1. (a) Determinare il resto della divisione per 55 del numero 3^{193}.
   (b) Determinare il resto della divisione per 91 del numero 5^{193}.
   (Sugg. fattorizzare 55 e 91 ed usare il Teorema Cinese del resto).

2. (mini-RSA) Sia $p = 7$ e $q = 13$ e sia $n = pq = 7 \cdot 13 = 91$ il modulo di questo sistema RSA. L'esponente pubblico è $E = 11$. Il messaggio è $m = 10$.
   (a) Cifrare il messaggio, cioè calcolare il resto $\tilde{m}$ della divisione di m^E per n.
   (b) Determinare l'esponente segreto D, cioè calcolare $D \in \mathbf{N}$ tale che $DE \equiv 1 \pmod{(p-1)(q-1)}$.
   (c) Decifrare $\tilde{m}$, cioè controllare che il resto della divisione di $\tilde{m}^D$ per n è uguale al messaggio originale m.

3. (a) Sia $n = 77$ il modulo di un sistema RSA. Sia $E = 13$ l'esponente che si usa per cifrare i messaggi. Determinare un esponente $D \in \mathbf{N}$ tale che $(x^E)^D \equiv x \pmod{n}$ per ogni messaggio $x \in \mathbf{Z}_{77}^*$.
   (b) Sia $n = 55$ il modulo di un sistema RSA. Sia $E = 13$ l'esponente che si usa per cifrare i messaggi. Determinare un esponente $D \in \mathbf{N}$ tale che $(x^E)^D \equiv x \pmod{n}$ per ogni messaggio $x \in \mathbf{Z}_{55}^*$.

4. Un *numero di Carmichael* è un numero naturale che non è primo, ma per cui $x^{n-1} \equiv 1 \pmod{n}$ per ogni $x \in \mathbf{Z}_n^*$.
   (a) Dimostrare che $561 = 3 \cdot 17 \cdot 31$ è un numero di Carmichael.
   (b) Dimostrare che $8911 = 7 \cdot 19 \cdot 67$ è un numero di Carmichael.
   (c) Dimostrare che un numero di Carmichael ha almeno tre fattori primi (Sugg. usare il fatto che per ogni primo p esiste $g \in \mathbf{Z}_p^*$ di ordine $p-1$).

5. (a) Sia $p > 2$ un primo. Dimostrare che $\{x \in \mathbf{Z}_p : x^2 = 1\} = \{\pm 1\}$.
   (b) Determinare tutti gli $x \in \mathbf{Z}_{15}^*$ per cui $x^2 = 1$. Stessa domanda per $\mathbf{Z}_{21}^*$.
   (c) Sia n prodotto di due primi dispari. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?
   (d) Determinare tutti gli $x \in \mathbf{Z}_9^*$ per cui $x^2 = 1$. Stessa domanda per $\mathbf{Z}_{25}^*$.
   (e) Sia n quadrato di un numero primo $p > 2$. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?

6. Per trasformare un testo in una serie di numeri, usiamo questa tabella.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	spazio
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	00

   (a) Verificare che il testo "PIPPO BAUDO" viene trasformato in "14091414130002011904 13".

   Il modulo del criptosistema RSA usato in questo esercizio è uguale a $n = 2000000002864822776563$. L'esponente pubblico è uguale a $E = 25042003$.
   (b) Far vedere che il messaggio "1409141413000201190413" della parte (a), cifrato tramite questo sistema RSA, è uguale a 474795864046624770221.
   (c) Supponiamo di intercettare il messaggio cifrato $\tilde{m} = 605233533198702885420$. Cercare di rompere questo sistema e di decifrare e leggere il messaggio. (Suggerimento: trovare la fattorizzazione $n = pq$ e calcolare l'esponente segreto, cioè determinare D tale che $DE \equiv 1 \pmod{(p-1)(q-1)}$. Il messaggio originale è allora uguale a $\tilde{m}^D \pmod{n}$.)

7. Alice e Bob vogliono comunicare in segreto. Decidono di usare il metodo delle applicazioni lineari. Come nell'esercizio 6, fanno corrispondere le lettere dell'alfabeto agli interi modulo 22 (cf. tabella). Fissano come chiave di crittaggio una matrice due per due K a coefficenti in $\mathbf{Z}/22\mathbf{Z}$ tale che esista K^{-1} nell'insieme $M_2(\mathbf{Z}/22\mathbf{Z})$. Ogni parola da codificare è suddivisa in coppie di due lettere consecutive $\mathbf{v} = [1^a\text{lettera}, 2^a\text{lettera}]^t$. La funzione di crittaggio è data da $\mathbf{v} \longmapsto e_K(\mathbf{v}) = K \cdot \mathbf{v} \pmod{22}$ e quella di decodifica da $\mathbf{w} \longmapsto d_K(\mathbf{w}) = K^{-1} \cdot \mathbf{v} \pmod{22}$. Alice e Bob scelgono la chiave $K = \begin{pmatrix} 4 & 5 \\ 1 & 10 \end{pmatrix}$
   (a) Trovare la chiave di decodifica.
   (b) Alice vuole mandare il messaggio CIAO a Bob. Che messaggio invia?
   (c) Testare la decodifica.
   (d) Bob propone ad Alice di usare la matrice $\begin{pmatrix} 1 & 0 \\ 10 & 11 \end{pmatrix}$ e Alice rifiuta. Perché?