Diskretna matematika 2

Zadaća 11

March 22, 2025

Borna Gojšić

---

1. U RSA kriptosustavu s javnim ključem (n, e), gdje je $n = 86267 = 281 \cdot 307$ i $e = 65537$, šifrirajte otvoreni tekst $x = 1245$. Odredite pripadni tajni ključ d.

Rj: Znamo da je $1245 = 3 \cdot 5 \cdot 83$. Dakle, imamo

$$\begin{aligned}
1245^e &\equiv 1245^{65537} \equiv 1245^{2^{16}} \cdot 1245 \equiv (-2781)^{2^{15}} \cdot 1245 \pmod{n} \\
&\equiv (-30069)^{2^{14}} \cdot 1245 \equiv (-19666)^{2^{13}} \cdot 1245 \equiv (16595)^{2^{12}} \cdot 1245 \pmod{n} \\
&\equiv (29761)^{2^{11}} \cdot 1245 \equiv (13832)^{2^{10}} \cdot 1245 \equiv (-15982)^{2^9} \cdot 1245 \pmod{n} \\
&\equiv (-12263)^{2^8} \cdot 1245 \equiv (17788)^{2^7} \cdot 1245 \equiv (-14412)^{2^6} \cdot 1245 \pmod{n} \\
&\equiv (-25192)^{2^5} \cdot 1245 \equiv 56812^{2^4} \cdot 1245 \equiv 9806^{2^3} \cdot 1245 \pmod{n} \\
&\equiv 56198^{2^2} \cdot 1245 \equiv (-19666)^2 \cdot 1245 \equiv 16595 \cdot 1245 \equiv 42962 \pmod{n}.
\end{aligned}$$

Dakle, šifrat je $y = 42962$. Znamo da je $\varphi(n) = (p-1)(q-1) = 280 \cdot 306 = 2^3 \cdot 5 \cdot 7 \cdot 2 \cdot 3^2 \cdot 17 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 = 85680$. Dakle, imamo

$$65537d \equiv 1 \pmod{85680} \Rightarrow 65537d = 85680k + 1 \Rightarrow 65537d - 85680k = 1.$$

Dakle, ovu kongruenciju možemo riješiti proširenim Euklidovim algoritmom.

x	y	g	u	v	w	$\left\lfloor \frac{g}{w} \right\rfloor$
1	0	85680	0	1	65537	1
0	1	65537	1	-1	20143	3
1	-1	20143	-3	4	5108	3
-3	4	5108	10	-13	4819	1
10	-13	4819	-13	17	289	16
-13	17	289	218	-285	195	1
218	-285	195	-231	302	94	2
-231	302	94	680	-889	7	13
680	-889	7	-9071	11859	3	2
-9071	11859	3	18822	-24607	1	3
18822	-24607	1			0	

Dakle, $85680 \cdot (18822) + 65537 \cdot (-24607) = 1$ pa je $d \equiv -24607 \equiv 61073 \pmod{85680}$.

2. U nekoj banci se za šifriranje troznamenkastih PIN-ova koristi RSA kriptosustav s javnim ključem (n, e), gdje je $n = 1411 = 17 \cdot 83$ i $e = 835$. Koji PIN ima Alice ako je šifrat njezinog PIN-a 002?

Rj: Budući da je $n = 17 \cdot 83 = 1411$, imamo $\varphi(n) = (17-1)(83-1) = 16 \cdot 82 = 1312$. Dakle, tražimo d takav da vrijedi $835d \equiv 1 \pmod{1312}$, tj. $835d - 1312k = 1$.

x	y	g	u	v	w	$\lfloor \frac{g}{w} \rfloor$
1	0	1312	0	1	835	1
0	1	835	1	-1	477	1
1	-1	477	-1	2	358	1
-1	2	358	2	-3	119	3
2	-3	119	-7	11	1	119
-7	11	1			0	

Dakle, $1312 \cdot (-7) + 835 \cdot (11) = 1$ pa je $d = 11$. Dakle, $002^{11} \equiv 2^{11} \equiv 2048 \equiv 637 \pmod{1411}$.

3. 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).

