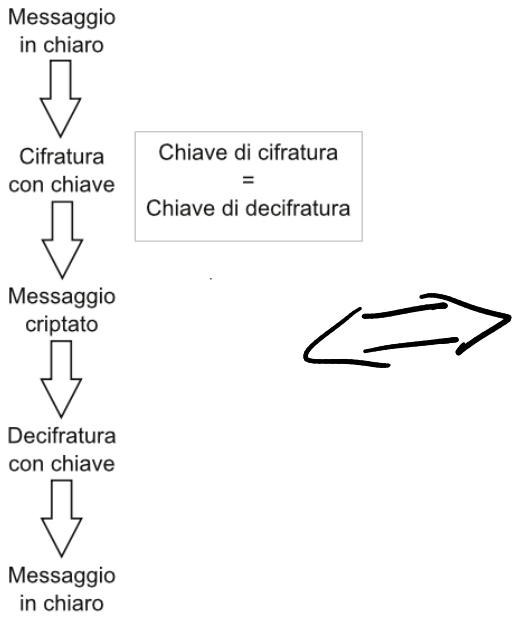
Il meccanismo della crittografia asimmetrica si basa invece sulle seguenti assunzioni:

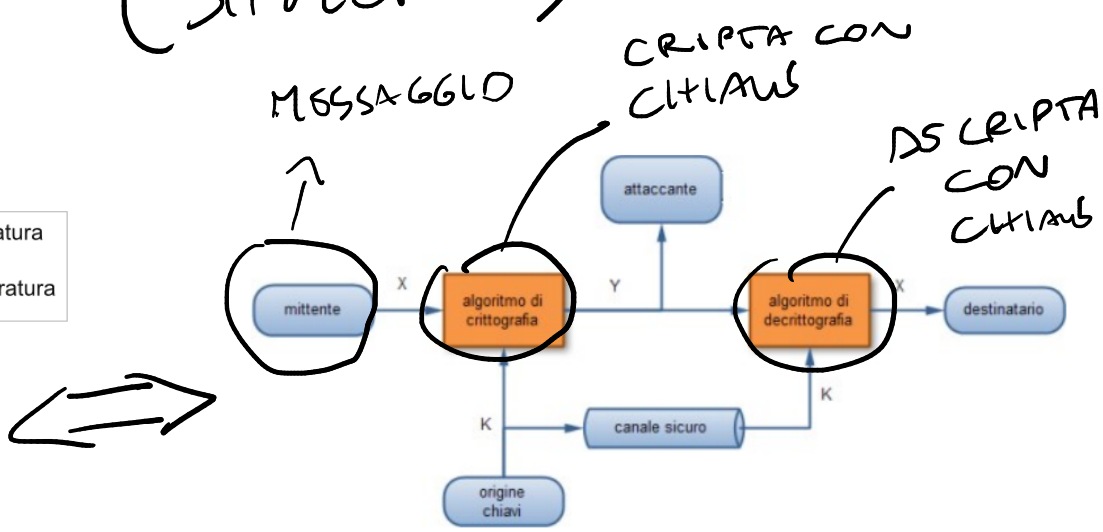
- la chiave privata non è ricavabile dalla chiave pubblica (o almeno non è facilmente ricavabile)
- se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.

] NO TORNARE INDIETRO

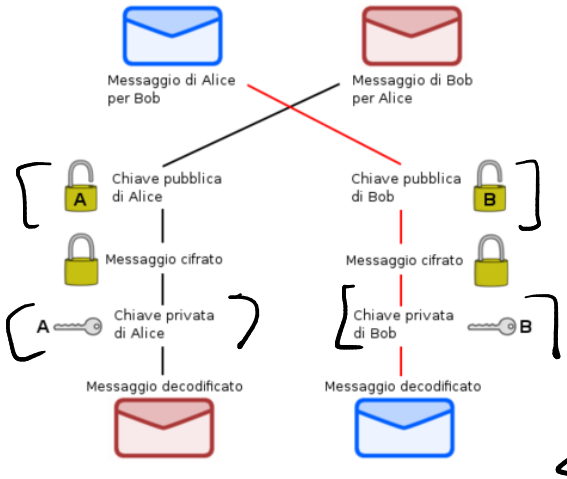
PUBBLICA → A e B DIPENDE DA ENTRAMBI !

