Università degli Studi Roma Tre
Corso di Studi in Matematica, a.a. 2016/2017
CR410 – Crittografia1
Esercizi
Foglio 5

1. In $\mathbb{F}_{16} \simeq \mathbb{Z}_2[x]/(x^4 + x + 1)$ calcolare
$$[x^2 + x] \cdot [x^3 + \bar{1}], \quad [x^2 + x]^{-1}, \quad [x^3 + x + \bar{1}]^{-1}.$$

2. In $\mathbb{F}_{27} \simeq \mathbb{Z}_3[x]/(x^3 - x - 1)$ calcolare
$$[-x^2 + x] \cdot [x^2 + \bar{2}], \quad [x^2 + \bar{2}x]^{-1}, \quad [x^2 + x + \bar{2}]^{-1}.$$

3. Calcolare la chiave comune di Alice e Bob nello scambio alla Diffie-Hellman con le scelte $G = \mathbb{Z}_{241}, g = 7$ e gli esponenti $a = 18$ e $b = 64$.

4. Sia G un gruppo ciclico moltiplicativo di ordine n, e sia $n = \prod_{i=1}^{s} p_i^{e_i}$. Mostrare che $g \in G$ è un generatore $\iff g^{\frac{n}{p_i}} \neq 1$ per $i = 1, \ldots, s$.

5. Trovare radici primitive per $\mathbb{F}_q$, con $q = 241, 487, 1187$.

6. La chiave Elgamal di Alice è $(p = 61, g = 2, a = 12, \beta = 9)$.
   - Cifrare e poi decifrare il messaggio $x = 21$ da inviare ad Alice.
   - Alice deve firmare il messaggio $x = 15$. Qual è la firma? Verificare l'autenticità della firma.

7. Applichiamo l'algoritmo di Shanks a $G = \mathbb{Z}_{61}^*$ con generatore $g = 2$. Nota la lista $L_1 = \{(0, 1), (1, 12), (5, 13), (3, 20), (2, 22), (6, 34), (7, 42), (4, 57)\}$, calcolare il logaritmo discreto di $y_1 = 27, y_2 = 37, y_3 = 47$.

8. Mostrare che l'algoritmo di Shanks funziona, cioè che è sempre possibile trovare una coppia in L_1 e un'altra in L_2 con la stessa seconda componente.