

**Лабораторные работы по разделу**  
**«Криптографические системы с открытым ключом»**  
**Лабораторная работа № 6**

**Расшифрование криптограммы на основе эллиптических кривых**

*Цель работы:* дан шифртекст, используя алфавит, приведенный в учебно-методическом пособии к выполнению лабораторного практикума по дисциплине «Криптография» в подразделе «Задачи к лабораторным работам по криптографии на эллиптических кривых (используется кривая  $E_{751}(-1,1)$  – и генерирующая точка  $G = (0,1)$ )» и зная секретный ключ  $n_b$ , найти открытый текст.

*Ход работы:*

– ознакомиться с теорией в учебном пособии «Криптография», а также в учебно-методическом пособии к выполнению лабораторного практикума по дисциплине «Криптография»;

– получить вариант задания у преподавателя;

– найти открытый текст;

– результаты и промежуточные вычисления оформить в виде отчета.

Алфавит представляет собой множество символов языка открытых текстов и соответствующих им текстов эллиптической кривой над конечным полем.

Для заданий лабораторной работы выбрана кривая  $E_{751}(-1,1)$ , т.е.  $y^2 = x^3 - x + 1 \pmod{751}$ . Предлагается следующий (один из возможных) алфавит, приведенный в таблице.

Таблица. Алфавит точек эллиптической кривой для выполнения лабораторных работ

№	символ	точка	35	В	(67, 84)	70	е	(99, 456)	105	Й	(198, 527)
1	пробел	(33, 355)	36	С	(67, 667)	71	ф	(100, 364)	106	К	(200, 30)
2	!	(33, 396)	37	Д	(69, 241)	72	g	(100, 387)	107	Л	(200, 721)
3	"	(34, 74)	38	Е	(69, 510)	73	h	(102, 267)	108	М	(203, 324)
4	#	(34, 677)	39	Ф	(70, 195)	74	i	(102, 484)	109	Н	(203, 427)
5	\$	(36, 87)	40	Г	(70, 556)	75	j	(105, 369)	110	О	(205, 372)
6	%	(36, 664)	41	Н	(72, 254)	76	k	(105, 382)	111	П	(205, 379)
7	&	(39, 171)	42	И	(72, 497)	77	l	(106, 24)	112	Р	(206, 106)
8	'	(39, 580)	43	Ж	(73, 72)	78	m	(106, 727)	113	С	(206, 645)
9	(	(43, 224)	44	К	(73, 679)	79	n	(108, 247)	114	Т	(209, 82)
10	)	(43, 527)	45	Л	(74, 170)	80	o	(108, 504)	115	У	(209, 669)
11	*	(44, 366)	46	М	(74, 581)	81	p	(109, 200)	116	Ф	(210, 31)
12	+	(44, 385)	47	Н	(75, 318)	82	q	(109, 551)	117	Х	(210, 720)
13	,	(45, 31)	48	О	(75, 433)	83	r	(110, 129)	118	Ц	(215, 247)
14	-	(45, 720)	49	Р	(78, 271)	84	s	(110, 622)	119	Ч	(215, 504)
15	.	(47, 349)	50	Q	(78, 480)	85	t	(114, 144)	120	Ш	(218, 150)
16	/	(47, 402)	51	Р	(79, 111)	86	u	(114, 607)	121	Щ	(218, 601)
17	0	(48, 49)	52	С	(79, 640)	87	v	(115, 242)	122	Ъ	(221, 138)
18	1	(48, 702)	53	Т	(80, 318)	88	w	(115, 509)	123	Ы	(221, 613)
19	2	(49, 183)	54	U	(80, 433)	89	x	(116, 92)	124	Ь	(226, 9)
20	3	(49, 568)	55	V	(82, 270)	90	y	(116, 659)	125	Э	(226, 742)

