Zadaci za vežbu - rešenja

Zadatak 1 *Odrediti sve generatore* $\mathbb{Z}/n\mathbb{Z}^*$ *za* $n = 11$.

Rešenje:

n	0	1	2	3	4	5	6	7	8	9	10
$2^n (mod\ 11)$	1	2	4	8	5	10	9	7	3	6	1

Znamo da je jedan generator ovde grupe broj 2 pa je svaka vrednost oblika 2^k takođe generator ako važi da je $NZD(k, 10) = 1$. Brojevi koji su uzajamno prosti sa 11 pripadaju skupu:

$$\{1, 3, 7, 9\}.$$

Na osnovu tog skupa dobijamo i generatore:

$$\{2, 8, 7, 6\}.$$

Zadatak 2 *Odrediti* x *ako važi* $8^x \equiv 15(mod\ 11)$

Rešenje:

$$\begin{aligned}
&8^x \equiv 15(mod\ 11)\\
&8^x \equiv 4(mod\ 11)\\
&2^{3x} \equiv 2^2(mod\ 11)\\
&2^{3x-2} \equiv 1(mod\ 11)\\
&2^{3x-2} \equiv 2^{10}(mod\ 11)\\
&3x - 2 \equiv 10k
\end{aligned}$$

Da bismo lakše proverili da li 10 deli $3k - 2$, računamo $NZD(2, 10) = 2$. Broj x možemo zapisati kao $2z, z \in \mathbb{N}$ i dobijamo:

$$\begin{aligned}
&6z - 2 = 10k\\
&3z - 2 = 5k
\end{aligned}$$

Sada ostaje da proverimo da li 5 deli $3z - 2$. Ovaj izraz možemo transformisati dodavanjem -5 (neće promeniti deljivost celog izraza jer je -5 deljivo brojem 5):

$$3z - 1 = 3z - 6 = 3(z - 2)$$

Da bi $3(z - 2)$ bilo deljivo brojem 5, $z - 2$ mora biti deljivo brojem 5, odnosno, broj z mora biti oblika $5k + 2$. Odatle dobijamo rešenje jednačine:

$$x = 10k + 4, k \in \mathbb{Z}$$

Zadatak 3 *Pomoću Euklidovog algoritma odrediti* $(x^3+x^2)^{-1}$ *u polju* $\mathbb{F}_2[x]/(x^5+x^2+1)$.

Rešenje: Prvo ćemo odrediti NZD ovih polinoma:

$$x^5+x^2+1=(x^2+x+1)\cdot(x^3+x^2)+\underline{1}$$

Zatim, određujemo linearnu kombinaciju polinoma koja daje vrednost njihovog NZD-a:

$$1=x^5+x^2+1+(x^2+x+1)\cdot(x^3+x^2)$$

Iz linearne kombinacije dobijamo da je $(x^3+x^2)^{-1}=x^2+x+1$ u polju $\mathbb{F}_2[x]/(x^5+x^2+1)$.

Zadatak 4 *Šifrovati otvoreni tekst "kG" algoritmom SAES, ako je ključ "Ma".*

Rešenje: Ključ ćemo zapisati u binarnom obliku: 01010001 01100101. Na osnovu ključa određujemo:

$$W[0]=0100\ 1101$$
$$W[1]=0110\ 0001$$

Da bismo odredili $W[2]$ potrebno je da odredimo vrednost $RCON[1]=RC[1]0000$:

$$RC[1]=x^3=1000$$
$$RCON[1]=1000\ 0000$$

Zatim, računamo $SubNib(RotNib(W[i-1])$:

$$SubNib(RotNib(W[1])=SubNib(RotNib(0110\ 0001))=0100\ 1000$$

Sada treba sabrati dobijenu vrednost sa $W[0]$ i $RCON[1]$ po modulu dva, bit po bit:

$$\begin{aligned}W[2]&=W[0]\oplus RCON[1]\oplus SubNib(RotNib(W[1])\\&=0100\ 1101\oplus 1000\ 0000\oplus 0100\ 1000\\&=1000\ 0101\end{aligned}$$

Sledeća vrednost koju računamo jeste $W[3]$:

$$\begin{aligned}W[3]&=W[1]\oplus W[2]\\&=0110\ 0001\oplus 1000\ 0101\\&=1110\ 0100\end{aligned}$$

