

# La scelta dell'esponente pubblico e

La scelta dell'esponente pubblico e in RSA è un passaggio fondamentale per la sicurezza e l'efficienza del sistema. Normalmente, si scelgono valori di e che sono coprimi rispetto a  $\phi(n)$  e che rendano i calcoli di cifratura efficienti.  **$\phi(n)$ ,  $\phi(n)$ ,  $\phi(n)$  indicano la stessa cosa**

In tutti i casi di implementazione del sistema RSA, le condizioni da rispettare per il valore di e sono:

## 1. Minore di $\phi(n)$ :

- e deve essere un numero minore di  $\phi(n)$ . Questa condizione è necessaria per garantire che ci siano sufficienti possibilità per la generazione della chiave privata e che il sistema funzioni correttamente.

## 2. Coprimo con $\phi(n)$ :

- e deve essere coprimo con  $\phi(n)$ . Ciò significa che il massimo comune divisore (MCD) tra e e  $\phi(n)$  deve essere 1. Questa condizione garantisce che l'inverso moltiplicativo di e modulo  $\phi(n)$  esista, il che è essenziale per calcolare la chiave privata.

**Valori comuni per e:** Il valore più comunemente utilizzato è **65537** (ovvero  $2^{16}+1$ ), rispettando le regole sopra indicate e per diverse ragioni:

1. **Efficienza:** 65537 è un numero relativamente piccolo, che rende più rapidi i calcoli durante la cifratura e la decifratura.
2. **Sicurezza:** Questo valore è abbastanza grande da prevenire attacchi noti, ma sufficientemente semplice per calcoli efficienti.
3. **Coprimalità:** 65537 è primo, quindi è quasi sempre coprimo con  $\phi(n)$  per qualsiasi p e q scelti, purché p e q non siano scelti in modo da renderlo divisore di  $\phi(n)$ .

**Procedura completa per scegliere e:**

1. **Calcola**  $\phi(n)=(p-1)(q-1)$ .
2. **Verifica che** 65537 **sia coprimo con**  $\phi(n)$  . Questo è vero nella stragrande maggioranza dei casi con valori di p e q adeguati.
3. **Se** 65537 **non fosse coprimo con**  $\phi(n)$  (caso comune con valori di p e q piccoli), scegli il primo valore dispari più piccolo (come 3, 5, 17...) che sia coprimo con  $\phi(n)$  .

In pratica, 65537 è il valore più usato per e nei sistemi RSA moderni, perché offre un buon bilancio tra sicurezza ed efficienza senza richiedere ulteriori controlli complessi.

In RSA, l'esponente è scelto come un numero intero, generalmente piccolo, per una delle due chiavi (tipicamente la **chiave pubblica**). Vediamo come funziona questo esponente e dove entra in gioco nella formula di cifratura e decifratura:

### 1. Chiave pubblica e privata:

- **Chiave pubblica:**  $(n,e)$
- **Chiave privata:**  $(n,d)$

Dove:

- $N = p \times q$  è il prodotto di due numeri primi.
- $e$  è l'esponente pubblico.
- $d$  è l'esponente privato, calcolato per garantire che  $d \times e \equiv 1 \pmod{\varphi(n)}$ , dove  $\varphi(n)$  è la funzione di Eulero di  $n$ .

### 2. Formula di cifratura (dove $e$ è l'esponente):

- Quando **cifri** un messaggio  $m$  con la chiave pubblica  $(n,e)$ , elevi il messaggio all'esponente  $e$ :

$$c \equiv m^e \pmod{n}$$

- $e$  agisce come un esponente in questa formula.  **$^e$  significa elevato ad  $e$ .**

### 3. Formula di decifratura (dove $d$ è l'esponente):

- Quando **decifri** il messaggio cifrato  $c$  con la chiave privata  $(n,d)$ , elevi il messaggio cifrato all'esponente  $d$ :

$$M \equiv c^d \pmod{n}$$

Qui  $d$  è l'esponente che, insieme a  $e$ , permette di ripristinare il messaggio originale  $m$  grazie alle proprietà dei moduli e alla relazione tra  $e$  e  $d$ .

### Perché si usa l'esponente

L'esponenziazione modulare è fondamentale per la sicurezza dell'RSA perché:

- È un'operazione che richiede molto tempo per essere invertita (decifrata) senza la conoscenza di  $d$ .
- Utilizzare l'esponenziazione con numeri molto grandi rende il processo sicuro contro tentativi di decifrazione brute-force.

**Il valore  $e$ , quindi, è scelto come esponente per permettere l'uso di questa proprietà.**