

LA FUNZIONE MODINVERSE

La funzione ModInverse calcola l'inverso moltiplicativo modulo, cioè trova un numero x che, moltiplicato per a , dia come risultato 1 quando diviso per m (modulo m). Questo numero è importante nell'RSA per calcolare la chiave privata.

Concetto dell'Inverso Moltiplicativo Modulare

Se abbiamo due numeri, a e m , il "modulo inverso" di a rispetto a m è un numero x tale che:

$$(a \times x) \bmod m = 1$$

Ad esempio, per $a = 3$ e $m = 11$, il numero x che soddisfa questa condizione è 4, perché:

$$(3 \times 4) \bmod 11 = 12 \bmod 11 = 1$$

Come Funziona la Funzione ModInverse

Questa funzione usa l'algoritmo di Euclide esteso, che è come una versione avanzata della divisione, per trovare l'inverso.

1. Inizializzazione:

- $m0$ memorizza il valore originale di m , perché alla fine servirà.
- $x0$ e $x1$ sono variabili usate per calcolare il risultato finale.

2. Ciclo Principale:

- Finché a è maggiore di 1, la funzione continua a calcolare:
 - q , cioè quante volte m entra in a ($q := a \div m$).
 - t memorizza temporaneamente il valore di m .
- Scambia i valori tra a e m , aggiornando il resto ($a \bmod m$) per proseguire il calcolo.
- Aggiorna anche $x0$ e $x1$ seguendo una formula specifica.

3. Aggiustamento Finale:

- Alla fine del ciclo, se $x1$ è negativo, viene aggiunto a $m0$ per ottenere un valore positivo.
- $x1$ viene restituito come risultato, ovvero l'inverso moltiplicativo modulo di a rispetto a m .

In pratica, questo algoritmo permette di calcolare un numero che "annulla" l'effetto di a in modulo m , e questo numero è proprio quello necessario per la chiave privata nell'RSA.