

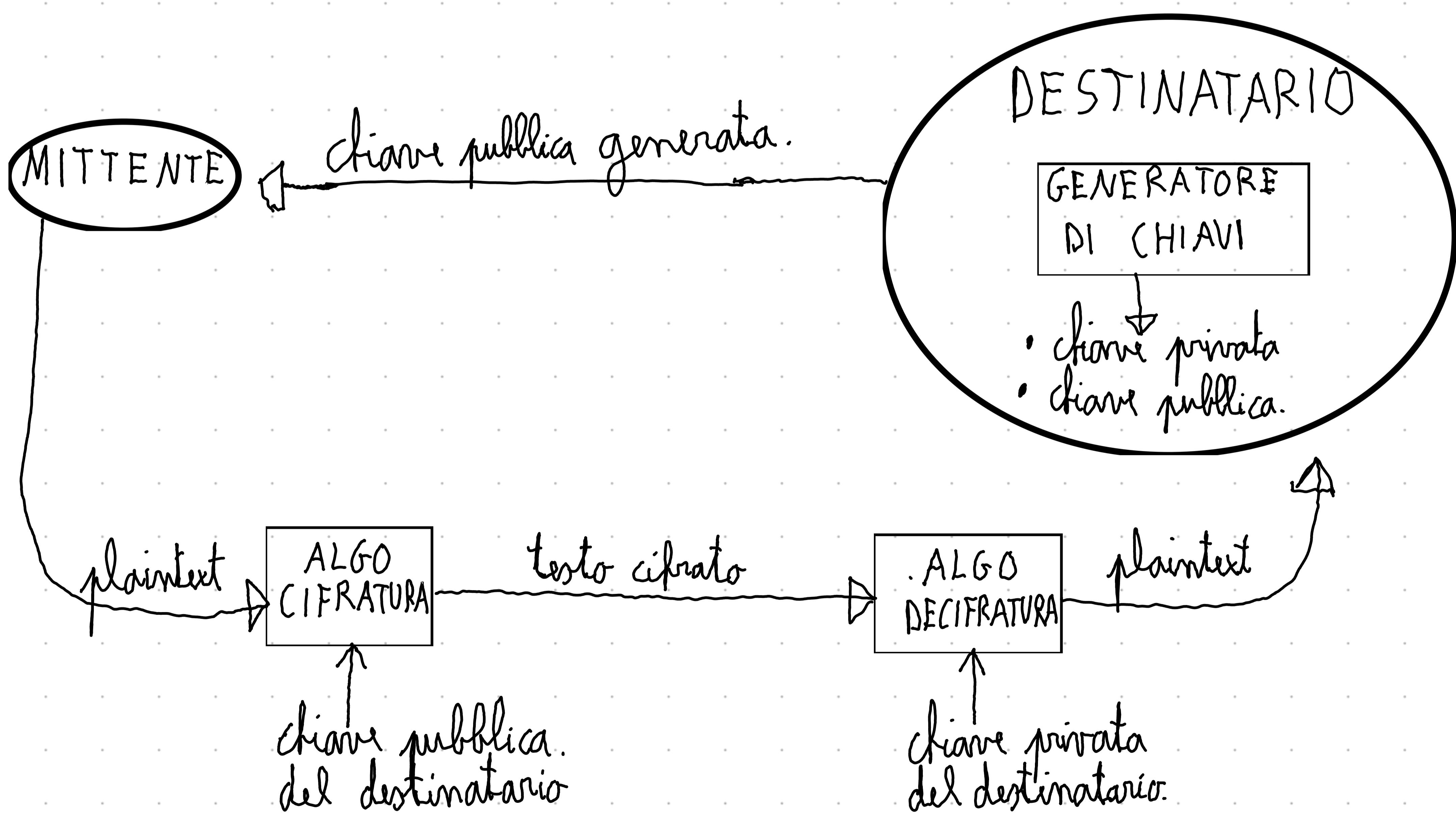
CRITTOGRAFIA a CHIAVE PUBBLICA

Nasce figlia di due problemi: la distribuzione delle chiavi e il problema delle firme, i quali sembravano insolubili per definizione.

Ma utilizzando una chiave pubblica che viene distribuita a tutti i destinatari e una chiave privata per ogni attore è possibile arginare questi due problemi.

