Eliptičke krivulje u kriptografiji

završni ispit - grupa A

4.6.2019.

1. Eliptička krivulja E nad poljem $\mathbb{F}_{19}$ zadana je jednadžbom $y^2 = x^3 + 2$. Dokažite da je $\alpha = (4, 3)$ generator grupe $E(\mathbb{F}_{19})$.

2. Pomoću Menezes-Vanstoneovog kriptosustava u kojem su javni ključ eliptička krivulja E i generator α iz 1. zadatka, te $\beta = (8, 18)$, šifrirajte otvoreni tekst $(x_1, x_2) = (7, 9)$, uz pretpostavku da je jednokratni ključ $k = 7$.

3. Eliptička krivulja E nad poljem $\mathbb{F}_{19}$ zadana je jednažbom $y^2 = x^3 + x + 5$. Za točke $P = (12, 4)$ i $Q = (4, 15)$ 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 $n = 1079$ pomoću ECM faktorizacije s parametrima

$$E: \quad y^2 = x^3 + 10x + 9,$$

$P = (0, 3)$ 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: ponedjeljak, 10.6.2019. u 14 sati. Andrej Dujella