Rj: Imamo sustav kongruencija:

$$x = m^3 \equiv 153 \pmod{217}, \quad x = m^3 \equiv 226 \pmod{299}, \quad x = m^3 \equiv 298 \pmod{319}.$$

Dakle, imamo $M = 217 \cdot 299 \cdot 319 = 20697677$ i $x_0 = 299 \cdot 319 x_1 + 217 \cdot 319 x_2 + 217 \cdot 299 x_3$.
Sada rješavamo kongruencije:

$$\begin{aligned} 299 \cdot 319 \cdot x_1 \equiv 118 \pmod{217} &\implies 118 \cdot x_1 \equiv 153 \pmod{217} \\ 217 \cdot 319 \cdot x_2 \equiv 154 \pmod{299} &\implies 154 \cdot x_2 \equiv 226 \pmod{299} \\ 217 \cdot 299 \cdot x_3 \equiv 298 \pmod{319} &\implies 126 \cdot x_3 \equiv 298 \pmod{319}. \end{aligned}$$

Dobivamo $x_1 = 176$, $x_2 = 17$, $x_3 = 53$ pa je $x_0 = 299 \cdot 319 \cdot 176 + 217 \cdot 319 \cdot 17 + 217 \cdot 299 \cdot 53 = 21402646 \equiv 704969 \pmod{M}$. Dakle, $m = \sqrt[3]{704969} = 89$.

4. 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).

Rj: Imamo sustav kongruencija:

$$x = m^3 \equiv 57 \pmod{161}, \quad x = m^3 \equiv 96 \pmod{247}, \quad x = m^3 \equiv 272 \pmod{493}.$$

Dakle, imamo $M = 161 \cdot 247 \cdot 493 = 19605131$ i $x_0 = 247 \cdot 493x_1 + 161 \cdot 493x_2 + 161 \cdot 247x_3$. Sada rješavamo kongruencije:

$$\begin{aligned} 247 \cdot 493 \cdot x_1 \equiv 57 \pmod{161} &\implies 55 \cdot x_1 \equiv 57 \pmod{161} \\ 161 \cdot 493 \cdot x_2 \equiv 96 \pmod{247} &\implies 86 \cdot x_2 \equiv 96 \pmod{247} \\ 161 \cdot 247 \cdot x_3 \equiv 272 \pmod{493} &\implies 327 \cdot x_3 \equiv 272 \pmod{493}. \end{aligned}$$

Dobivamo $x_1 = 83, x_2 = 116, x_3 = 34$ pa je $x_0 = 247 \cdot 493 \cdot 83 + 161 \cdot 493 \cdot 116 + 161 \cdot 247 \cdot 34 = 20666339 \equiv 1061208 \pmod{M}$. Dakle, $m = \sqrt[3]{1061208} = 102$.

5. Zadan je RSA kriptosustav s javnim ključem $(n, e) = (69627997, 43206989)$. Odredite pomoću Wienerovog napada skup mogućih tajnih ključeva d ako je poznato da vrijedi $d < \frac{1}{3}\sqrt[4]{n}$.

Rj: Winerov napad počinjemo zapisivanjem $\frac{e}{n}$ u obliku verižnog razlomka. Dakle, imamo:

$$\begin{aligned}
69627997 &= 1 \cdot 43206989 + 26421008 \\
43206989 &= 1 \cdot 26421008 + 16785981 \\
26421008 &= 1 \cdot 16785981 + 9635027 \\
16785981 &= 1 \cdot 9635027 + 7150954 \\
9635027 &= 1 \cdot 7150954 + 2484073 \\
7150954 &= 2 \cdot 2484073 + 2182808 \\
2484073 &= 1 \cdot 2182808 + 301265 \\
2182808 &= 7 \cdot 301265 + 73953 \\
301265 &= 4 \cdot 73953 + 5453 \\
73953 &= 13 \cdot 5453 + 3064 \\
5453 &= 1 \cdot 3064 + 2389 \\
3064 &= 1 \cdot 2389 + 675 \\
2389 &= 3 \cdot 675 + 364 \\
675 &= 1 \cdot 364 + 311 \\
364 &= 1 \cdot 311 + 53 \\
311 &= 5 \cdot 53 + 46 \\
53 &= 1 \cdot 46 + 7 \\
46 &= 6 \cdot 7 + 4 \\
7 &= 1 \cdot 4 + 3 \\
4 &= 1 \cdot 3 + 1 \\
3 &= 3 \cdot 1 + 0
\end{aligned}$$