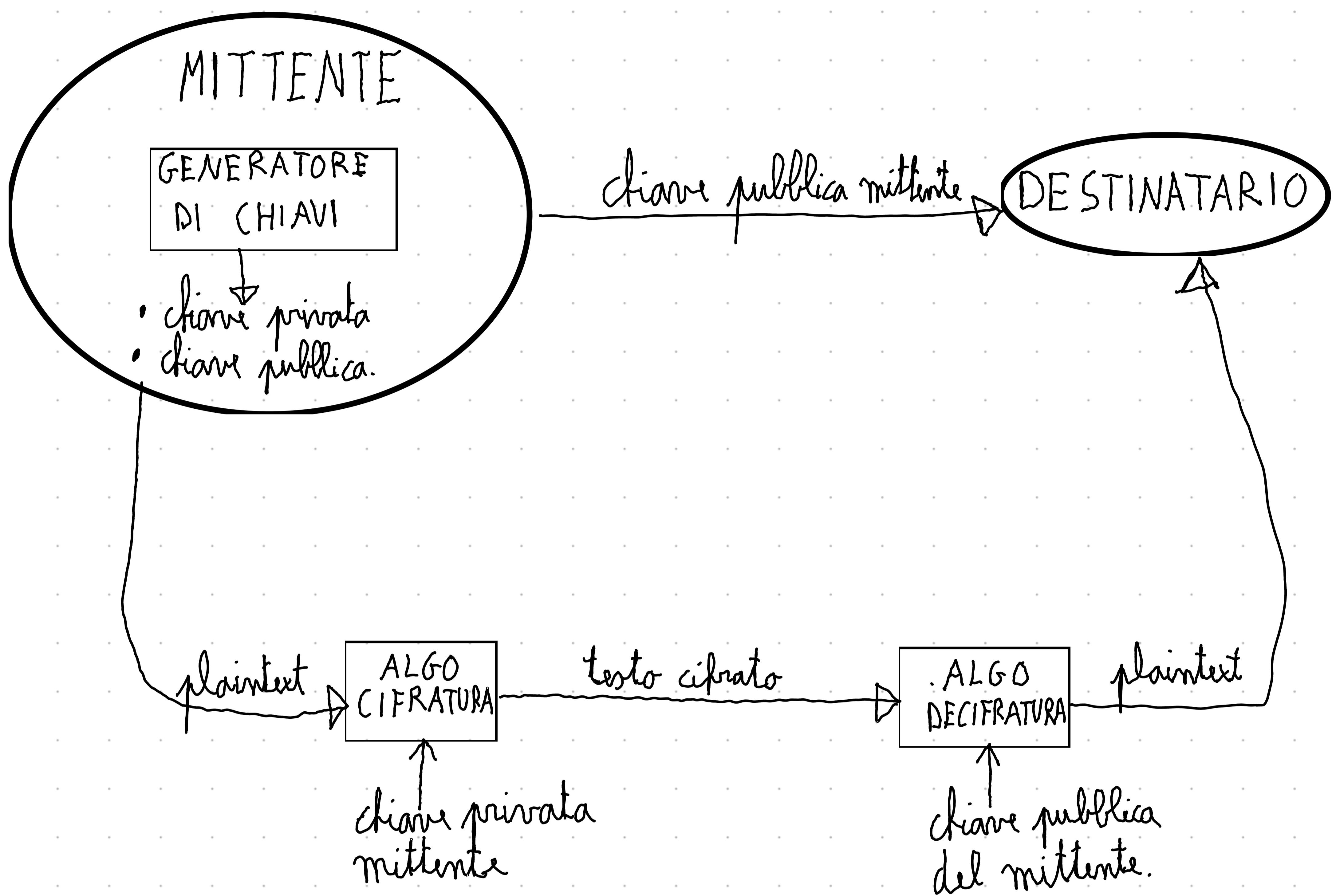
Sono quindi necessarie un numero totale di chiavi pari a $2 \cdot \# \text{ATTORI}$

• SEGRETEZZA: assicurare la riservatezza.

