1. Inverso di e (mod f)

- Definizione: Dato e ed f coprimi, l'inverso d è tale che: `de ≡ 1 mod f`
  - Coprimi = NON hanno divisori in comune!
  - ≡ -> Congruenza (vale la divisione modulo f dello stesso numero)
- Proprietà chiave: d esiste se e solo se e ed f sono coprimi (GCD(e,f) = 1)
- Calcolo: Si utilizza l'algoritmo di Euclide esteso
  - Ti permette di usarlo in algoritmi di crittografia
- Esempio pratico:
  - Per e=5, f=7: l'inverso è d=3 perché 3×5 mod 7 = 1
  - Non esiste inverso se i numeri non sono coprimi

2. Algoritmo di Diffie-Hellman

- Scopo: Condivisione sicura di una chiave segreta su canale insicuro
- Passi:
  1. A e B conoscono g, p pubblici (p primo)
  2. A genera segreto a, calcola A = g^a mod p
  3. B genera segreto b, calcola B = g^b mod p
  4. A calcola K = B^a mod p
  5. B calcola K = A^b mod p
- Risultato: K = g^(ab) mod p è la chiave condivisa
- Sicurezza: Basata sulla difficoltà del logaritmo discreto

3. Funzione di Eulero Φ(n)

- Definizione: Conta i numeri coprimi con n minori di n
- Per n = p×q (p,q primi):
  - Φ(n) = (p-1)(q-1)
- Utilizzo principale: Generazione chiavi RSA
- Formula: f = Φ(n) = (p-1)(q-1) = n-p-q+1

4. Calcolare la chiave pubblica

- Componenti: (n,e)
- Passi:
  1. Scegliere p,q primi
  2. Calcolare n = p×q
  3. Calcolare Φ(n)
  4. Scegliere e coprimo con Φ(n), 1 < e < Φ(n)

5. Calcolare la chiave segreta d

- d è l'inverso moltiplicativo di e modulo Φ(n)
- Calcolo mediante algoritmo di Euclide esteso
- Proprietà: d×e ≡ 1 mod Φ(n)
- Componenti chiave privata: (n,d)

6. Codificare e decodificare un messaggio m

- Cifratura: c = m^e mod n
- Decifratura: m = c^d mod n
- Vincoli: 0 < m < n
- Esempio:
  - Con chiave pubblica (33,7)
  - Con chiave privata (33,3)
  - Messaggio m=2: c = 2^7 mod 33 = 29
  - Decifratura: m = 29^3 mod 33 = 2