Dakle, $\frac{43206989}{69627997} = [0; 1, 1, 1, 1, 1, 2, 1, 7, 4, 13, 1, 4, 3, 1, 5, 1, 6, 1]$. Sada znamo da je d nazivnik neke od konvergenti za koji je $d < \frac{1}{3}\sqrt[4]{n} < 31$. Dakle, imamo $q_{-1} = 0, q_0 = 1$ i rekurziju $q_i = q_{i-1}a_i + q_{i-2}$ za $i \geq 1$.

i	-1	0	1	2	3	4	5	6	7	8
a_i		0	1	1	1	1	1	2	1	7
q_i	0	1	1	2	3	5	8	21	29	224

Dakle, $d \in \{1, 2, 3, 5, 8, 21, 29\}$.

6. Zadan je RSA kriptosustav s javnim ključem $(n, e) = (60677801, 47474687)$. Odredite pomoću Wienerovog napada skup mogućih tajnih ključeva d ako je poznato da vrijedi $d < \frac{1}{3}\sqrt[4]{n}$.

Rj: Wienerov napad počinjemo zapisivanjem $\frac{e}{n}$ u obliku verižnog razlomka. Dakle, imamo:

$$\begin{aligned}
60677801 &= 1 \cdot 47474687 + 13203114 \\
47474687 &= 3 \cdot 13203114 + 7865345 \\
13203114 &= 1 \cdot 7865345 + 5337769 \\
7865345 &= 1 \cdot 5337769 + 2527576 \\
5337769 &= 2 \cdot 2527576 + 282617 \\
2527576 &= 8 \cdot 282617 + 266640 \\
282617 &= 1 \cdot 266640 + 15977 \\
266640 &= 16 \cdot 15977 + 11008 \\
15977 &= 1 \cdot 11008 + 4969 \\
11008 &= 2 \cdot 4969 + 1070 \\
4969 &= 4 \cdot 1070 + 689 \\
1070 &= 1 \cdot 689 + 381 \\
689 &= 1 \cdot 381 + 308 \\
381 &= 1 \cdot 308 + 73 \\
308 &= 4 \cdot 73 + 16 \\
73 &= 4 \cdot 16 + 9 \\
16 &= 1 \cdot 9 + 7 \\
9 &= 1 \cdot 7 + 2 \\
7 &= 3 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Dakle, $\frac{47474687}{60677801} = [0; 1, 3, 1, 1, 2, 8, 1, 16, 1, 2, 4, 1, 1, 1, 4, 4, 1, 1, 3, 2]$. Sada znamo da je d nazivnik neke od konvergenti za koji je $d < \frac{1}{3}\sqrt[4]{n} < 30$. Dakle, imamo $q_{-1} = 0, q_0 = 1$ i rekurziju $q_i = q_{i-1}a_i + q_{i-2}$ za $i \geq 1$.

i	-1	0	1	2	3	4	5	6
a_i		0	1	3	1	1	2	8
q_i	0	1	1	4	5	9	23	193

Dakle, $d \in \{1, 4, 5, 9, 23\}$.

7. U RSA kriptosustavu je $n = pq = 51809$, gdje su p i q prosti brojevi. Špijuniranjem ste otkrili da je $\sigma(n) = 52416$ ($\sigma(n)$ je suma djelitelja broja n). Odredite p i q bez poznavanja faktorizacije od n. Uputa: Iskoristite multiplikativnost od σ i Viètеove formule.

Rj: Budući da je

$$\sigma(n) = \sigma(pq) = \sigma(p)\sigma(q) = (p+1)(q+1) = 1 + p + q + pq = 1 + p + q + n$$

Imamo $p + q = \sigma(n) - n - 1 = 52416 - 51809 - 1 = 606$ te znamo $pq = 51809$. Dakle, p i q su rješenja kvadratne jednadžbe $x^2 - 606x + 51809 = 0$. Rješenja su $p = 103$ i $q = 503$.

8. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (2773, 47, 59),$$

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

Rj: Najprije trebamo naći kvadratne korijene od y modulo p i modulo q. Budući da je $p \equiv q \equiv 3 \pmod 4$, imamo

$$x = \pm\sqrt{y} \pmod p = \pm\sqrt{2729} \pmod{47} \equiv \pm 2729^{12} \equiv \pm 3^{12} \pmod{47}$$
$$x = \pm\sqrt{y} \pmod q = \pm\sqrt{2729} \pmod{59} \equiv 2729^{15} \equiv \pm 15^{15} \pmod{59}$$

Nadalje, imamo:

$$x \equiv \pm 9^6 \equiv \pm 81^3 \equiv \pm 34^3 \equiv \pm 28 \cdot 34 \equiv \pm 12 \pmod{47},$$
$$x \equiv \pm 15^{14} \cdot 15 \equiv \pm 48^7 \cdot 15 \equiv \pm 48^6 \cdot 12 \equiv \pm 3^3 \cdot 12 \equiv \pm 29 \pmod{59}.$$

Sada rješavamo ovaj sustav od 4 kongruencije malim kineskim teoremom. Dakle, trebamo naći u i v takve da je $59u + 47v = 1$. Te ćemo brojeve naći proširenim Euklidovim algoritmom.

x	y	g	u	v	w	$\lfloor \frac{g}{w} \rfloor$
1	0	59	0	1	47	1
0	1	47	1	-1	12	3
1	-1	12	-3	4	11	1
-3	4	11	4	-5	1	11
4	-5	1			0	

Dakle, $u = 4$ i $v = -5$. Sada su rješenja sustava kongruencija dana s $x \equiv 59 \cdot 4 \cdot (\pm 12) + 47 \cdot (-5) \cdot (\pm 29) \pmod{2773}$. Dakle, $x \equiv \pm 1563, \pm 1328 \pmod{2773}$, tj. imamo

$$x_1 = 1563 = 11000011011_2$$
$$x_2 = 1210 = 10010111010_2$$
$$x_3 = 1328 = 10100110000_2$$
$$x_4 = 1445 = 10110100101_2.$$

Dakle, otvoreni tekst je $x = 1328$.

9. U Rabinovom kriptosustavu s parametrima

$$(n, p, q) = (2021, 43, 47),$$

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

Rj: Najprije trebamo naći kvadratne korijene od y modulo p i modulo q. Budući da je $p \equiv q \equiv 3 \pmod 4$, imamo

$$x = \pm 917^{11} \equiv \pm 14^{10} \cdot 14 \equiv \pm 24^4 \cdot 24 \cdot 14 \equiv \pm 17^2 \cdot 35 \equiv \pm 10 \pmod{43},$$
$$x = \pm 917^{12} \equiv \pm 24^{12} \equiv \pm 12^6 \equiv \pm 3^3 \equiv \pm 27 \pmod{47}.$$

Sada rješavamo ovaj sustav od 4 kongruencije malim kineskim teoremom. Dakle, trebamo naći u i v takve da je $47u + 43v = 1$. Te ćemo brojeve naći proširenim Euklidovim algoritmom.

x	y	g	u	v	w	$\lfloor \frac{g}{w} \rfloor$
1	0	47	0	1	43	1
0	1	43	1	-1	4	10
1	-1	4	-10	11	3	1
-10	11	3	11	-12	1	3
11	-12	1			0	

Dakle, $u = 11$ i $v = -12$. Sada su rješenja sustava kongruencija dana s $x \equiv 47 \cdot 11 \cdot (\pm 10) + 43 \cdot (-12) \cdot (\pm 27) \pmod{2021}$. Dakle, $x \equiv \pm 1343, \pm 913 \pmod{2773}$, tj. imamo

$$x_1 = 1343 = 10100111111_2$$
$$x_2 = 913 = 1110010001_2$$
$$x_3 = 678 = 1010100110_2$$
$$x_4 = 1108 = 10001010100_2.$$

Dakle, otvoreni tekst je $x = 1343$.

10. Neka je u Diffie-Hellmanovom protokolu $G = \mathbb{Z}_p^*$, $p = 87671$, $g = 2$, $a = 1234$ i $b = 4321$. Odredite ključ $K = g^{ab}$.

