

Università degli Studi Roma Tre
CR410 – Crittografia a chiave pubblica
Esercizi
Foglio 5

1. In $\mathbb{F}_{16} \simeq \mathbb{Z}_2[x]/(x^4 + x + 1)$ calcolare

$$[x^2 + x] \cdot [x^3 + \bar{1}], \quad [x^2 + x]^{-1}, \quad [x^3 + x + \bar{1}]^{-1}.$$

Sol. $[x^2 + x] \cdot [x^3 + \bar{1}] = [x + \bar{1}], \quad [x^2 + x]^{-1} = [x^2 + x + \bar{1}],$
 $[x^3 + x + \bar{1}]^{-1} = [x^2 + \bar{1}]$

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

$$[-x^2 + x] \cdot [x^2 + \bar{2}], \quad [x^2 + \bar{2}x]^{-1}, \quad [x^2 + x + \bar{2}]^{-1}.$$

Sol. $[-x^2 + x] \cdot [x^2 + \bar{2}] = [\bar{2}x + \bar{1}], \quad [x^2 + \bar{2}x]^{-1} = [x + \bar{1}],$
 $[x^2 + x + \bar{2}]^{-1} = [\bar{2}x^2 + x + \bar{2}].$

3. Calcolare la chiave comune di Alice e Bob nello scambio alla Diffie-Hellman con le scelte $G = \mathbb{Z}_{61}^*, g = 2$ e gli esponenti $a = 12$ e $b = 33$.

Sol. 58

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?

Sol. Eve conosce g^a e g^b , per ottenere la chiave basta che calcoli $g^a \cdot g^b$.

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 $i = 1, \dots, s$.

Sol. Se g è un generatore, allora $g^k \neq 1$ per ogni $k < n$, quindi $g^{\frac{n}{p_i}} \neq 1$ per $i = 1, \dots, s$.

Se g non è generatore, allora esiste $k < n$ con $g^k = 1$. Si ha $k|n$ per il teorema di Lagrange, e siccome $k < n$, si ha $p_i k|n$ per qualche p_i divisore di n , e cioè $n = p_i k h$ per qualche $h \geq 1$; dunque $g^{\frac{n}{p_i}} = g^{kh} = 1$.

6. Trovare una radice primitiva per \mathbb{F}_{83} e una per \mathbb{F}_{163} .

Sol. Sia per \mathbb{F}_{83} che per \mathbb{F}_{163} , si ha che 2 è una radice primitiva.

7. 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.

Sol. Qui il risultato dipende dalla scelta di h . Con $h = 17$ si ha $e(21, 17) = (44, 54)$.

8. 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 $y_1 = 27, y_2 = 37, y_3 = 47$.

Sol: I LD sono rispettivamente 18, 39, 20

9. Utilizzare l'algoritmo di Pohlig-Hellman per trovare il logaritmo discreto di 118 in base 2 in \mathbb{Z}_{181} .

[informazioni parziali: $2^{60} \equiv 48 \quad 2^{36} \equiv 59$]

Sol: $x = 37$

10. Utilizzare il metodo dell'indice (index calculus) per calcolare il logaritmo discreto $\log_7(19)$ su \mathbb{F}_{71} .

Sol: $x = 16$. Una possibile scelta è $x_1 = 6$ e $x^* = 2$

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

$$(a + b)^{p^k} = a^{p^k} + b^{p^k}$$

Sol. Basta osservare che se p è primo allora $p \mid \binom{p}{i}$ per $1 \leq i \leq p - 1$.
La seconda uguaglianza si dimostra per induzione su k .