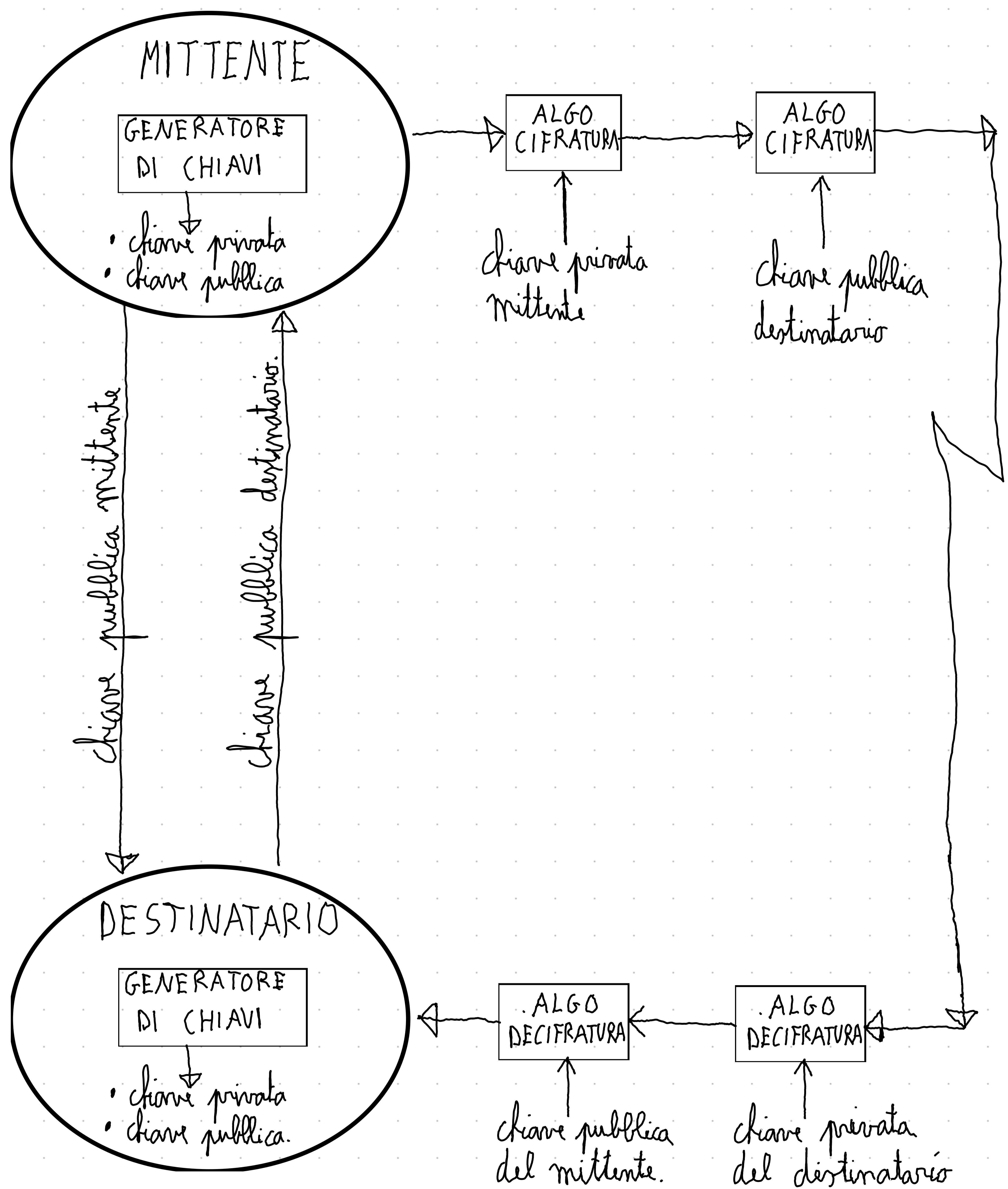


Non viene garantita l'autenticità del mittente...

• AUTENTICITÀ: assicurare l'autenticità del mittente



• SEGRETEZZA e AUTENTICITÀ:



• RSA:

Una delle caratteristiche principali di un algoritmo a chiavi pubblica è quello di avere una scarsa correlazione tra chiave pubblica e chiave privata, questo viene sfruttato molto bene dal algoritmo RSA sfruttando la difficoltà da parte dei calcolatori nella fattorizzazione numeri a molte cifre.