Rj: Budući da je $\varphi(87671) = 87670$ i $1234 \cdot 4321 \equiv 71914 \pmod{87670}$, imamo

$$K = g^{ab} = 2^{1234 \cdot 4321} = 2^{71914}$$

Nadalje, imamo:

$$2^{16} = 65536, \quad 2^{32} = 52677, \quad 2^{64} = 79179 = -8492, \quad 2^{128} = 48502, \quad 2^{256} = 55732$$
$$2^{512} = 47636, \quad 2^{1024} = 3, \quad 2^{16384} = 3^{16} = 260, \quad 2^{65536} = 260^4 = 84467$$

$$\begin{aligned} 2^{71914} &= 2^{65536} \cdot 2^{6144} \cdot 2^{128} \cdot 2^{64} \cdot 2^{32} \cdot 2^{10} = 84467 \cdot 3^6 \cdot 48502 \cdot (-8492) \cdot 52677 \cdot 1024 \\ &= 84467 \cdot 729 \cdot 48502 \cdot (-8492) \cdot 23583 = 31401 \cdot 48502 \cdot 61399 = 78361 \cdot 61399 \\ &= 77901 \end{aligned}$$

Dakle, ključ je $K = 77901$.

11. Zadan je ElGamalov kriptosustav s ključem $K = (p = 41, \alpha = 6, a = 10, \beta = 32)$. Dešifrirajte šifrat $(y_1, y_2) = (11, 21)$.

Rj: Da bismo dešifrirali šifrat, potrebno je izračunati $y_2 \cdot (y_1^a)^{-1} \pmod p$. Dakle, prvo ćemo izračunati $y_1^a \pmod p$.

$$y_1^a \equiv 11^{10} \equiv (-2)^5 \equiv -32 \equiv 9 \pmod{41}.$$

Sada trebamo izračunati inverz broja 9 modulo 41. To možemo napraviti proširenim Euklidovim algoritmom.

x	y	g	u	v	w	$\lfloor \frac{g}{w} \rfloor$
1	0	41	0	1	9	4
0	1	9	1	-4	5	1
1	-4	5	-1	5	4	1
-1	5	4	2	-9	1	4
2	-9	1			0	

Dakle, $41 \cdot (2) + 9 \cdot (-9) = 1$, tj. $9 \cdot (-9) \equiv 1 \pmod{41}$. Dakle, $y_1^{-a} \equiv 9^{-1} \equiv -9 \pmod{41}$. Sada možemo izračunati $y_2 \cdot (y_1)^{-a} \equiv 21 \cdot -9 \equiv 16 \pmod{41}$. Dakle, dešifrirani tekst je 16.

12. Neka je u ElGamalovom kriptosustavu $p = 1777$, $\alpha = 6$ i $a = 1009$.
    a) Šifrirajte otvoreni tekst $x = 1483$, uz pretpostavku da je jednokratni ključ $k = 701$.
    b) Dešifrirajte šifrat $(1664, 1031)$.

Rj:

a) Da bismo šifrirali otvoreni tekst, trebamo izračunati $e(x, k) = (\alpha^k \pmod p, x \cdot \beta^k \pmod p)$. Dakle, imamo

$$\begin{aligned}
\alpha^k &\equiv 6^{701} \equiv 6^{512} \cdot 6^{128} \cdot 6^{32} \cdot 6^{16} \cdot 6^8 \cdot 6^4 \cdot 6 \pmod{1777} \\
&\equiv 1296^{128} \cdot 1296^{32} \cdot 1296^8 \cdot 1296^4 \cdot 1296^2 \cdot 1296 \cdot 6 \pmod{1777} \\
&\equiv 351^{64} \cdot 351^{16} \cdot 351^4 \cdot 351^2 \cdot 351 \cdot 668 \equiv 588^{32} \cdot 588^8 \cdot 588^2 \cdot 588 \cdot 1681 \pmod{1777} \\
&\equiv 1006^{16} \cdot 1006^4 \cdot 1006 \cdot 416 \equiv 923^8 \cdot 923^2 \cdot 901 \equiv 746^4 \cdot 746 \cdot 901 \pmod{1777} \\
&\equiv 315^2 \cdot 440 \equiv 1490 \cdot 440 \equiv 1664 \pmod{1777}.
\end{aligned}$$

