ESERCIZI SU RSA

(1) Sia $q = 60$. Determinare $\phi(q)$, dove ϕ è la funzione di Eulero.
SOL $\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = (2^2 - 2) \cdot 2 \cdot 4 = 16.$

(2) Calcolare il resto di 3^{24} nella divisione per 23 (suggerimento: applicare il Teorema di Eulero).
SOL $\phi(23) = 22$, $MCD(3, 23) = 1$. Per il Teorema di Eulero si ha:

$$3^{22} \equiv_{33} 1$$

Quindi $3^{24} = 3^{22}3^2 \equiv_{33} 3^2 = 9$ che è il resto cercato.

(3) Le seguenti coppie possono essere utilizzate come modulo e chiave pubblica nel codice RSA?

V	**F**	$(105, 6)$;
V	**F**	$(77, 7)$;
V	**F**	$(39, 20)$.

SOL $105 = 21 \cdot 5 = 3 \cdot 5 \cdot 7$ quindi $\phi(105) = 2 \cdot 4 \cdot 6 = 48$. $MCD(48, 6) \neq 1$. Risposta NO.
$\phi(77) = \phi(7 \cdot 11) = \phi(7)\phi(11) = 6 \cdot 10 = 60$, $MCD(60, 7) = 1$, risposta SI.
$\phi(39) = \phi(3 \cdot 13) = \phi(3)\phi(13) = 2 \cdot 12 = 24$, $MCD(24, 20) \neq 1$, rispsota NO.

(4) Esiste un codice RSA che ha chiave pubblica uguale a $(15, 5)$ e chiave privata uguale a $(15, 3)$?
SOL $\phi(15) = \phi(3 \cdot 5) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8$. Inoltre $MCM(8, 5) = 1$, quindi la chiave pubblica è corretta, ma non corrisponde alla chiave provata perché $3 \cdot 5 = 15 \not\equiv_8 1$.

(5) Esiste un codice RSA che ha chiave pubblica uguale a $(55, 13)$ e chiave privata uguale a $(55, 37)$?
SOL $\phi(55) = \phi(5 \cdot 11) = \phi(5) \cdot \phi(11) = 4 \cdot 10 = 40$. Inoltre $MCM(13, 40) = 1$ e $13 \cdot 37 = 481 \equiv_{40} 1$. Quindi la risposta è positiva.

(6) Sia $m = 43 \cdot 7 = 301$, $s_1 = 2$ e $s_2 = 5$.
Possiamo utilizzare i numeri m e s_1 come modulo e chiave pubblica nel sistema RSA?
Possiamo utilizzare i numeri m e s_2 come modulo e chiave pubblica nel sistema RSA?
Nel caso di risposta affermativa, trovare la chiave privata corrispondente.
SOL $\phi(m) = \phi(7) \cdot \phi(43) = 6 \cdot 42 = 252$. $MCD(252, 2) \neq 1$. Risposta NO

Se invece $s_2 = 5$, abbiamo $MCD(\phi(m), s_2) = MCD(252, 5) = 1$. Inoltre, utiizzando l'algoritmo di Euclide si vede che $1 = 101 \cdot 5 - 2 \cdot 252$. Quindi la chiave privata corrispondente è $t = 101$.

(7) Inventare un codice RSA con modulo $m = 35$, ovvero trovare due numeri s, t tali che $(35, s)$ e $(35, t)$ possono essere utilizzati come chiave pubblica e chiave privata, rispettivamente.

SOL Poiché $m = 5 \cdot 7$ e 5 e 7 sono relativamente primi, sappiamo che $\phi(m) = \phi(5) \cdot \phi(7) = 4 \cdot 6 = 24$, dove ϕ è la funzione di Eulero. La condizione per creare un codice è che $s \cdot t \equiv_{\phi(m)} 1$, quindi, ad esempio, possiamo scegliere $s = t = 5$ perché in questo caso $s \cdot t = 25 \equiv_{24} 1$.

(8) Sia $q = 33$. Mostrare che la coppia $(q, 3)$ può essere scelta come chiave pubblica del codice RSA. Trovare inoltre la chiave privata corrispondente e cifrare il numero 4, e decifrare il risultato ottenuto.

SOL $4^3 = 64 \equiv_{33} -2 \equiv_{33} 31$. Quindi se codifichiamo il numero 4 otteniamo il numero 31. Se decodfichiamo 31, dovremmo ottenere 4. Verifichiamolo:
$31^7 \equiv_{33} (-2)^7 = (-2)^2 \cdot (-2)^5 = 4 \cdot (-32) \equiv_{33} 4$.

(9) In questo esercizio è consentito l'uso della calcolatrice tascabile, ma cercate di ridurre il più possibile i numeri prima di fare le operazioni. Considera il codice RSA con chiave privata $(33, 3)$. Usando tale chiave, decodifica i cinque numeri seguenti:

1 8 28 20 15

Se n_1, n_2, n_3, n_4, n_5 sono i cinque numeri ottenuti, traduci ogni numero in una lettera utilizzando la tabella seguente e leggi il messaggio che corrisponde a

$$n_1 - n_2 - n_3 - n_2 - n_4 - n_5$$

A	1	N	14
B	2	O	15
C	3	P	16
D	4	Q	17
E	5	R	14
F	6	S	15
G	7	T	16
H	8	U	17
I	9	V	18
J	10	W	19
K	11	X	20
L	12	Y	21
M	13	Z	22

Infine, utiizzando la chiave pubblica $(33, 7)$ e la stessa tabella di corrispondenza numeri-lettere. utilizza i 6 numeri per la risposta "GRAZIE", e codificali.