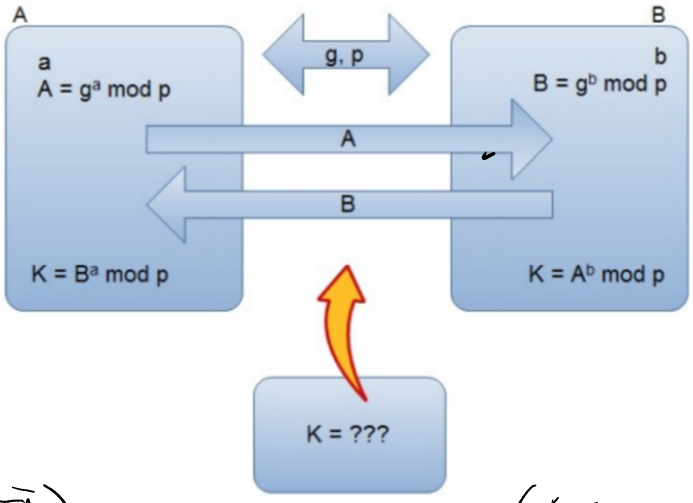
SISTEMI. Compito scritto in classe sui seguenti argomenti:

RSA
- Inverso di e (mod f)
- Algoritmo di Diffie-Hellman ← DA VEDERE (FATTO)
- Funzione di Eulero Φ(n)
- Calcolare la chiave pubblica
- Calcolare la chiave segreta d
- Codificare e decodificare un messaggio m

[DIFFIE - HELLMAN] → ALGORITMO (A)SIMMETRICO?



(+ VELOCITÀ)

SIMMETRICO

PUBBLICA

1 CHIAVE → PUBBLICA (COMUNE)

(+ SICUREZZA)

ASIMMETRICO

PUBBLICA

1 PRIVATA (A)

1 PRIVATA (B)

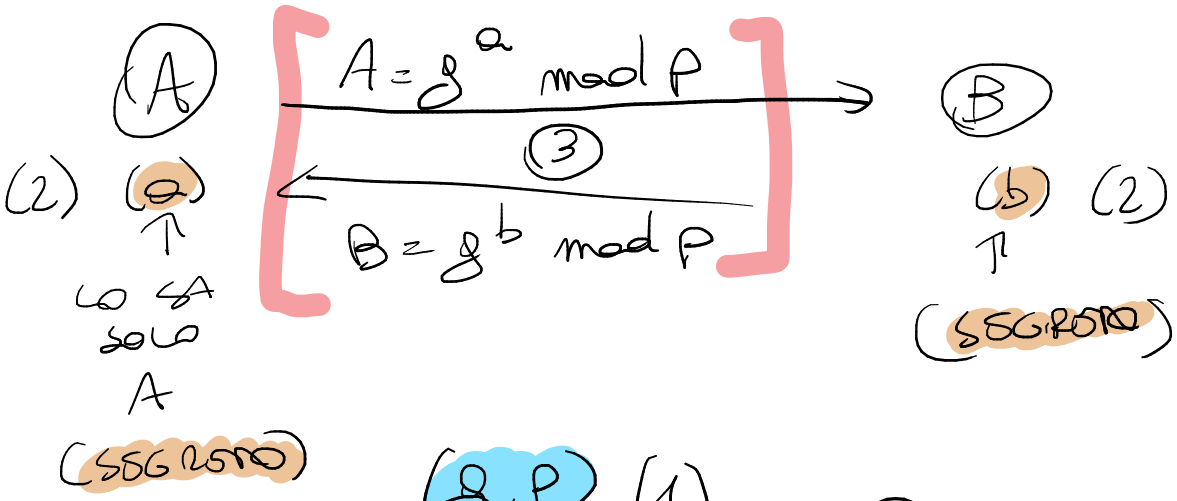
- A e B conoscono due numeri g e p pubblici (p **primo** *cioè un numero naturale maggiore di 1 che sia divisibile solamente per 1 e per sé stesso*) → ① SCEGLI NUMERI PRIMI
- A conosce un numero segreto a
- B conosce un numero segreto b → ② SCEGLI SEGRETI
- A calcola $A = g^a \bmod p$ e lo comunica a B
- B calcola $B = g^b \bmod p$ e lo comunica a A → ③ MANDA E RICEVI USANDO NUM. SEGRETI + NUM. PUBBLICI
- A calcola $K = B^a \bmod p$
- B calcola $K = A^b \bmod p$

