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.

   Sol. Qui il risultato dipende dalla scelta di h. Con $h = 17$ si ha $e(21, 17) = (44, 54)$. Per la firma, sempre con $h = 17$, si ha $l = 53$, $z_2 = (x - az_1)l = 51 \pmod{60}$, e la firma è $(15, 44, 51)$.

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

   Sol: Se non mettiamo in atto anche un autenticazione, Eve può sostituirsi a Bob nel protocollo: sceglie una coppia (e_E, d_E), intercetta le trasmissioni da Bob e sostituisce $m^{e_A e_B}$ con $m^{e_A e_E}$, e alla fine del protocollo può leggere il messaggio di Alice.

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

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

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.

   Sol: Usando l'interpolazione di Lagrange per ricostruire il temine noto, abbiamo $L_{x_1=2}(x) = \frac{(x-3)(x-5)}{(2-3)(2-5)}$, quindi $L_{x_1=2}(0) \equiv 5$; analogamente, $L_{x_2=3}(0) \equiv -5$ e $L_{x_3=5}(0) \equiv 1$. Il termine noto è quindi $24 \cdot 5 + 8(-5) + 6 \equiv 24$.

   Il polinomio è $5x^2 + 21x + 24$.

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.

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

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 a

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

   Sol: Gli errori nelle parole 1010110, 1101101, 0111110 sono rispettivamente in prima, quinta e sesta posizione.

   Il codice di Hamming contiene $2^4 = 16$ parole. Il numero di parole nella 'sfera' di centro una parola del codice e raggio 1 è $1+7 = 8 = 2^3$, e siccome il codice è 1-correttore queste sfere sono fra loro disgiunte. Tali sfere contengono quindi $2^3 \cdot 2^4 = 2^7$ parole, e quindi ogni parola di $\mathbb{Z}_2^7$ è a distanza minore o uguale a 1 da una parola del codice.

   In modo analogo, osservando che una sfera di centro una parola e raggio t contiene $\sum_{i=0}^{t} \binom{n}{i}$ parole, si dimostra l'ultima affermazione.