Università degli Studi Roma Tre
Corso di Studi in Matematica
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. Considerare una versione dello scambio di Diffie-Hellmann in cui Alice, scelto a e ricevuto g^b da Bob, calcola $g^{b+a} \pmod p$, e analogamente Bob scelto b e ricevuto g^a, calcola $g^{a+b} \pmod p$. Che problemi ci sono con questa versione del protocollo?

5. 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 $i = 1, \ldots, s$.

6. Una *falsificazione* per l'utente Alice in uno schema di firma è una coppia (x, y) che supera la verifica senza essere stata prodotta da Alice.

   Nello schema RSA con chiave *pubblica* di Alice ($N_A = 187, e_A = 7$), produrre una falsificazione (senza ricavare la chiave privata).

7. Mostrare che in $\mathbb{F}_{p^m}$ si ha che $(a + b)^p = a^p + b^p$.

8. Trovare radici primitive per $\mathbb{F}_q$, con $q = 163$ e 271.

9. 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.