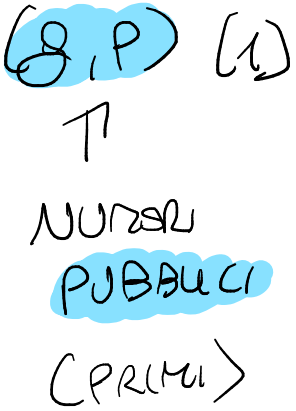
Ma:

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

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

A e B hanno condiviso un segreto (**il numero K**) senza comunicarlo esplicitamente!
Un eventuale attaccante può osservare A, B, g, p ma questa informazione non è sufficiente per ricavare K.
K è calcolabile solo conoscendo a o b, che tuttavia sono segreti e non vengono mai trasmessi.
Ricavare a da A (o analogamente b da B) significa risolvere un logaritmo discreto, difficile dal punto di vista computazionale.





(4)

TROVANO LA CHIAVE

$K = B^a \bmod p$ (A)

$K = A^b \bmod p$ (B)

SISTEMI. Compito scritto in classe sui seguenti argomenti:

1. Inverso di e (mod f)
2. Funzione di Eulero Φ(n)
3. Calcolare la chiave pubblica
4. Calcolare la chiave segreta d
5. Codificare e decodificare un messaggio m

RSA → NUMERI PRIMI !

↓

ASIMMETRICO

(p, q)

RSA → RIVEST / ADLEMAN / SHAMIR (CREATORI)

↓

USA MODULO = SICUREZZA SU UNICITÀ NUMERI

******** Passaggi algoritmo RSA ********

(1). Scegli due numeri "primi" (p, q) → Numeri segreti ⟷ p = 3, q = 7

(2). Calcolare il prodotto " n = p * q " = 3 * 7 = 21

(3). Calcolo funzione di Eulero (la lettera ϕ si legge "phi" (letto "fi"))

f = ϕ(n) = (p − 1)(q − 1) = (3 − 1)(7 − 1) = 2 * 6 = 12

(4). Trovare un numero compreso tra 1 ed f (12) coprimo con f (12) → 5

Coprimo → Numero che non ha divisori in comune con il tuo numero

(5). Trovare "d * e ≡ 1 mod f" → "d * 5 ≡ 1 mod 12" = Troviamo "d"

Congruenza (≡) → Assicura che i numeri "tornino indietro" (Euclide esteso)

Inverso mod f → Un modo per vedere se l'algoritmo è corretto → Ti dà resto 1

(d * 5) / 12 = 1? ⟷ C'è un numero "d" tale che il resto della divisione (d * e) / f è 1?

Inverso (mod 12) di 5 → (5 * 3) = 15 MA 15 (mod 12) ≠ 1 (NON SI USA - CAMBIA NUMERI PRIMI..

ALLORA scegliamo altri numeri! Numeri segreti ⟷ p = 3, q = 5

(2). Prodotto → n = p * q = 3 * 5 = 15

(3). Funzione di Eulero → f = ϕ(n) = (p − 1)(q − 1) = 2 * 4 = 8

(4). e = Numero coprimo con 8 compreso tra 1 e 8 → 3

(5). Trovare "inverso mod f" = "d * e ≡ 1 mod f" → "d * 3 ≡ 1 mod 8" = Troviamo "d"

(d * e) / f è 1? (d * 3) / 8 = 1? Inverso (d) = 3 (d)
Inverso (mod 8) di 3 → (3 * 3) = 9 e 9 (mod 8) = 1 (GIUSTO → Dà resto 1)

(6).

**** CHIAVI **** → Comunicazione asimmetrica

- Codifica e decodifica del messaggio -

(n, e) = Chiave pubblica = (8, 3)
(n, d) = Chiave privata = (8, 3)

Dato un messaggio m → (0 < m < n) → (0 < m < 15) - Scelgo 2
- PRIMA Cifratura: Calcolare → c = m^e mod n = 2^3 mod 15 = 8 mod 15 = 8
- DOPO Decifratura: Calcolare → m = c^d mod n = 8^3 mod 15 = 2

Output → c = 8, m = 2