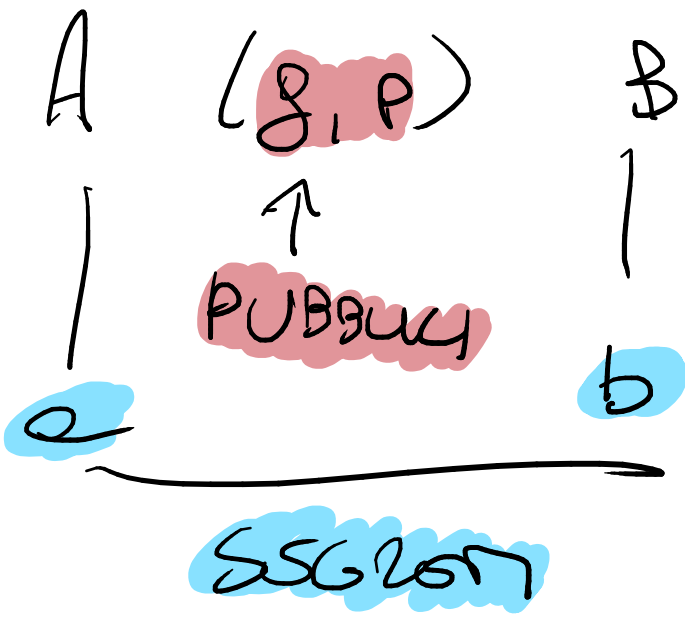
DIFFIE-HELLMAN (DH)



1°

[A manda a B

$A = g^a \bmod p$]

2°

[B manda ad A

$B = g^b \bmod p$]

3°

[$A \rightarrow K = B^a \bmod p$

$B \rightarrow K = A^b \bmod p$]

RSA

CHECK PER LA CORRETTEZZA DI (P, Q)

→ INVERSO DI E (MOD F)

E/F NUMERI COPRIMI

↓

NON HANNO DIVISORI IN COMUNE

↓

RISULTATO!

RSA → ASIMMETRICO

P, Q (NUMERI PUBBLICI)

↓

$n = p \cdot q$

BUONO → $\varphi(n)$

↑

(FI / PHI)

$= (p-1)(q-1)$

CHIAVE PUBBLICA → (e)

✓

$1 < e < \varphi(n)$ INTERO non $\neq$

RESTO → 1

CHIAVE PRIVATA → (d)

SISTEMI. Compito scritto in classe sui seguenti argomenti:

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

resto 1 → ? (RSA è giusto?)

resto ! = 1

numeri p, q sono sbagliati

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

$n = p \cdot q$

$e \rightarrow 0 < e < \varphi(n)$

coprimo $0 < \dots < 10$

7

$[d e \equiv 1 \bmod \varphi] \Rightarrow$ inverso

[congruenza!]

chiave pubblica → (n, e)

chiave privata → (n, d)

CIFRATURA $\rightarrow$ $C = m^e \bmod n$

DECIFRATURA $\rightarrow$ $m = C^d \bmod n$

?

PLAINTEXT = TESTO IN CHIARO