Za $W[4]$ potrebno je odrediti $RCON[2]$ i $SubNib(RotNib(W[3])$:

$$RC[2]=x^4=x+1=0011$$
$$RCON[2]=0011\ 0000$$
$$SubNib(RotNib(W[3])=1101\ 1111$$

Sada možemo izračunati $W[4]$:

$$\begin{aligned}W[4]&=W[2]\oplus RCON[2]\oplus SubNib(RotNib(W[3])\\&=1000\ 0101\oplus 0011\ 0000\oplus 1101\ 1111\\&=0110\ 1010\end{aligned}$$

Na kraju ostaje $W[5]$:

$$\begin{aligned} W[5] &= W[3] \oplus W[4] \\ &= 1110\ 0100 \oplus 0110\ 1010 \\ &= 1000\ 1110 \end{aligned}$$

Prošireni ključ je $W_0W_1W_2W_3W_4W_5$ odnosno:

$$0100\ 1101\ 0110\ 0001\ 1000\ 0101\ 1110\ 01000110\ 1010\ 1000\ 1110$$

Sledeći korak je zapis otvorenog teksta:

$$OT = [0110\ 1011\ 0100\ 0111]$$

Sada treba primeniti kompoziciju funkcija počevši od A_{K_0}:

$$\begin{array}{|c|c|} \hline 0110 & 0100 \\ \hline 1011 & 0111 \\ \hline \end{array} \xrightarrow{A_{K_0}} \begin{array}{|r|c|} \hline 0110 & 0100 \\ \oplus\ 0100 & 0110 \\ \hline 1011 & 0111 \\ \oplus\ 1101 & 0001 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 0010 & 0010 \\ \hline 0110 & 0110 \\ \hline \end{array} \xrightarrow{NS} \begin{array}{|c|c|} \hline 1010 & 1010 \\ \hline 1000 & 1000 \\ \hline \end{array} \xrightarrow{SR} \begin{array}{|c|c|} \hline 1010 & 1010 \\ \hline 1000 & 1000 \\ \hline \end{array}$$

$$\xrightarrow{MC} \begin{array}{|c|c|} \hline 1100 & 1100 \\ \hline 0110 & 0110 \\ \hline \end{array} \xrightarrow{A_{K_1}} \begin{array}{|r|c|} \hline 1100 & 1100 \\ \oplus\ 1000 & 1110 \\ \hline 0110 & 0110 \\ \oplus\ 0101 & 0100 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 0010 & 0010 \\ \hline 0011 & 0010 \\ \hline \end{array} \xrightarrow{NS} \begin{array}{|c|c|} \hline 1101 & 1010 \\ \hline 1011 & 1010 \\ \hline \end{array}$$

$$\xrightarrow{SR} \begin{array}{|c|c|} \hline 1101 & 1010 \\ \hline 1010 & 1011 \\ \hline \end{array} \xrightarrow{A_{K_2}} \begin{array}{|r|c|} \hline 1101 & 1010 \\ \oplus\ 0110 & 1000 \\ \hline 1010 & 1011 \\ \oplus\ 1010 & 1110 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 1011 & 0010 \\ \hline 0000 & 0101 \\ \hline \end{array}$$

Primenom algoritma dobili smo šifrat 1011 0000 0010 0101.

Zadatak 5 *Dešifrovati šifrat 1011 0000 0010 0101 algoritmom SAES, ako je ključ "Ma".*

Rešenje: Prvi korak je proširivanje ključa, što je već učinjeno u prethodnom zadatku.
Sada treba primeniti kompoziciju inverznih funkcija počevši od A_{K_2}:

$$\begin{array}{|c|c|} \hline 1011 & 0010 \\ \hline 0000 & 0101 \\ \hline \end{array} \xrightarrow{A_{K_2}} \begin{array}{|r|c|} \hline 1011 & 0010 \\ \oplus\ 0110 & 1000 \\ \hline 0000 & 0101 \\ \oplus\ 1010 & 1110 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 1101 & 1010 \\ \hline 1010 & 1011 \\ \hline \end{array} \xrightarrow{SR} \begin{array}{|c|c|} \hline 1101 & 1010 \\ \hline 1011 & 1010 \\ \hline \end{array} \xrightarrow{NS^{-1}} \begin{array}{|c|c|} \hline 0010 & 0010 \\ \hline 0011 & 0010 \\ \hline \end{array}$$

$$\xrightarrow{A_{K_1}} \begin{array}{|r|c|} \hline 0100 & 0010 \\ \oplus\ 1000 & 1110 \\ \hline 0011 & 0010 \\ \oplus\ 0101 & 0100 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 1100 & 1100 \\ \hline 0110 & 0110 \\ \hline \end{array} \xrightarrow{MC^{-1}} \begin{array}{|c|c|} \hline 1010 & 1010 \\ \hline 1000 & 1000 \\ \hline \end{array} \xrightarrow{SR} \begin{array}{|c|c|} \hline 1010 & 1010 \\ \hline 1000 & 1000 \\ \hline \end{array}$$

