RSA

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

(2) Calcolare prodotto → n = p * q → 3 * 5 = 15

(3) Calcolare Eulero → f=ϕ(n) → ϕ(15) = (p-1)(q-1) = (3-1)(5-1) = 2 * 4 = 8

(4) Scegliamo un numero "e" compreso tra 1 e 8 coprimo con 8 → 7
Coprimo = Non hanno divisori in comune

(5) Calcolare "d*e" congruente a 1 mod f

(d * 7) mod 15 = 1 mod 15

de mod f = 1 mod f
de mod f = 1

Conosco il numero **e**, conosco il numero **f** e so che sono coprimi.

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

(d * 7) / 15 è 1?

inverso (mod 15 di 7) è 2 → 2 * 7 = 14 e 15(mod 14) = 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

RSA → CHIAVI

- La coppia **(n, e)** (15, 7) *è la **chiave pubblica** di Bob*
- La coppia **(n, d)** (15, 2) *è la **chiave privata** di Bob*