Eliptičke krivulje u kriptografiji

završni ispit - grupa A

8.6.2015.

1. Eliptička krivulja E nad poljem $\mathbb{F}_{17}$ zadana je jednadžbom $y^2 = x^3 + 7x + 4$. Dokažite da je $\alpha = (0, 2)$ generator grupe $E(\mathbb{F}_{17})$.

2. Pomoću Menezes-Vanstoneovog kriptosustava u kojem su javni ključ eliptička krivulja E i generator α iz 1. zadatka, te $\beta = (16, 8)$, šifrirajte otvoreni tekst $(x_1, x_2) = (5, 11)$, uz pretpostavku da je jednokratni ključ $k = 6$.

3. Eliptička krivulja E nad poljem $\mathbb{F}_{13}$ zadana je jednažbom $y^2 = x^3 + 10x + 9$. Za točke $P = (0, 3)$ i $Q = (3, 12)$ na E riješite problem eliptičkog diskretnog logaritma $Q = [m]P$ Pohlig-Hellmanovim algoritmom ako je poznato da je točka P reda 15.

4. Faktorizirajte broj $n = 391$ pomoću ECM faktorizacije s parametrima

$$E: \quad y^2 = x^3 + 8x + 1,$$

$P = (0, 1)$ i $B = 3$.

Dozvoljeno je korištenje džepnog kalkulatora, te dva papira s formulama.
Kalkulatori se mogu koristiti za standardne operacije, ali nije dozvoljeno korištenje gotovih funkcija za algoritme iz eliptičkih krivulja i teorije brojeva.

Rezultati: utorak, 16.6.2015. u 14 sati.

Andrej Dujella