$$\xrightarrow{NS^{-1}} \begin{array}{|c|c|} \hline 0010 & 0010 \\ \hline 0110 & 0110 \\ \hline \end{array} \xrightarrow{A_{K_0}} \begin{array}{|r|c|} \hline 0010 & 0010 \\ \oplus\ 0100 & 0110 \\ \hline 0110 & 0110 \\ \oplus\ 1101 & 0001 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 0110 & 0100 \\ \hline 1011 & 0111 \\ \hline \end{array}$$

Primenom algoritma dobili smo otvoreni tekst 01101011 01000111, odnosno "Ok".

Zadatak 6 *Prikazati postupak Massey-Omura razmene ključeva za* $q = 809$, $K = 97$, $e_A = 325$, $e_B = 517$.

Rešenje: Osoba A određuje svoj privatni ključ[1] d_A:

$$d_A = e_A^{-1}(mod\ q-1) = 325^{-1}(mod\ 808) = 629$$

Osoba B određuje svoj privatni ključ d_B:

$$d_B = e_B^{-1}(mod\ q-1) = 517^{-1}(mod\ 808) = 261$$

Osoba A računa K^{e_A} i to šalje osobi B:

$$K^{e_A} = 97^{325}(mod\ 809) = 97^{256} \cdot 97^{64} \cdot 97^4 \cdot 97^1(mod\ 677) = 560(mod\ 809)$$

Osoba B dobijeni broj stepenuje na e_B, i vraća novu vrednost osobi A:

$$K^{e_A e_B} = 560^{517}(mod\ 809) = 560^{512} \cdot 560^4 \cdot 560^1(mod\ 809) = 638(mod\ 809)$$

Sada osoba A stepenuje dobijeni broj na d_A i vraća vrednost osobi B:

$$K^{e_A e_B d_A} = 638^{629}(mod\ 809) = 638^{512} \cdot 638^{64} \cdot 638^{32} \cdot 638^{16} \cdot 638^4 \cdot 638^1(mod\ 809) = 648(mod\ 809)$$

Na kraju, osoba B stepenuje dobijeni broj na d_B čime dobija ključ K:

$$K^{e_A e_B d_A d_B} = 648^{261}(mod\ 809) = 648^{256} \cdot 648^4 \cdot 648^1(mod\ 809) = 97(mod\ 809)$$

Zadatak 7 *Prikazati razmenu poruka u sistemu RSA ako je* $n = 703$, $e = 611$, $M = 77$.

Rešenje: Da bi osoba A poslala poruku M osobi B, potrebno je da iskoristi javni ključ osobe B i odredi $M^e(mod\ n)$. Vrednost se može odrediti algoritmom stepenovanje kvradriranjem.

$$77^{611}(mod\ 703) = 77^{512} \cdot 77^{64} \cdot 77^{32} \cdot 77^2 \cdot 77^1 = 210(mod\ 703)$$

Osoba A šalje 210 osobi B. Da bi osoba B dešifrovala poruku potrebno je da izračuna $M^d(mod\ n)$. Odredimo prvo tajni ključ d:

$$\varphi(703) = \varphi(19) \cdot \varphi(37) = 18 \cdot 36 = 648$$
$$d = e^{-1}(mod\ \varphi(n)) = 611^{-1}(mod\ 648) = 35(mod\ 648)$$

Sada možemo da dešifujemo poruku:

$$210^{35}(mod\ 703) = 210^{32} \cdot 210^2 \cdot 210^1(mod\ 703)$$
$$210^2 \equiv 514$$
$$210^{32} \equiv (210^2)^{16} \equiv ((514^2)^8 \equiv (571^2)^4 \equiv (552^2)^2 \equiv 305^2 \equiv 229$$
$$210^{35}(mod\ 703) = 229 \cdot 514 \cdot 210 = 77(mod\ 703)$$

[1] Napomena: Rešenja su data bez međuračuna.

