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

Appello A

ESERCIZIO 1.

(a) Descrivere il test di Solovay-Strassen, e usarlo (per due iterazioni) per testare la primalità di $n = 29$.
(b) Sia m un intero dispari. Sia $G(m)$ l'insieme formato dagli elementi b di $U(\mathbb{Z}_m)$ tali che m è uno pseudo-primo di Eulero in base b. Dimostrare che $G(m)$ è un gruppo. Dimostrare che l'ordine di $G(m)$ è pari.
(c) Descrivere la fattorizzazione alla Fermat e applicarla a $N = 667$.
(d) Sia dato un crittosistema RSA con $N = 667$, con esponente di cifratura $e = 5$; determinare l'esponente di decifratura d e cifrare il messaggio $m = 14$.

ESERCIZIO 2.

(a) Utilizzare l'algoritmo di Pohlig-Hellman per trovare il logaritmo discreto di 7 in base 5 in $\mathbb{Z}_{73}$, descrivendo brevemente l'algoritmo. [informazioni parziali: $5^{24} \equiv 8$]
(b) Descrivere lo schema di firma di Elgamal.

ESERCIZIO 3.

In uno schema di secret sharing a soglia di Shamir in $\mathbb{Z}_{29}$ con $m = 3$ valore della soglia, per gli utenti A, B, C abbiamo che le ombre $(x, f(x))$ sono rispettivamente $(2, 23)$, $(3, 0)$ e $(5, 22)$. Descrivere lo schema e determinare il segreto.