Eliptičke krivulje u kriptografiji

završni ispit - grupa A

10.6.2025.

1. Eliptička krivulja E nad poljem $\mathbb{F}_{17}$ zadana je jednadžbom $y^2 = x^3 + 7x + 4$. Odredite red grupe $E(\mathbb{F}_{17})$. 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 $\beta = (15, 13)$, šifrirajte otvoreni tekst $(x_1, x_2) = (7, 11)$, uz pretpostavku da je jednokratni ključ $k = 8$.

3. Eliptička krivulja E nad poljem $\mathbb{F}_{19}$ zadana je jednažbom $y^2 = x^3 + 8x + 12$. Za točke $P = (2, 6)$ i $Q = (17, 8)$ na E riješite problem eliptičkog diskretnog logaritma $Q = [m]P$ Pohlig-Hellmanovim algoritmom ako je poznato da je točka P reda 15.

4. Dokažite da je broj $n = 251$ prost koristeći metodu dokazivanja prostosti pomoću eliptičkih krivulja. Možete koristiti eliptičku krivulju

$$E: \quad y^2 = x^3 + 9x - 1,$$

   točku P na E s prvom koordinatom jednakom 1, te činjenicu da je $|E_{251}| = 259 = 37 \cdot 7$.

5. Faktorizirajte broj $n = 319$ pomoću ECM faktorizacije s parametrima

$$E: \quad y^2 = x^3 + 9x + 4,$$

   $P = (0, 2)$ 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.

Andrej Dujella