(a) Supponiamo si voler utilizzare RSA per spedire il messaggio $PERA$ utilizzando un alfabeto di 22 lettere (compreso lo spazio).

(b) Scegliere due numeri primi p e q in modo che sia possibile spedire il messaggio utilizzando un'unica trasmissione.

(c) Dopo aver calcolato $n = p \cdot q$ e $\varphi(n)$, si scelga come esponente di codifica $e = 2$ e si codifichi il messaggio.

(d) Si scriva il messaggio crittografato in termini dell' alfabeto.

1. Si elenchino con una breve descrizione tutti i possibili errori nell'implementazione del' RSA.

2. Sia $q = 37$ e $p = 41$.

   (a) Utilizzare $n = pq$ per spedire il messaggio "MAI" utilizzando RSA. Fare le cose in modo che sia necessario spedire il numero minimo di trasmissioni. (Scegliere a caso il valore di e)

   (b) decodificare il messaggio "NO" utilizzando le notazioni precedenti e sapendo che il messaggio è stato ottenuto utilizzando una sola trasmissione.

3. Sia $p = 29, q = 31, n = pq$. Assumiamo che la chiave (pubblica) di codifica sia $e = 13$.

   (a) Calcolare la chiave (segreta) di decodifica d.

   (b) Crittografare la parola "**ciao**". (Usare 4 messaggi).

   (c) Dire se è possibile scegliere $e = 5$ come chiave pubblica