

**Università degli Studi Roma Tre**  
**Corso di Studi in Matematica**  
**CR410 – Crittografia1**  
**Esercizi**  
**Foglio 6**

1. 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

2. 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:**  $x = 37$

3. 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  $x^* = 2$

4. In una versione del crittosistema di Massey-Omura in  $\mathbb{F}_{32} = \mathbb{Z}_2[x]/(x^5 + x^3 + 1)$ , si ha per Alice  $e_A = 5$  e per Bob  $e_B = 16$ . Determinare  $d_A$  e  $d_B$  e descrivere il procedimento (e i conti) che portano alla cifratura e alla decifratura del messaggio  $m = x + 1$

**Sol:**  $d_A = 25, d_B = 2 \cdot (1 + x)^5 = x + x^3 + x^4; (x + x^3 + x^4)^{16} = x^4; (x^4)^{25} = 1 + x + x^3$ .

5. In uno schema a soglia di Shamir in  $\mathbb{Z}_{31}$  con  $m = 3$  valore della soglia, per gli utenti  $A, B, C$  abbiamo che le ombre  $(x, f(x))$  sono rispettivamente  $(2, 24), (3, 8)$  e  $(5, 6)$ . Determinare il segreto.

**Sol:** Il polinomio è  $5x^2 + 21x + 24$ .

6. Sia dato un sistema di Diffie-Hellman per lo scambio di chiavi nel campo  $\mathbb{Z}_{181}$  con radice primitiva  $g = 2$ .

Supponiamo che due utenti  $A$  e  $B$  si siano scambiati una chiave con questo sistema:  $A$  invia  $g^a = 125$  e  $B$  risponde inviando  $g^b = 66$ .

Utilizzando un algoritmo a vostra scelta, calcolare  $a$  e trovare la chiave privata condivisa da  $A$  e  $B$ .

**Sol:**  $a = 108$ , chiave = 42