21	4	(53, 277)	56	W	(82, 481)	91	z	(120, 147)	126	Ю	(227, 299)
22	5	(53, 474)	57	X	(83, 373)	92	{	(120, 604)	127	Я	(227, 452)
23	6	(56, 332)	58	Y	(83, 378)	93		(125, 292)	128	а	(228, 271)
24	7	(56, 419)	59	Z	(85, 35)	94	}	(125, 459)	129	б	(228, 480)
25	8	(58, 139)	60	[	(85, 716)	95	~	(126, 33)	130	в	(229, 151)
26	9	(58, 612)	61	\	(86, 25)	96	A	(189, 297)	131	г	(229, 600)
27	:	(59, 365)	62	]	(86, 726)	97	Б	(189, 454)	132	д	(234, 164)
28	;	(59, 386)	63	^	(90, 21)	98	В	(192, 32)	133	е	(234, 587)
29	<	(61, 129)	64	_	(90, 730)	99	Г	(192, 719)	134	ж	(235, 19)
30	=	(61, 622)	65	`	(93, 267)	100	Д	(194, 205)	135	з	(235, 732)
31	>	(62, 372)	66	a	(93, 484)	101	Е	(194, 546)	136	и	(236, 39)
32	?	(62, 379)	67	b	(98, 338)	102	Ж	(197, 145)	137	й	(236, 712)
33	@	(66, 199)	68	c	(98, 413)	103	З	(197, 606)	138	к	(237, 297)
34	A	(66, 552)	69	d	(99, 295)	104	И	(198, 224)	139	л	(237, 454)

140	м	(238, 175)	145	с	(243, 664)	150	ц	(250, 14)	155	ы	(253, 540)
141	н	(238, 576)	146	т	(247, 266)	151	ч	(250, 737)	156	ь	(256, 121)
142	о	(240, 309)	147	у	(247, 485)	152	ш	(251, 245)	157	э	(256, 630)
143	п	(240, 442)	148	ф	(249, 183)	153	щ	(251, 506)	158	ю	(257, 293)
144	р	(243, 87)	149	х	(249, 568)	154	ъ	(253, 211)	159	я	(257, 458)

Заметим, что мощность множества точек на этой кривой  $N = 727$ , поэтому при необходимости можно точками закодировать и некоторые специальные знаки (например, знак интеграла и т.п.), а также целые слова.

### Пример шифрования

Пусть выбрана генерирующая точка  $G = (0,1)$ . Предположим, пользователь А решил отправить пользователю В сообщение: строчную латинскую букву «А». В нашем алфавите эта буква кодируется точкой  $P_m = (66, 522)$ . Пусть пользователь А выбрал случайное значение  $k = 3$ , а открытым ключом В является точка  $P_B = (406, 397)$ , при этом секретным ключом В является число  $n_b = 45$ .

Шифрованный текст имеет вид  $C_m = \{kG, P_m + kP_B\}$ .

Находим  $kG = 3 \times (0,1)$ .

Для нахождения  $3G$  используем правила сложения точек эллиптической кривой. Напомним их:

$$\begin{aligned}
 x_3 &= \lambda^2 - x_1 - x_2 \pmod{p} \\
 y_3 &= \lambda(x_1 - x_3) - y_1 \pmod{p} \\
 \lambda &= \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{если } P \neq Q; \\ \frac{3x_1^2 + a}{2y_1}, & \text{если } P = Q. \end{cases}
 \end{aligned}$$

Вычисляем  $2G$ :

$$\lambda = \frac{3(0^2) - 1}{2 \times 1} = \frac{-1}{2} \equiv 375 \pmod{751} \left( \frac{-1 + 751}{2} = 375 \right)$$

$$x_3 = 375^2 - 0 - 0 = 140625 \equiv 188 \pmod{751}$$

$$y_3 = 375(0 - 188) - 1 = -70501 \equiv 93 \pmod{23}$$

Итак, мы нашли  $2G = (188, 93)$ . Теперь находим  $3G$ .

$$\lambda = \frac{188 - 0}{93 - 1} = \frac{188}{92} \equiv 368 \pmod{751}$$

$$x_3 = 368^2 - 0 - 188 = 135236 \equiv 56 \pmod{751}$$

$$y_3 = 368(0 - 56) - 1 = 20607 \equiv 419 \pmod{751}$$

Таким образом, мы нашли точку  $kG = 3 \cdot (0, 1) = (56, 419)$ .

Вычисляем  $P_m + kP_B = (66, 552) + 3 \cdot (406, 397) = (301, 734)$ .

В результате:  $C_m = \{(56, 419), (301, 734)\}$ .

Пользователь В для расшифрования сообщения должен провести следующие вычисления:

$$P_m + kP_B - n_B(kG) = P_m + k(n_B G) - n_B(kG) = (301, 734) - 45 \cdot (56, 419) = (301, 734) + (175, 559) = (66, 552).$$

После этого пользователь В по алфавиту определяет открытый буквенный текст: точке  $(66, 552)$  соответствует строчная латинская буква «А».