Zadatak 8 *Za eliptičku krivu $E : y^2 = x^3 + x + 4$ nad poljem F_{11} pokazati da je tačka $G = (2, 5)$ generator i napraviti tabelu umnožaka te tačke.*

Rešenje: Prvo je potrebno odrediti skup tačaka ove krive[2]:

$$\{\varnothing, (0,2), (0,9), (2,5), (2,6), (3,1), (3,10), (9,4), (9,7)\}$$

Kako bismo pokazali da je tačka $G = (2, 5)$ generator, potrebno je da odredimo tačke $nG, \forall n \in [2, 8]$ (jer u skupu ima 9 tačaka). Za $n = 0$ dobijamo $\varnothing$, a za $n = 1$ je početna tačka $(2, 5)$.

- $2G = (x_g, y_g) = G + G$

$$k = \frac{3 \cdot 4 + 1}{2 \cdot 5} = 13 \cdot 10^{-1} = -13 = 9$$
$$n = 5 - 9 \cdot 2 = -13 = 9$$

  Jednačina tangete koja prolazi kroz tačku G je $y = 9x + 9$.

$$x_g = 9^2 - 2 \cdot 2 = 4 - 4 = 0$$
$$y_g = 9 \cdot 0 + 9 = 9$$
$$2G = (0, -9) = (0, 2)$$

- $3G = (x_g, y_g) = 2G + G$

$$k = \frac{5 - 2}{2 - 0} = 3 \cdot 2^{-1} = 3 \cdot 6 = 7$$
$$n = 2 - 0 \cdot 7 = 2$$

  Jednačina prave koja prolazi kroz tačke G i $2G$ je $y = 7x + 2$.

$$x_g = 7^2 - 0 - 2 = 3$$
$$y_g = 7 \cdot 3 + 2 = 1$$
$$3G = (3, -1) = (3, 10)$$

- $4G = (x_g, y_g) = 3G + G$

$$k = \frac{10 - 5}{3 \cdot 2} = 5$$
$$n = 10 - 5 \cdot 3 = -5 = 6$$

  Jednačina prave koja prolazi kroz tačke $3G$ i G je $y = 5x + 5$.

$$x_g = 5^2 - 3 - 2 = 9$$
$$y_g = 5 \cdot 9 + 6 = 7$$
$$4G = (9, -7) = (9, 4)$$

- $5G = (x_g, y_g) = 4G + G$

$$k = \frac{5 - 4}{2 - 9} = 4^{-1} = 3$$
$$n = 5 - 3 \cdot 2 = 10$$
$$x_g = 3^2 - 9 - 2 = -2 = 9$$
$$y_g = 3 \cdot 9 + 10 = 4$$
$$5G = (9, -4) = (9, 7)$$

[2] Odrediti ovaj skup za vežbu.

- $6G = (x_g, y_g) = 5G + G$

$$k = \frac{7-5}{9-2} = 5$$
$$n = 7 - 5 \cdot 9 = 6$$
$$x_g = 5^2 - 9 - 2 = 3$$
$$y_g = 5 \cdot 3 + 6 = 10$$
$$6G = (3, -10) = (3, 1)$$

- $7G = (x_g, y_g) = 6G + G$

$$k = \frac{1-5}{3-2} = -4 = 7$$
$$n = 1 - 7 \cdot 3 = -20 = 2$$
$$x_g = 7^2 - 3 - 2 = 0$$
$$y_g = 7 \cdot 0 + 2 = 2$$
$$7G = (0, -2) = (0, 9)$$

- $8G = (x_g, y_g) = 7G + G$

$$k = \frac{5-9}{2-0} = -2 = 9$$
$$n = 9 - 9 \cdot 0 = 9$$
$$x_g = 9^2 - 2 - 0 = 2$$
$$y_g = 9 \cdot 2 + 9 = 5$$
$$8G = (2, -5) = (2, 6)$$

Dobili smo sve tačke iz skupa pa zaključujemo da tačka $G = (2, 5)$ jeste generator. Ostaje još da napravimo tabelu umnožaka:

n	0	1	2	3	4	5	6	7	8
nG	∅	(2,5)	(0, 2)	(3, 10)	(9, 4)	(9,7)	(3, 1)	(0, 9)	(2, 6)

Zadatak 9 *Eliptička kriva koja se koristi za problem usaglašavanja ključeva Diffie-Helman protokola je* $E : y^2 = x^3 + x + 4$ *nad poljem* $\mathbb{F}_{11}$*. Ako se koristi generator* $G = (9, 4)$*, tajni ključevi* $e_A = 5$*,* $e_B = 9$*, odrediti tačku koja se dobija kao rezultat usaglašavanja.*

Rešenje: Javni podaci su $G = (9, 4)$ i $n = 13$. Radi lakšeg računa G ćemo predstaviti kao $4(2, 5)$ i koristićemo tabelu umnožaka koju smo napravili u prethodnom zadatku.

