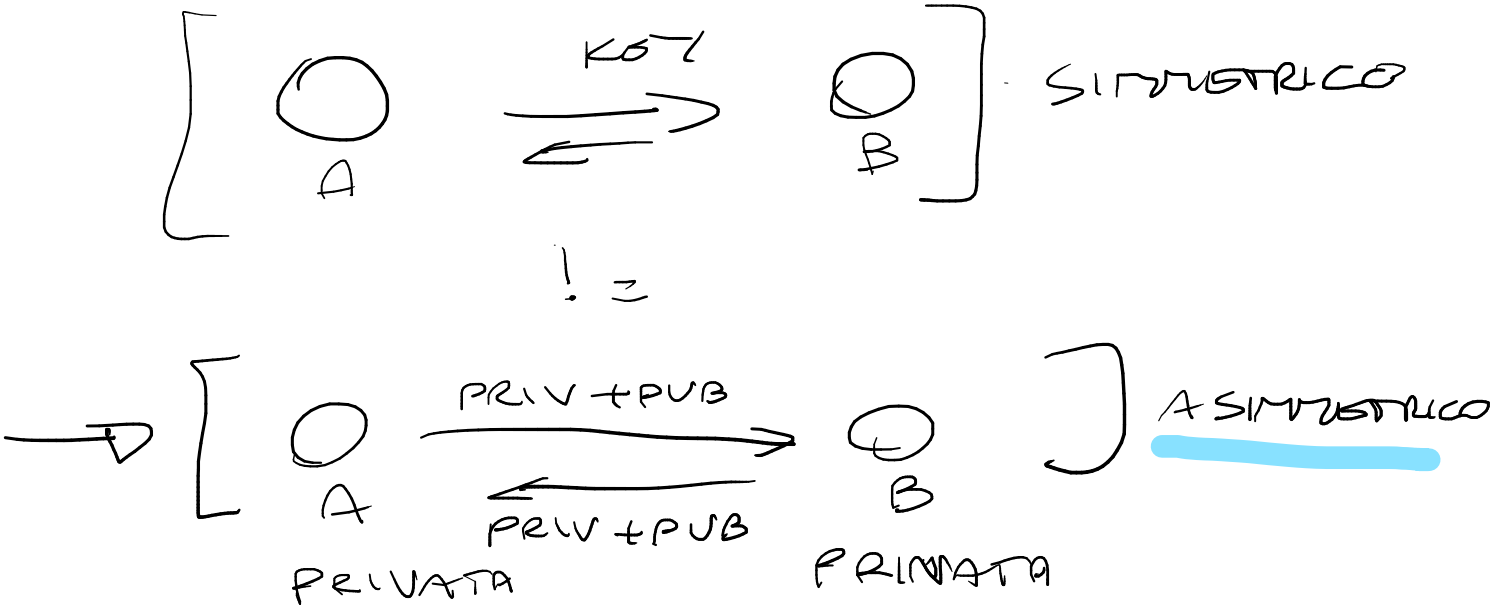
RSA → Algoritmo di crittografia asimmetrico



(1). Scegliere due numeri primi → p = 3, q = 5

Numero primo = Numero che si divide solamente per sé stesso e per 1

(2). Calcoli il prodotto "n = p * q" → 3 * 5 = 15

(3). Calcolare Eulero "f = ϕ(n)" = (p − 1)(q − 1) = (3 − 1)(5 − 1) = 8

Trovare "e" → Inverso di e (mod f) → Questo garantisce sicurezza

(4). Scegliere "e" compreso tra 1 e "f" (8) coprimo con "f" (8)

Numero "e" coprimo con 8 → e = 3 (Non ha divisori comuni con f = 8)

Coprimi → Non hanno divisori comuni

Esempio: 8, 9 (non hanno divisori comuni)
9 → Divisori: 3, 9
8 → Divisori: 2, 4, 8

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

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

(d * 3) / 8 = 1? Inverso (d) = 1
Inverso (mod 8) di 3 → (1 * 8) = 8 e 9 (mod 8) = 1

INVERSO = RESTO 1

Di seguito alcuni esempi:

- l'inverso (mod 7) di 5 è 3 perché 3 x 5 = 15 e 15(mod 7) = 1
- l'inverso (mod 7) di 3 è 5 perché 3 x 5 = 15 e 15(mod 7) = 1
- l'inverso (mod 7) di 6 è 6 perché 6 x 6 = 36 e 36(mod 7) = 1
- l'inverso (mod 43) di 11 è 4 perché 11 x 4 = 44 e 44(mod 43) = 1

MODULO → DIVISIONE INTERA

8 mod 2 = 0

8 mod 3 = 2 ↔ (3 · 2) + 2
(7.)

3 mod 2 = 1 ↔ (1 · 2) + 1

INVERSO → DÀ RESTO 1.

(n, e) = Chiave pubblica = (8, 3)
(n, d) = Chiave privata = (8, 1)

→

Dato un messaggio m (0 < m < n)
1. Cifratura: calcolare $c = m^e \bmod n$
2. Decifratura: calcolare $m = c^d \bmod n$

(6) Tra 0 < m < 8 → c = (m)^3 mod 8 → 8 mod 8 = 0
→ m = (c)^1 mod 8 → 2 mod 8 = 2

ESEMPI COMPLETI MODULO

→ (4 mod 8) = 4

4 % 8 (0 · 8) + 4
DIVISIONE RESTO

→ (10 mod 8) = 2 → MODULO

10 % 8 (1 · 8) + 2
QUOZIENTE RESTO

→ (8 mod 8) → 1

8 % 8 (1 · 8) + 1
QUOZIENTE RESTO

→ (18 mod 8) → (8 · 2) + 2
1
RESTO

********** ESEMPIO COMPLETO RSA **********

(1). Scegliere due numeri primi → p = 3, q = 11

Numero primo = Numero che si divide solamente per sé stesso e per 1

(2). Calcoli il prodotto "n = p * q" → 3 * 11 = 33

(3). Calcolare Eulero "f = ϕ(n)" = (p − 1)(q − 1) = (3 − 1)(11 − 1) = 20

Trovare "e" → Inverso di e (mod 20)

(4). Scegliere "e" compreso tra 1 e "f" (20) coprimo con "f" (20) → 7

(5). Trovare "d * e ≡ 1 mod f" → "d * 7 ≡ 1 mod 20" = Troviamo "d"

(d * 7) / 20 = 1? Inverso (d) = 3
Inverso (mod 20) di 7 → (3 * 7) = 21 e 21 (mod 20) = 1 (Resto fa "1" → d=3)

(n, e) = Chiave pubblica = (8, 7)
(n, d) = Chiave privata = (8, 3)

(6).
Dato un messaggio m → (0 < m < 20) → 12

- Cifratura: Calcolare → c = 12^7 mod 20 = 8
- Decifratura: Calcolare → m = c^d mod n = (8^3) mod 20 = 12

Termini:

- n → Modulo dell'RSA
- e → Esponente pubblico
- d → Esponente privato

Sostituisci numeri e poi applica questo algoritmo così....