

E' MATEMATICAMENTE NORMALE CHE IL MESSAGGIO ORIGINALE SIA TALVOLTA UGUALE AL MESSAGGIO CIFRATO ?

Sì, è possibile che, in alcuni casi, il messaggio cifrato sia uguale al messaggio originale, anche con l'algoritmo RSA. Questo succede per alcuni valori specifici, ed è una particolarità matematica di RSA dovuta alla struttura modulare.

Motivo Matematico (^ segno di elevazione a potenza)

Con RSA, il messaggio m viene cifrato tramite la formula:

$$c = m^e \bmod n$$

Dove:

- c è il messaggio cifrato,
- m è il messaggio originale,
- e è l'esponente pubblico,
- $n = p \cdot q$ è il prodotto di due numeri primi.

In alcuni casi, quando il messaggio originale m e n non sono **coprimi** tra loro, ovvero quando il massimo comune divisore tra m e n è diverso da 1 (ad esempio, se dividono uno o entrambi i fattori di n), il calcolo di $m^e \bmod n$ può restituire m stesso.

Esempio

Nel tuo caso:

$$c = 285^5 \bmod 323$$

Se 285 e 323 non sono coprimi, può succedere che il messaggio cifrato risulti uguale al messaggio originale, come accade qui.

Soluzioni per Evitare questa Situazione

1. **Scelta del messaggio m :** Bisogna fare attenzione a scegliere m che sia coprimo con n (ad esempio, escludendo numeri multipli di p o q).
2. **Blocco di padding:** In scenari reali, l'uso di "padding" (aggiunta di bit o simboli) al messaggio originale è comune e riduce la probabilità di questo tipo di coincidenza.

In pratica, però, questo problema non si presenta spesso perché, con chiavi grandi, la probabilità di incontrare numeri non coprimi a n è molto bassa.