Osoba A generiše svoj javni ključ G^{e_A}:

$$G^{e_A} = e_A \cdot G = 5 \cdot 4(2, 5) = 20(2, 5) = 2(2, 5) = (0, 2)$$

Osoba B generiše svoj javni ključ G^{e_B}:

$$G^{e_B} = e_B \cdot G = 8 \cdot 4(2, 5) = 32(2, 5) = 5(2, 5) = (9, 7)$$

Kako bi se usaglasili, osoba A računa $(G^{e_B})^{e_A}$, a osoba B računa $(G^{e_A})^{e_B}$:

$$(G^{e_B})^{e_A} = 5 \cdot (9, 7) = 25(2, 5) = 7(2, 5) = (0, 9)$$
$$(G^{e_A})^{e_B} = 8 \cdot (0, 2) = 16(2, 5) = 7(2, 5) = (0, 9)$$

Zadatak 10 *Za sistem El Gamal koristi se eliptička kriva $E : y^2 = y^2 = x^3 + x + 4$ nad poljem $\mathbb{F}_{11}$. Generator je $G = (2, 6)$. Ako su tajni ključevi $e_A = 3$ i $e_B = 7$, prikazati postupak šifrovanja poruke $M = (9, 7)$ (koristi se slučajan broj $k = 5$), a zatim postupak dešifrovanja šifrata.*

Rešenje: Javni parametri su $G = (2, 6) = 8(2, 5)$ i $n = 13$. Osobe A i B generišu svoje javne ključeve:

$$G^{e_A} = e_A \cdot G = 3(2, 6) = 24(2, 5) = 6(2, 5) = (3, 1)$$
$$G^{e_B} = e_B \cdot G = 7(2, 6) = 56(2, 5) = 2(2, 5) = (0, 2)$$

Osoba A određuje vrednost maskirajućeg ključa G^k:

$$G^k = k \cdot G = 5(2, 6) = 40(2, 5) = 4(2, 5) = (9, 4)$$

Zatim, osoba A šifruje poruku M pomoću maskirajućeg ključa i javnog ključa učesnika B:

$$G^{e_B k} = 5G^{e_B} = 5(0, 2) = 10(25, 5) = (2, 5)$$
$$MG^{e_B k} = (9, 7) + (2, 5) = 5(2, 5) + (2, 5) = (3, 1)$$

Osoba A šalje osobi B par $(MG^{e_B k}, G^k)$. Da bi osoba B dešifrovala poruku, prvo mora izračunati $G^{e_B k}$, a zatim $(G^{e_B k})^{-1}$. Dobijene vrednost primenjuje u formuli $MG^{e_B k}(G^{e_B k})^{-1}$ čime dobija M.

$$G^{e_B k} = 7G^k = 7(9, 4) = 28(2, 5) = (2, 5)$$
$$(G^{e_B k})^{-1} = -(2, 5) = (2, 6)$$
$$MG^{e_B k}(G^{e_B k})^{-1} = (3, 1) + (2, 6) = 14(2, 5) = 5(2, 5) = (9, 7)$$

Zadatak 11 *Korisnik A ima javni ključ $e = 11$, $n = 899$. Kako glasi njegov RSA digitalni potpis poruke 876?*

Rešenje:

$$\begin{aligned}
\varphi(899) &= \varphi(29) \cdot \varphi(31) = 840 \\
d &= 11^{-1}(mod\ 840) = 229(mod\ 611) \\
M^d &= 876^{611}(mod\ 899) = 876^{512} \cdot 876^{64} \cdot 876^{32} \cdot 876^2 \cdot 876(mod\ 899) \\
&\quad 876^2 \equiv 529 \\
&\quad 876^{32} \equiv (876^2)^{16} \equiv (529^2)^8 \equiv (252^2)^4 \equiv (574^2)^2 \equiv 442^2 \equiv 281 \\
&\quad 876^{64} \equiv (876^{32})^2 \equiv 28^2 \equiv 748 \\
&\quad 876^{512} \equiv (876^{64})^8 \equiv (748^2)^4 \equiv (326^2)^2 \equiv 194^2 \equiv 777 \\
M^d &= 876^{512} \cdot 876^{64} \cdot 876^{32} \cdot 876^2 \cdot 876(mod\ 899) \\
&= 777 \cdot 748 \cdot 281 \cdot 529 \cdot 876(mod\ 899) = 225
\end{aligned}$$