Matematica Discreta. Esercizi 8. Baby-steps-giant-steps. Applicazioni del logaritmo discreto. Roma, 25 aprile 2008.

N.B.: nei calcoli aiutarsi con PARI/GP.

1. Sia $p = 37$.
   (a) Verificare che $\bar{2}$ è una radice primitiva in $\mathbf{Z}_p^*$.
   (b) Fissata la base $\bar{g} = \bar{2}$, calcolare $\log 2$, $\log 5$, $\log 11$. (Usare il calcolo dell'indice oppure baby-steps-giant-steps).

2. Il signor Bianchi e il signor Rossi vogliono condividere un codice segreto senza il rischio che venga intercettato. Si accordano sul primo $p = 97$ e la radice primitiva $\bar{g} = \bar{5}$ (è la più piccola...verificare...). Bianchi usa il suo esponente segreto b e spedisce a Rossi $\bar{g}^b = 28$, Rossi usa il suo esponente segreto r e spedisce a Bianchi $\bar{g}^r = 21$. Qual è il codice segreto comune di Bianchi e Rossi??

Consideriamo adesso la seguente tabella di conversione.

1	2	3	4	5	6	7	8	9	?	-	-	-	-	-	-	-	-	-	-	-
01	02	03	04	05	06	07	08	09	10	-	-	-	-	-	-	-	-	-	-	-

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	-	-
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	-	-

3. Il signor Rossi desidera ricevere messaggi criptati e decide di adottare il criptosistema ElGamal. Le sue chiavi pubbliche sono il primo $p = 31$, la classe primitiva $\bar{g} = \bar{3}$ e il numero $E = 26$.
   (a) Una spia è riuscita però a ricostruire la sua chiave segreta D. Qual è?
   (b) Rossi riceve da Bianchi un messaggio composto dalle seguenti tre stringhe:

$$(c_1, c_2) = (\overline{9}, \overline{15}), \qquad (d_1, d_2) = (\overline{27}, \overline{25}), \qquad (e_1, e_2) = (\overline{19}, \overline{19}).$$

   Che cosa gli ha mandato a dire?
   (c) Riusciamo a ricostruire il messaggio di Bianchi anche senza sapere la chiave segreta di Rossi?

4. Bianchi ha chiavi pubbliche il primo $p' = 59$, la classe primitiva $\bar{g}' = \bar{2}$ e il numero $E' = 5$. Rossi gli risponde con le due stringhe

$$(f_1, f_2) = (\overline{12}, \overline{16}) \qquad (r_1, r_2) = (\overline{12}, \overline{6}).$$

   (a) La spia è riuscita però a ricostruire anche la chiave segreta di Bianchi D'. Qual è?
   (b) Cosa gli ha risposto Rossi?
   (c) Riusciamo a ricostruire la risposta di Rossi anche senza sapere la chiave segreta di Bianchi?

5. Il signor Rossi desidera ricevere messaggi criptati e decide di adottare il criptosistema RSA. La ditta gli fornisce un kit con chiavi pubbliche N ed E e chiave segreta D.
   (a) Vanno bene $N = 91$, $E = 5$ e $D = 29$??
   (b) Preparare un kit di N', E' e D' per il signor Bianchi.