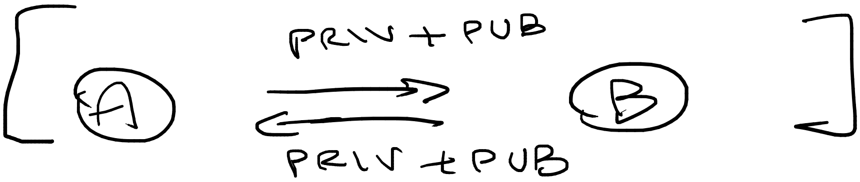
RSA → Algoritmo di crittografia asimmetrico

"Asimmetrico"
1) A e B condividono una stessa chiave (pubblica)
2) Ma ognuno ha anche la propria chiave private (sia A che B)



ASIMMETRICO

(1). Scegli due numeri "primi" (p, q) → p = 3, q = 11 ESEMPIO 1

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

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

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

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

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

Numero coprimo = Non ha divisori comuni con te

Esempio: 8, 9 → 8 ha (2, 4, 8), mentre 9 ha (3, 9)

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

C'è un numero "d" tale che la divisione sia (d * e) / f = 1? → d = 3

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

La regola dell'inverso è che devi trovare un numero che mod f ti dà resto 1.

a

- 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

← INVERSI

(6). Coppia di chiavi

(n, e) = Chiave pubblica = (33, 7)
(n, d) = Chiave privata = (33, 3)

(7). Formule di:
- Cifratura (Lo rende sicuro con algoritmo RSA)
- Decifratura (Decodifica il pacchetto per leggerlo)

Dato un messaggio "m" → (0 < m < n) → (0 < m < 33)
- PRIMA Cifratura → c = m^e mod n = (2^7) mod 33 = 128 mod 33 = 29
128 mod 33 = 29 perché (3 * 33) + 29 = 99 + 29 = 128
- POI Decifratura → m = c^d mod n = (29)^3 mod 33 = 2

(1). Scegli due numeri "primi" (p, q) → p = 5, q = 7 → ESEMPIO 2

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

(2). Trova il prodotto "n = p * q" → n = 5 * 7 = 35

(3). Calcolare Eulero "f = ϕ(n)" = (p − 1)(q − 1) = (5 − 1)(7 − 1) = 24

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

(4). Scegliere "e" compreso tra 1 ed "f" (24) coprimo con 24 → 5

Numero coprimo = Non ha divisori comuni con te

(5). Trovare "d * e ≡ 1 mod f" → "d * 5 ≡ 1 mod 24" = Trovare "d" (inverso)

C'è un numero "d" tale che la divisione sia (d * e) / f = 1? → d = 5

(d * 5) / 24 = 1?
Inverso (mod 24) di 5 = 5 → 5 * 5 = 25 e 25 (mod 24) = 1

La regola dell'inverso è che devi trovare un numero che mod f ti dà resto 1.
Se il numero "e" non va bene, si cambia! (come abbiamo fatto tra 9 e 5).

• 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

← INVERSI

(6). Coppia di chiavi

(n, e) = Chiave pubblica = (35, 5)
(n, d) = Chiave privata = (35, 5)

(7). Formule di:
- Cifratura (Lo rende sicuro con algoritmo RSA)
- Decifratura (Decodifica il pacchetto per leggerlo)

Dato un messaggio "m" → (0 < m < n) → (0 < m < 35) → (0 < 2 < 35
- PRIMA Cifratura → c = m^e mod n = (2^5) mod 35 = 32 mod 35 = 32

Esempi di ragionamento modulo ⟷ 38 mod 35 = 3, 42 mod 35 = 7

- POI Decifratura → m = c^d mod n = (32)^5 mod 35 = 2

Termini:

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

[(1). Scegli due numeri "primi" (p, q) → p = 3, q = 5] → ESEMPIO 3

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

(2). Trova il prodotto "n = p * q" → n = 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 ed "f" (8) coprimo con 8 → 3

Numero coprimo = Non ha divisori comuni con te

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

C'è un numero "d" tale che la divisione sia (d * e) / f = 1? → d = 3

(d * 3) / 8 = 1?
Inverso (mod 8) di 3 = 5 → 3 * 3 = 9 e 9 (mod 8) = 1

La regola dell'inverso è che devi trovare un numero che mod f ti dà resto 1.
Se il numero "e" non va bene, si cambia! (come abbiamo fatto tra 9 e 5).

(6). Coppia di chiavi

(n, e) = Chiave pubblica = (15, 3)
(n, d) = Chiave privata = (15, 3)

(7). Formule di:
- Cifratura (Lo rende sicuro con algoritmo RSA)
- Decifratura (Decodifica il pacchetto per leggerlo)

Dato un messaggio "m" → (0 < m < n) → (0 < m < 15) → (0 < 2 < 15)
- PRIMA Cifratura → c = m^e mod n = (2^3) mod 15 = 8 mod 15 = 8

- POI Decifratura → m = c^d mod n = (8)^5 mod 15 = 8