CR1 – Crittografia 1

Alfonso Pesiri - Fabrizio Zaccari

Tutorato 7 – 22 Maggio 2008

Esercizio 1. Si costruisca $\mathbb{F}_9$ e si determini una sua radice primitiva. Utilizzando tali parametri (campo, polinomio e radice primitiva), si effettui uno scambio di chiavi con l'algoritmo di Diffie – Hellmann.

Esercizio 2. Utilizzando l'algoritmo di Pohlig – Hellmann, calcolare i seguenti logaritmi discreti:

1. $\log_3 4$, $p = 7$;
2. $\log_{71} 210$, $p = 251$;
3. $\log_2 28$, $p = 37$.

Esercizio 3. Si consideri l'alfabeto binario $\{0, 1\}$. Un utente A vuole spedire, utilizzando il crittosistema di El Gamal con pacchetti fissi di 7 caratteri, il seguente messaggio: 10110101010101. Dopo aver stabilito i parametri coerentemente con i dati iniziali, si consideri $x_B = 7$.

Esercizio 4. Sia dato un crittosistema di El Gamal con chiavi pubbliche

$$(p, g, g^{x_A}) = (31, 3, 25), \ (p, g, g^{x_B}) = (31, 3, 17),$$

dove B invia un messaggio ad A. Sia $c = 21$. Decifrare c attaccando il crittosistema con un algoritmo per il calcolo del logaritmo discreto.

Esercizio 5. Costruire un crittosistema di El Gamal in $\mathbb{F}_9$ che invia pacchetti di 2 bit e spedire il seguente messaggio: 1001

Esercizio 6. Si consideri l'alfabeto binario $\{0, 1\}$ e un sistema di Massay – Omura che invia pacchetti fissi di 6 caratteri. Si supponga che l'utente B ricevente utilizzi $x_B = 3$. Dopo aver fissato i parametri coerentemente con i dati iniziali, spedire il seguente messaggio:

$$010010110111$$