UNIVERSITÀ DEGLI STUDI ROMA TRE
Corso di Laurea in Matematica
CR410 - Crittografia 1
A.A. 2016/2017

II Esonero

ESERCIZIO 1.

Illustrare il metodo ρ di Pollard e utilizzarlo per fattorizzare $n = 899$.
[Potete scegliere per esempio $x_0 = 20$.]

ESERCIZIO 2.

1. Illustrando il procedimento utilizzato, verificare che 2 è una radice primitiva in $\mathbb{Z}_{59}^*$ e trovare un'altra radice primitiva per $\mathbb{Z}_{59}^*$.

2. Usare l'algoritmo di Shanks per calcolare in $\mathbb{Z}_{59}^*$ il logaritmo discreto di 7 in base 2; la lista L_1 (da riordinare) è

$$\{(1, 20), (2, 46), (3, 35), (4, 51), (5, 17), (6, 45), (7, 15), (8, 5)\}.$$

3. Descrivere il crittosistema di Elgamal e lo schema di firma di Elgamal.

4. Fare un esempio di cifratura/decifratura **oppure** firma/verifica Elgamal usando i parametri $(p = 59, g = 2, a = 19)$ e un messaggio a vostra scelta.

ESERCIZIO 3.

1. Costruire un campo con 27 elementi $\mathbb{F}_{27}$.

2. Descrivere il crittosistema di Massey-Omura.

3. Supponiamo di avere un CS di Massey-Omura in $\mathbb{F}_{27}$ in cui per Alice si ha $e_A = 3$ e per Bob $e_B = 5$. Determinare d_A e d_B e calcolare i primi passaggi del CS per il messaggio $m = x + \bar{1}$ (cioè potete fermarvi a $m^{e_A e_B}$).