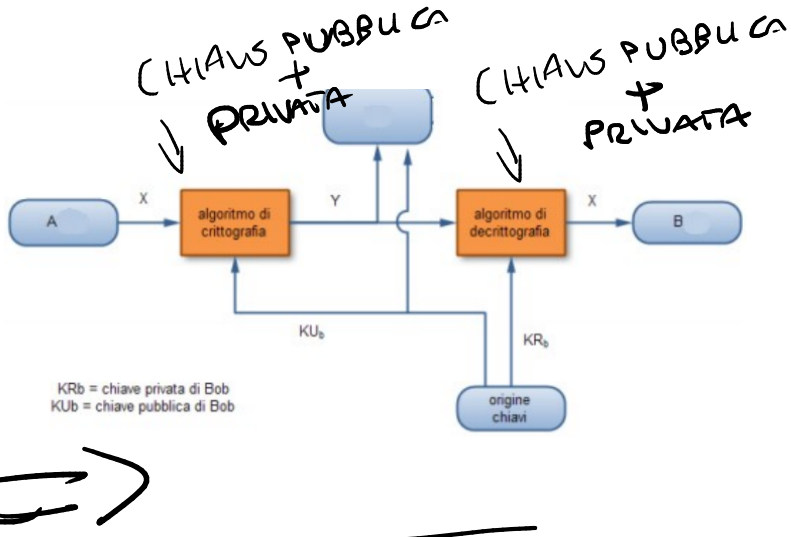
(SIMMETRICA)





(ASIMMETRICA).





[FORMAT]

→ P = NUMERO PRIMO

S = NUMERO DIVISIBILE SOLO PER SÈ STESSO O PER 1

5/5 → (1) ⟩ (5)

5/1 → (5) ⟩ (5)

↳ IL NUMERO STESSO

ARITMETICA MODULARE → MODULO

$5 \bmod 2 = 1$

$5/2 = 2$ (RIS.)

$(2 * [2]) + 1 = 5$ ([2] RIS.)

MODULO ⇓ I NUMERI SIANO UNICI → NUMERI PRIMI!

[TEOREMA DI FERMAT] ⇓

- p = NUMERO PRIMO
- e = NUMERO INTERO ESSERE ✓

[$[5] =$ INTERO $[5.4]$ → DECIMALE]

$a^p \equiv a \bmod p$

$e = 2, \quad p = 5$

$[2^5 \equiv 5 \bmod 2]$

Il piccolo teorema di Fermat dice che se p è un numero primo, allora per ogni intero a:

$$a^p \equiv a \pmod{p}$$

Questo significa che se si prende un qualunque numero a, lo si moltiplica per se stesso p volte e si sottrae a, il risultato è divisibile per p (aritmetica modulare).

$2^5 - 2 = 32 - 2 = 30$

$30 / 5 = 6$

ESEMPIO CON

$p = 5$, $a = 2$

$[p = 3 \quad , a = 4]$

1 PRENDIAMO "a" → 4

2 LO MOLTIPLICHIAMO PER SÉ STESSO "p" VOLTE → $4 \cdot 4 \cdot 4 = 4^3$

→ 3

3 SOTTRAI "a" (4) ⇒ $4^3 - 4$

$64 - 4 = 60$

4 RIS. DIVISIBILE PER "a" → $60 / 3 = 20$

$a^p \equiv a \bmod p$

DICE ESATTAMENTE QUESTO

NOTA: LA FORMA

$a^{p-1} \equiv 1 \pmod p$

È EQUIVALENTE A DIRE LA STESSA COSA DI

$a^p \equiv a \pmod p$

STESSO RISULTATO!

