Elementi di Crittografia
Esercitazione

1. Descrivere lo schema di cifrario di Feistel.
2. La chiave RSA di Alice è $N = 5 \cdot 13$ con $e = 29$ esponente pubblico di cifratura.
   (a) Determinare l'esponente privato di decifratura d.
   (b) Cifrare il messaggio 2 da inviare a Alice.
   (c) Alice deve firmare il messaggio 6. Determinare la coppia (messaggio, firma).
3. Sia (N, e) la chiave pubblica RSA di Alice. Spiegare perché se Eve riesce a fattorizzare N, allora può decifrare i messaggi per Alice.
4. Descrivere la modalità di funzionamento CBC. La cifratura che si ottiene in questa modalità è deterministica?
5. Descrivere lo scambio della chiave alla Diffie Hellman. Modificare questo protocollo in modo che tre utenti A, B, e C possano ottenere una chiave comune (a tutti e tre).
6. Bob sceglie $p = 11, g = 2$ e esponente privato $a = 5$. Cifrare con il crittosistema di Elgmal il messaggio $x = 7$.
7. Descrivere uno schema a soglia $(3, 6)$ per condividere il segreto $M = 19$.
8. Mostrare che il numero 91 è uno pseudoprimo in base 3.
9. Alice vuole regalare la sua bicicletta a Bob, ma purtroppo Alice lavora di giorno e Bob di notte e non possono incontrarsi. Alice sa che sia lei che Bob possiedono una catena con un lucchetto. Alice chiama Bob e dice: "Idea! Lascio la bici sotto casa mia e ...". Quale potrebbe essere la sua idea?
10. $(*)$ Alice and Bob sono molto amici e decidono di condividere lo stesso modulo RSA N. Hanno diversi esponenti di cifratura e_A e e_B – e si ha che e_A e e_B sono primi fra loro. La loro amica Carol manda lo stesso messaggio x a Bob e Alice, ottenendo $y_A = x^{e_A}$ e $y_B = x^{e_B} \pmod N$. Mostrare che Eve, che conosce le chiavi pubbliche e osserva i CT y_A e y_B, può ricavare x.