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

1. 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.

2. Quali problemi di sicurezza, legati all'autenticazione, può presentare un crittosistema basato sul doppio lucchetto (Shamir o Massey-Omura)?

3. 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 parte dei conti) che portano alla cifratura e alla decifratura del messaggio $m = x + \bar{1}$

4. 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.

5. 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.

6. Si consideri il codice binario di Hamming di lunghezza 7 e dimensione 4. Correggere gli eventuali errori nelle parole 1010110, 1101101, 0111110. Mostrare che ogni parola di $\mathbb{Z}_2^7$ è a distanza minore o uguale a 1 da una parola del codice.

   Mostrare che un codice binario di lunghezza n che corregge t errori può contenere un numero di parole minore o uguale di

$$\frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}}.$$