COGNOME ..... *NOME* .....

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare e sintetiche*.
NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 6 punti.

1(a) *Calcolare la cardinalità di* $\mathbf{Z}_n^*$, *dove* $n = 2 \cdot 5^3 \cdot 7^2$.
(b) Elencare gli elementi di $\mathbf{Z}_{18}^*$ *e per ognuno di essi indicare il suo inverso moltiplicativo.*

(a) Il valore in n della funzione φ di Eulero è per definizione la cardinalità di $\mathbf{Z}_n^*$, il gruppo degli elementi di $\mathbf{Z}_n$ che hanno inverso moltiplicativo. Abbiamo

$$\varphi(2 \cdot 5^3 \cdot 7^2) = \varphi(2)\varphi(5^3)\varphi(7^2) = 1 \cdot 5^3(1 - \frac{1}{5}) \cdot 7^2(1 - \frac{1}{7}) = 4200.$$

(b) Gli elementi di $\mathbf{Z}_{18}^*$ sono dati dagli $\bar{x} \in \mathbf{Z}_{18}$ per cui $mcd(x, 18) = 1$:

$$\mathbf{Z}_{18}^* = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}, \overline{13}, \overline{17}\}.$$

Dalla tavola moltiplicativa di $\mathbf{Z}_{18}^*$ si trova facilmente che

$$\bar{1} = \bar{1}^{-1}, \quad \bar{5}^{-1} = \overline{11}, \quad \bar{7}^{-1} = \overline{13}, \quad \overline{17}^{-1} = \overline{17}.$$

2. *Calcolare il resto della divisione di* 5^{100} *per* 63 *(Determinare un numero* $x \in \{0, \ldots, 62\}$ *etc...).*

Si calcola facilmente $\bar{5}^2 = \overline{25}$ e $\bar{5}^3 = \overline{125} = \overline{-1}$. Da ciò segue che

$$\bar{5}^{100} = \bar{5}^{3 \cdot 33} \cdot \bar{5} = \overline{-1}^{33} \cdot \bar{5} = \overline{-5} = \overline{58} \mod 63.$$

3.(a) *Verificare che* $n = 21$ *non soddisfa il Piccolo Teorema di Fermat.*
.(b) Applicare a $n = 91$ *il test di Miller-Rabin con base* $a = 3$.

(a) Dobbiamo far vedere che esiste almeno una classe $\bar{a} \in \mathbf{Z}_n$ diversa da $\bar{0}$ tale che $a^{n-1} \not\equiv 1 \mod n$. Prendiamo ad esempio $\bar{a} = \bar{2}$. Troviamo infatti

$$\bar{2}^{20} = \bar{2}^6 \cdot \bar{2}^6 \cdot \bar{2}^6 \cdot \bar{2}^2 \equiv \bar{4} \not\equiv 1 \mod 21.$$

(b) Scriviamo $91 - 1 = 90 = 2 \cdot 45$. Sia

$$\bar{b} = \bar{3}^{45} = \bar{3}^{6 \cdot 7} \cdot \bar{3}^3 = \bar{1}^7 \cdot \overline{27} = \overline{27}.$$

Poiché $\bar{b}^2 = \overline{729} = \bar{1}$, mentre $\bar{b} \neq \overline{-1}$, il test di Rabin-Miller indica che 91 non è primo. Giustamente. Infatti $91 = 7 \cdot 13$.

4. *Il signor Rossi desidera ricevere messaggi criptati e decide di adottare il criptosistema RSA. La ditta gli fornisce un kit con chiavi pubbliche* N *ed* E *e chiave segreta* D.
   (a) La ditta gli fornisce un kit con chiavi pubbliche $N = 143$ *ed* $E = 23$ *e chiave segreta* $D = 3$. *Vanno bene? (spiegare)*
   (b) Preparare un kit di chiavi pubbliche N', E' *e chiave segreta* D' *per il signor Bianchi, con* $N' = 77$ *ed* $E' = 7$.
   (c) Spedire a Verdi, con chiavi pubbliche $N = 77$ *ed* $E = 7$, *il messaggio* $m = 13$ *dopo averlo criptato.*

(a) Il numero N si fattorizza come $N = p \cdot q$ con $p = 11$ e $q = 13$. In questo caso $(p-1)(q-1) = 10 \cdot 12 = 120$. La chiave $E = 23$ soddisfa $mcd(23, 120) = 1$. Dunque appartiene a Z_{120}^*, come deve essere. Invece la chiave

$D = 3$ non appartiene Z^*_{120}, in quanto $mcd(3, 120) = 3 \neq 1$. Inoltre $E \cdot D = \overline{69} \neq \bar{1}$ in Z^*_{120}. Conclusione questo kit non va bene.
(b) Il numero N' si fattorizza come $N' = p' \cdot q'$ con $p' = 7$ e $q' = 11$. In particolare $(p-1)(q-1) = 60$. La chiave $E' = 7$ soddisfa $mcd(7, 60) = 1$, quindi appartiene a $\mathbf{Z}^*_{60}$ come deve. La chiave segreta D' è l'inverso di E' modulo 60, ossia: $D' = (7)^{-1}$ modulo 60. Risolvendo l'equazione diofantea $7D' + k60 = 1$ con l'algoritmo di Euclide si trova $D' = 43$.
(c) Osserviamo innanzitutto che $mcd(m, N) = mcd(13, 77) = 1$ come deve essere. Il messaggio $m = 13$ criptato con chiavi pubbliche $N = 77$ ed $E = 7$ è dato m^E mod N, ossia $13^7 = 62$ mod 77.

5. *Il signor Rossi e il signor Bianchi desiderano condividere un codice segreto e lo fanno adottando il sistema Merkle-Diffie-Hellman. Si accordano pubblicamente sul numero primo $p = 37$ e sulla radice primitiva $\bar{g} = \bar{2}$.*

(a) Verificare che $\bar{g} = \bar{2}$ è effettivamente una radice primitiva in $\mathbf{Z}^*_{37}$.
(b) Una spia intercetta i numeri che vengono scambiati fra Bianchi e Rossi $\overline{n} = \overline{17}$ e $\overline{m} = \overline{13}$. Cosa deve fare per ricostruire il codice segreto di Bianchi e Rossi?
(c) La spia ricostruisce il codice segreto. Qual è questo codice?

(a) Si verifica facilmente che $\bar{2}^{12} = \overline{26} \neq \bar{1}$ e $\bar{2}^{18} = \overline{36} = \overline{-1} \neq \bar{1}$ modulo 37. Dunque $\bar{g} = \bar{2}$ è effettivamente una radice primitiva in $\mathbf{Z}^*_{37}$.
(b) I numeri che vengono scambiati fra Bianchi e Rossi sono $\overline{n} = \overline{17} = \bar{2}^b$ e $\overline{m} = \overline{13} = \bar{2}^r$, dove b ed r sono rispettivamente gli esponenti segreti di Bianchi e Rossi. Per ricostruire il codice segreto $\bar{2}^{br} = 2^{rb}$ la spia ha bisogno di b ed r. Quindi deve calcolare il logaritmo discreto in base 2 di $\bar{n}$ e $\bar{m}$ in $\mathbf{Z}^*_{37}$.
(c) Usando il calcolo dell'indice o l'algoritmo baby-steps-giant-steps o calcolando le prime potenze di $\bar{2}$ modulo 37 si trova

$$\log \overline{17} = 7, \quad \log \overline{13} = 11.$$

Dunque il codice segreto risulta $\bar{2}^{77} = \overline{32}$.