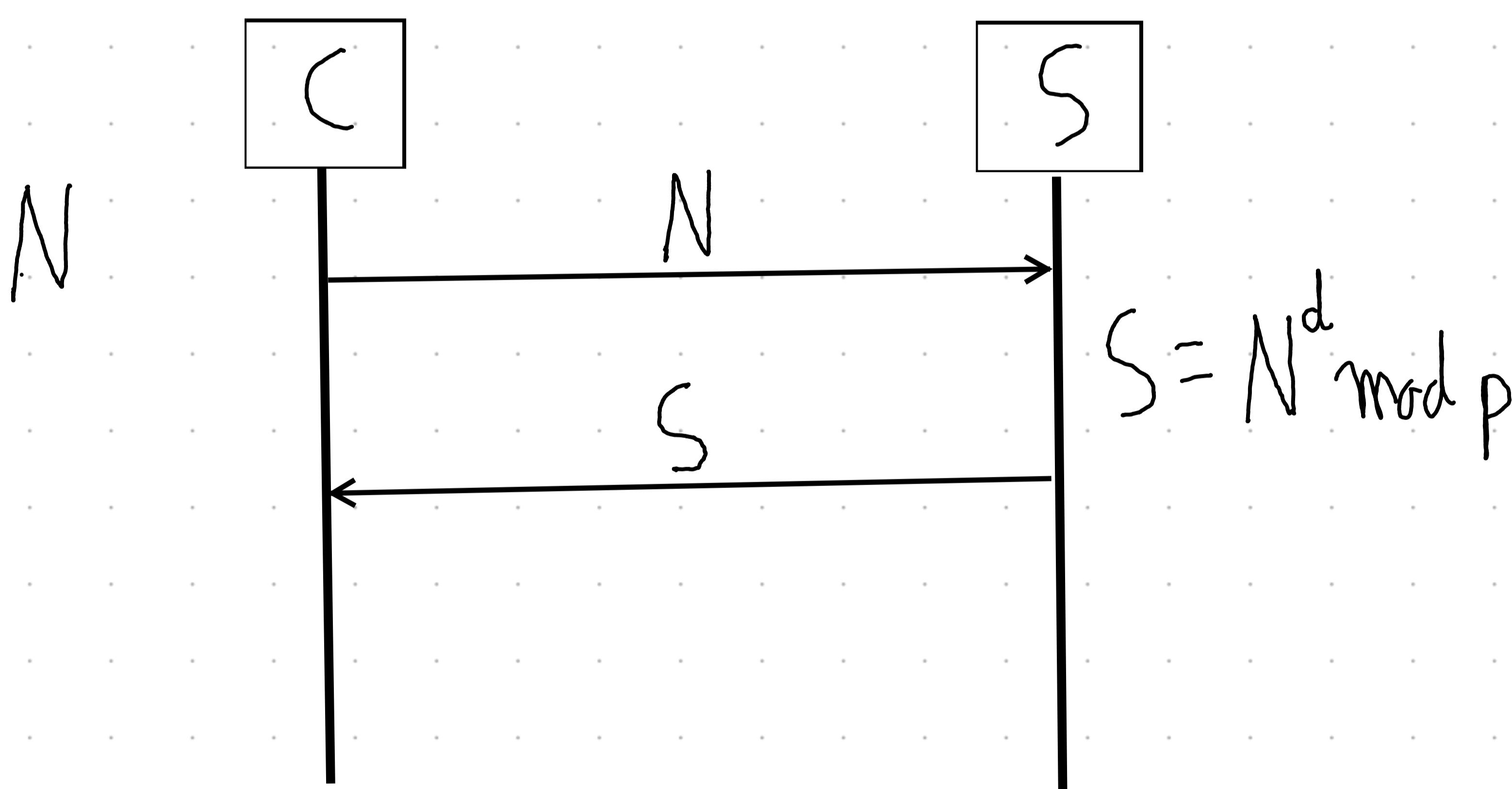
($\rightarrow S : N$

$S \rightarrow C : N^d \text{ mod } n$

$$S_{\text{PUB}} = (e, n)$$



n è sempre la moltiplicazione
di due numeri primi $n = (p \cdot q)$



Il grosso problema degli algoritmi a chiave pubblica è la lentezza, per questo motivo viene utilizzato solo per scambiarsi le chiavi per la crittografia simmetrica (RSA è circa 1000 volte più lento di DES).

