Ime i prezime: _____

1	2	3	4	Σ

Eliptičke krivulje u kriptografiji -

Završni ispit, 13. 06. 2014.

1. Neka je $E/\mathbb{Q}$ eliptička krivulja zadana s

$$E : y^2 = x^3 + 37x + 36.$$

   Odredite $E(\mathbb{Q})_{tors}$.

2. Odredite rang eliptičke krivulje $y^2 = x^3 - 11x$ nad $\mathbb{Q}$.

3. Neka je E eliptička krivulja $y^2 = x^3 + x + 1$ nad $\mathbb{F}_{59}$. Grupa $E(\mathbb{F}_{59})$ ima red 63 i generirana je elementom $P = (0, 1)$. Rješite problem diskretnog logaritma $mP = (38, 49)$ BSGS metodom.

4. Faktorizirajte broj 851 korištenjem eliptičke krivulje $E : y^2 = x^3 + 3$, točke $P = (1, 2)$ na njoj i ograde $B = 3$.

Tablica inverza u $\mathbb{F}_{59}^{\times}$; u ptvom, trećem i petom redu su elementi iz $\mathbb{F}_{59}^{\times}$, ispod svakog od njih je njegov inverz.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
30	20	15	12	10	17	37	46	6	43	5	50	38	4	48	7	23	28	3
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
45	51	18	32	26	25	35	19	57	2	40	24	34	33	27	41	8	14	56
40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
31	36	52	11	55	21	9	54	16	53	13	22	42	49	47	44	39	29	58