

# Eliptičke krivulje u kriptografiji

završni ispit - grupa A

24.5.2013.

1. Eliptička krivulja  $E$  nad poljem  $\mathbb{F}_{13}$  zadana je jednažbom  $y^2 = x^3 + 2x + 4$ . Dokažite da je  $\alpha = (0, 2)$  generator grupe  $E(\mathbb{F}_{13})$ .
2. Pomoću Menezes-Vanstoneovog kriptosustava u kojem su javni ključ eliptička krivulja  $E$  i generator  $\alpha$  iz 1. zadatka, te  $\beta = (9, 7)$ , šifrirajte otvoreni tekst  $(x_1, x_2) = (7, 10)$ , uz pretpostavku da je jednokratni ključ  $k = 6$ .
3. Eliptička krivulja  $E$  nad poljem  $\mathbb{F}_{11}$  zadana je jednažbom  $y^2 = x^3 + 7x + 1$ . Za točke  $P = (0, 1)$  i  $Q = (3, 7)$  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  $n = 247$  pomoću ECM faktorizacije s parametrima

$$E : y^2 = x^3 + 7x + 4,$$

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

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.

Rezultati: ponedjeljak, 3.6.2013. u 11 sati.

Andrej Dujella