Sada možemo izračunati $\beta^k \equiv (\alpha^k)^a \pmod p$.

$$\begin{aligned}
\beta^k &\equiv 1664^{1009} \equiv 1664^{512} \cdot 1664^{256} \cdot 1664^{128} \cdot 1664^{64} \cdot 1664^{32} \cdot 1664^{16} \cdot 1664 \pmod{1777} \\
&\equiv 330^{256} \cdot 330^{128} \cdot 330^{64} \cdot 330^{32} \cdot 330^{16} \cdot 330^8 \cdot 1664 \pmod{1777} \\
&\equiv 503^{128} \cdot 503^{64} \cdot 503^{32} \cdot 503^{16} \cdot 503^8 \cdot 503^4 \cdot 1664 \pmod{1777} \\
&\equiv 713^{32} \cdot 713^{16} \cdot 713^8 \cdot 713^4 \cdot 713^2 \cdot 713 \cdot 1664 \pmod{1777} \\
&\equiv 147^{16} \cdot 147^8 \cdot 147^4 \cdot 147^2 \cdot 147 \cdot 1173 \equiv 285^8 \cdot 285^4 \cdot 285^2 \cdot 285 \cdot 62 \pmod{1777} \\
&\equiv 1260^4 \cdot 1260^2 \cdot 1260 \cdot 1677 \equiv 739^2 \cdot 739 \cdot 167 \equiv 582 \cdot 800 \equiv 26 \pmod{1777}.
\end{aligned}$$

Dakle, šifrat je $(1664, 1241)$.

b) Da bismo dešifrirali šifrat, trebamo izračunati $y_2 \cdot (y_1^a)^{-1} \pmod p$. Dakle, prvo ćemo izračunati $y_1^a \pmod p$.

$$y_1^a \equiv 1664^{1009} \equiv 26 \pmod{1777}.$$

Sada trebamo naći inverz broja 26 modulo 1777. To možemo napraviti proširenim Euklidovim algoritmom.

x	y	g	u	v	w	$\lfloor \frac{g}{w} \rfloor$
1	0	1777	0	1	26	68
0	1	26	1	-68	9	2
1	-68	9	-2	137	8	1
-2	137	8	3	-205	1	8
3	-205	1			0	

Dakle, $1777 \cdot 3 + 26 \cdot (-205) = 1$, tj. $26 \cdot (-205) \equiv 1 \pmod{1777}$. Dakle, $y_1^{-a} \equiv 26^{-1} \equiv -205 \pmod{1777}$. Sada možemo izračunati $y_2 \cdot (y_1)^{-a} \equiv 1031 \cdot -205 \equiv 108 \pmod{1777}$. Dakle, otvoreni tekst je $x = 108$.

13. Zadan je Merkle-Hellmanov kriptosustav s ključem $K = (v, p, a, t)$ gdje je

$$v = (3, 6, 24, 48, 95, 187, 380, 760),$$
$$p = 1571,\ a = 111,$$
$$t = (333, 666, 1093, 615, 1119, 334, 1334, 1097).$$

Dešifrirajte šifrat $y = 3379$.

Rj: Najprije izračunamo inverz od a modulo p. To možemo napraviti proširenim Euklidovim algoritmom.

x	y	g	u	v	w	$\lfloor \frac{g}{w} \rfloor$
1	0	1571	0	1	111	14
0	1	111	1	-14	17	6
1	-14	17	-6	85	9	1
-6	85	9	7	-99	8	1
7	-99	8	-13	184	1	8
-13	184	8			0	

Dakle, $a^{-1} \equiv 184 \pmod{1571}$. Sada računamo $z = y \cdot a^{-1} \pmod p$ i dobivamo $z = 1191$. Sada rješavamo superrastući problem ruksaka sa $v = (3, 6, 24, 48, 95, 187, 380, 760)$ i $V = 1191$. Budući da je $1191 = 760 + 380 + 48 + 3$, dobivamo $x = (1, 0, 0, 1, 0, 0, 1, 1)$.