DIFFIE-HELLMAN

A → SEGRETO "a" → 2

B → SEGRETO "b" → 3

g E p → PUBBLICI

(4 E 5)

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	$K = A^b \bmod p$		

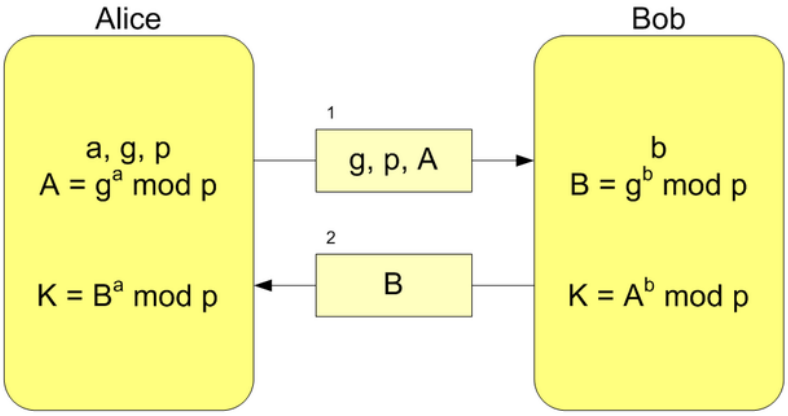
Ma:

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

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

PASSI FISSI → K (RISULTATO)

SEGRETO → CALCOLABILE SOLO CONOSCENDO A e B



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

Si tratta di un sistema di aritmetica degli interi, in cui i numeri "si avvolgono su loro stessi" ogni volta che raggiungono i multipli di un determinato numero n, detto **modulo**. Per capire, si pensi al funzionamento di un orologio in formato da 12 ore: trascorse quest'ultime "si ricomincia" dal numero 1 a contare le ore. Dire "sono le 3 del pomeriggio" (formato 12 ore) equivale a dire "sono le 15" (formato 24 ore). Tradotto in termini matematici, significa che $15 \equiv 3 \pmod{12}$. Si legge, 15 è congruente a 3, modulo 12.

- 12 H
3.00 PM
- 24 H.
15.00

$15 \equiv 3 \pmod{12}$

$(12 \cdot 1) + 3 = 15$

ARITM. MODULARE

a mod m = resto divisione
a ≡ b mod m significa a mod m = b mod m

Proprietà aritmetica modulare:

[(a mod m) + (b mod m)] mod m = (a+b) mod m
[(a mod m) - (b mod m)] mod m = (a-b) mod m
[(a mod m) · (b mod m)] mod m = (a·b) mod m
[(a mod m)^k] mod m = a^k mod m

PRATICO

$[a = 3 \quad b = 4 \quad m = 5]$

$$[(a \bmod m) \cdot (b \bmod m)] \bmod m = (a \cdot b) \bmod m$$

$a = 7 \quad b = 3 \quad m = 2$

$$[(7 \bmod 2) \cdot (3 \bmod 2)] \bmod 2 =$$

$$(7 \cdot 3) \bmod 2$$

$7 / 2 \rightarrow 3$

$(3 \cdot 2) + (1) = 7 \rightarrow 7 \bmod 2 = (1)$ ↓ resto

$3 / 2 \rightarrow 1$

$(1 \cdot 2) + (1) = 3 \rightarrow 3 \bmod 2 = (1)$ ↓ resto

$$[1 \cdot 1] \bmod 2 = 21 \bmod 2$$

$$1 \bmod 2 = 21 \bmod 2$$

$1 \bmod 2 \rightarrow 1 / 2 \rightarrow 0$ (intero)

$= 1 \qquad (0 \cdot 2) + 1 = 1$

$21 \bmod 2 \rightarrow 21 / 2 \rightarrow 10$ (intero)

$(10 \cdot 2) + 1 = 21$

$1 = 1$