Elementi di Crittografia
Esercitazione

1. 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).
2. 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).
3. Bob sceglie $p = 11, g = 2$ e esponente privato $a = 5$. Cifrare con il crittosistema di Elgmal il messaggio $x = 7$.
4. Descrivere uno schema a soglia $(3, 6)$ per condividere il segreto $M = 19$.
5. Mostrare che il numero 91 è uno pseudoprimo in base 3.

6.($*$) 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.