

# Eliptičke krivulje u kriptografiji

završni ispit

17.6.2021.

1. Eliptička krivulja  $E$  nad poljem  $\mathbb{F}_{17}$  zadana je jednažbom  $y^2 = x^3 + 7x + 4$ . Odredite red grupe  $E(\mathbb{F}_{17})$ . Dokažite da je  $\alpha = (3, 1)$  generator grupe  $E(\mathbb{F}_{17})$ .
2. Pomoću Menezes-Vanstoneovog kriptosustava u kojem su javni ključ eliptička krivulja  $E$  i generator  $\alpha$  iz 1. zadatka, te  $\beta = (16, 9)$ , 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  $y^2 = x^3 + 12x + 12$ . Za točke  $P = (2, 5)$  i  $Q = (14, 6)$  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  $n = 341$  pomoću ECM faktorizacije s parametrima

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

$$P = (0, 2) \text{ i } B = 3.$$

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