#### Варианты заданий

№ варианта	Секретный ключ $nb$	Шифртекст
1	29	$\{(440, 539), (128, 672)\}; \{(489, 468), (282, 341)\};$ $\{(489, 468), (45, 720)\}; \{(72, 254), (227, 299)\};$ $\{(188, 93), (251, 506)\}; \{(72, 254), (319, 518)\};$ $\{(745, 210), (129, 659)\}; \{(286, 136), (515, 684)\};$ $\{(568, 355), (395, 414)\}$
2	25	$\{(72, 254), (397, 184)\}; \{(188, 93), (526, 412)\};$ $\{(188, 93), (328, 290)\}; \{(135, 82), (433, 47)\};$ $\{(179, 275), (711, 341)\}; \{(568, 355), (546, 670)\};$ $\{(16, 416), (734, 170)\}; \{(568, 355), (371, 14)\};$ $\{(596, 433), (604, 610)\}; \{(16, 416), (734, 170)\}$
3	40	$\{(188, 93), (573, 583)\}; \{(188, 93), (128, 79)\};$ $\{(425, 663), (703, 125)\}; \{(489, 468), (109, 200)\};$ $\{(568, 355), (348, 27)\}; \{(377, 456), (323, 657)\};$ $\{(72, 254), (399, 65)\}; \{(16, 416), (660, 275)\};$ $\{(179, 275), (267, 670)\}; \{(568, 355), (642, 53)\}$
4	34	$\{(618, 206), (426, 662)\}; \{(72, 254), (67, 667)\}; \{(286, 136), (739, 574)\};$ $\{(16, 416), (143, 602)\}; \{(618, 206), (313, 203)\}; \{(618, 206), (114, 607)\};$ $\{(618, 206), (438, 711)\}; \{(188, 93), (573, 168)\}$
5	41	$\{(283, 493), (314, 127)\}; \{(425, 663), (561, 140)\};$ $\{(568, 355), (75, 433)\}; \{(440, 539), (602, 627)\};$ $\{(188, 93), (395, 414)\}; \{(179, 275), (25, 604)\};$ $\{(72, 254), (47, 349)\}; \{(72, 254), (417, 137)\};$ $\{(188, 93), (298, 225)\}; \{(56, 419), (79, 111)\}$

6	44	$\{(377, 456), (367, 360)\}; \{(425, 663), (715, 398)\};$ $\{(188, 93), (279, 353)\}; \{(179, 275), (128, 79)\};$ $\{(568, 355), (515, 67)\}; \{(568, 355), (482, 230)\}; \{(377, 456),$ $(206, 645)\}; \{(188, 93), (300, 455)\};$ $\{(489, 468), (362, 446)\}; \{(16, 416), (69, 510)\};$ $\{(425, 663), (218, 601)\}$
7	12	$\{(16, 416), (128, 672)\}; \{(56, 419), (59, 386)\};$ $\{(425, 663), (106, 24)\}; \{(568, 355), (145, 608)\};$ $\{(188, 93), (279, 398)\}; \{(425, 663), (99, 295)\}; \{(179, 275),$ $(269, 187)\}; \{(188, 93), (395, 337)\};$ $\{(188, 93), (311, 68)\}; \{(135, 82), (556, 484)\};$ $\{(56, 419), (106, 727)\}; \{(16, 416), (307, 693)\}$
8	45	$\{(745, 210), (259, 401)\}; \{(568, 355), (606, 147)\};$ $\{(188, 93), (407, 82)\}; \{(56, 419), (739, 574)\};$ $\{(286, 136), (329, 447)\}; \{(425, 663), (520, 749)\}; \{(72, 254),$ $(374, 315)\}; \{(188, 93), (149, 97)\};$ $\{(745, 210), (13, 134)\}; \{(440, 539), (235, 19)\};$ $\{(425, 663), (128, 79)\}$
9	32	$\{(188, 93), (623, 166)\}; \{(725, 195), (513, 414)\};$ $\{(346, 242), (461, 4)\}; \{(489, 468), (739, 574)\};$ $\{(725, 195), (663, 476)\}; \{(745, 210), (724, 522)\};$ $\{(725, 195), (663, 476)\}; \{(618, 206), (438, 40)\};$ $\{(286, 136), (546, 670)\}; \{(179, 275), (73, 72)\}$ $\{(179, 275), (269, 564)\}; \{(179, 275), (73, 72)\};$ $\{(440, 539), (189, 454)\}; \{(618, 206), (628, 458)\};$
10	18	$\{(568, 355), (660, 275)\}; \{(72, 254), (709, 595)\}; \{(745, 210),$ $(12, 314)\}; \{(188, 93), (36, 664)\};$ $\{(618, 206), (530, 22)\}; \{(286, 136), (532, 50)\};$ $\{(425, 663), (660, 275)\}; \{(725, 195), (482, 230)\}$