

Scheda RSA codifica e decodifica

Consegna: Determinare, dati p e q , chiave pubblica e chiave privata di Alice. Codificare i messaggi facendo uso della chiave pubblica e decodificarli facendo uso della chiave privata.

Durata: 1 ora

$p = 7, q = 11, e = 17; p = 13, q = 23, e = 25;$

Messaggi da comunicare: $M = 15; M = 121;$

Svolgimento

Chiave pubblica:

Chiave privata:

Messaggi Codificati:

Decodifica Messaggi:

Chiave pubblica:

Chiave privata:

Messaggi Codificati:

Decodifica Messaggi
