1	2	3	4	5	6	Σ

Ime i Prezime

1. (10) Alice je poslala istu poruku m nekolicini agenata. Eva je presrela šifrate c_1, c_2, c_3 za trojicu agenata čiji su javni ključevi n_1, n_2 i n_3. Poznato je da Alice i agenti koriste RSA kriptosustav s javnim eksponentom $e = 3$. Za zadane

$$\begin{aligned} n_1 &= 217, & c_1 &= 153, \\ n_2 &= 299, & c_2 &= 226, \\ n_3 &= 319, & c_3 &= 298. \end{aligned}$$

pokažite kako će Eva otkriti poruku m (bez poznavanja faktorizacije modula n_1, n_2, n_3).

2. (10) Konačno polje $GF(2^3)$ realizirano je skupom $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$ uz operacije zbrajanja i množenja polinoma u $\mathbb{Z}_2[x]$ modulo polinom $f(x) = x^3 + x + 1$.

   (a) Provjerite da je polinom $g(x) = x + x^2$ generator multiplikativne grupe $GF(2^3)^*$.

   (b) Zadan je ElGamalov kriptosustav u $GF(2^3)^*$ s parametrima

   $$\alpha = g(x) = x + x^2, \ a = 3, \ \beta = \alpha^a.$$

   Dešifrirajte šifrat $(y_1, y_2) = (1 + x + x^2, x^2)$.

3. (8) U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (2\,773, 47, 59),$$

dešifrirajte šifrat $y = 2729$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

4. (6) Ispitajte je li 133

   a) Eulerov pseudoprosti broj u bazi 11,

   b) jaki pseudoprosti broj u bazi 11.

5. (6) Neka je $n = 137\,833 = p \cdot q$ gdje su p i q prosti brojevi. Uz pretpostavku da su sve potencije prostih brojeva koje dijele $p - 1$ manje ili jednake $B = 7$, odredite faktorizaciju broja n pomoću Pollardove $p - 1$ metode.

Dozvoljeno je korištenje džepnog kalkulatora, te papir s formulama.
Kalkulatori se mogu koristiti za standardne operacije, ali nije dozvoljeno korištenje gotovih funkcija za modularno potenciranje, modularni inverz, rješavanje linearnih kongruencija i sustava linearnih kongruencija, faktorizaciju i sl.

Rezultati/ uvidi / upis ocjena: ponedjeljak, 27.1.2020. u 14-15.30 sati.

Zrinka Franušić

1	2	3	4	5	6	Σ

____

Ime i Prezime

1. (10) Alice je poslala istu poruku m nekolicini agenata. Eva je presrela šifrate c_1, c_2, c_3 za trojicu agenata čiji su javni ključevi n_1, n_2 i n_3. Poznato je da Alice i agenti koriste RSA kriptosustav s javnim eksponentom $e = 3$. Za zadane

$$\begin{aligned} n_1 &= 161, & c_1 &= 57, \\ n_2 &= 247, & c_2 &= 96, \\ n_3 &= 493, & c_3 &= 272. \end{aligned}$$

pokažite kako će Eva otkriti poruku m (bez poznavanja faktorizacije modula n_1, n_2, n_3).

2. (10) Konačno polje $GF(2^3)$ realizirano je skupom $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$ uz operacije zbrajanja i množenja polinoma u $\mathbb{Z}_2[x]$ modulo polinom $f(x) = x^3 + x + 1$.

   (a) Provjerite da je polinom $g(x) = 1 + x^2$ generator multiplikativne grupe $GF(2^3)^*$.

   (b) Zadan je ElGamalov kriptosustav u $GF(2^3)^*$ s parametrima

   $$\alpha = g(x) = 1 + x^2, \ a = 4, \ \beta = \alpha^a.$$

   Dešifrirajte šifrat $(y_1, y_2) = (x + x^2, x + x^2)$.

3. (8) U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (2\,021, 43, 47),$$

dešifrirajte šifrat $y = 917$. Poznato je da je otvoreni tekst prirodan broj $x < n$ kojem su zadnja četiri bita u binarnom zapisu međusobno jednaka.

4. (6) Ispitajte je li 217

   a) Eulerov pseudoprosti broj u bazi 7,

   b) jaki pseudoprosti broj u bazi 7.

5. (6) Neka je $n = 128\,417 = p \cdot q$ gdje su p i q prosti brojevi. Uz pretpostavku da su sve potencije prostih brojeva koje dijele $p - 1$ manje ili jednake $B = 7$, odredite faktorizaciju broja n pomoću Pollardove $p - 1$ metode.

Dozvoljeno je korištenje džepnog kalkulatora, te papir s formulama.
Kalkulatori se mogu koristiti za standardne operacije, ali nije dozvoljeno korištenje gotovih funkcija za modularno potenciranje, modularni inverz, rješavanje linearnih kongruencija i sustava linearnih kongruencija, faktorizaciju i sl.

Rezultati/ uvidi / upis ocjena: ponedjeljak, 27.1.2020. u 14-15.30 sati.

Zrinka Franušić