Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет ИТМО»
Мегафакультет: Компьютерных технологий и Управления
Факультет: Безопасности информационных технологий
Направление (специальность): «Информационная безопасность»
Профиль: 10.03.01 «Комплексная защита объектов информатизации»

Лабораторные работы

по дисциплине

Криптографические методы защиты информации

Тема задания: «Эллиптические кривые»

Выполнил:
студент Смирнов М. Г. _____
Проверил:
к.т.н., доцент Михайличенко О.В._____

Дата: _____
Оценка: _____

Санкт-Петербург, 2019 г.

Содержание

1 Шифрование открытого текста на основе эллиптических кривых

Цель работы - зашифровать открытый текст, используя алфавит, приведённый в учебно-методическом пособии к выполнению лабораторного практикума по дисциплине «Криптография» в подразделе «Задачи к лабораторным работам по криптографии на эллиптических кривых (используется кривая $E751(-1,1)$ − и генерирующая точка $G = (0, 1)$)».

Номер варианта	7
Открытый текст	терпеливо
Открытый ключ B	(725, 195)
Значения случайных чисел k для букв открытого текста	17, 5, 4, 17, 13, 2, 17, 14, 19

Пользователь A решил передать пользователю B сообщение «**терпеливо**». В нашем алфавите эти буквы кодируются как представлено в таблице 1.

Таблица 1: Кодирование заданного сообщения

Символ	Точка
т	(247, 266)
е	(234, 587)
р	(243, 87)
п	(240, 442)
е	(234, 587)
л	(237, 454)
и	(236, 39)
в	(229, 151)
о	(240, 309)

Для заданий лабораторной работы выбрана кривая E751 $(-1,1)$, т.е. $y^2 = x^3 - x + 1 \pmod{751}$. Кривая представлена на рисунке 1.

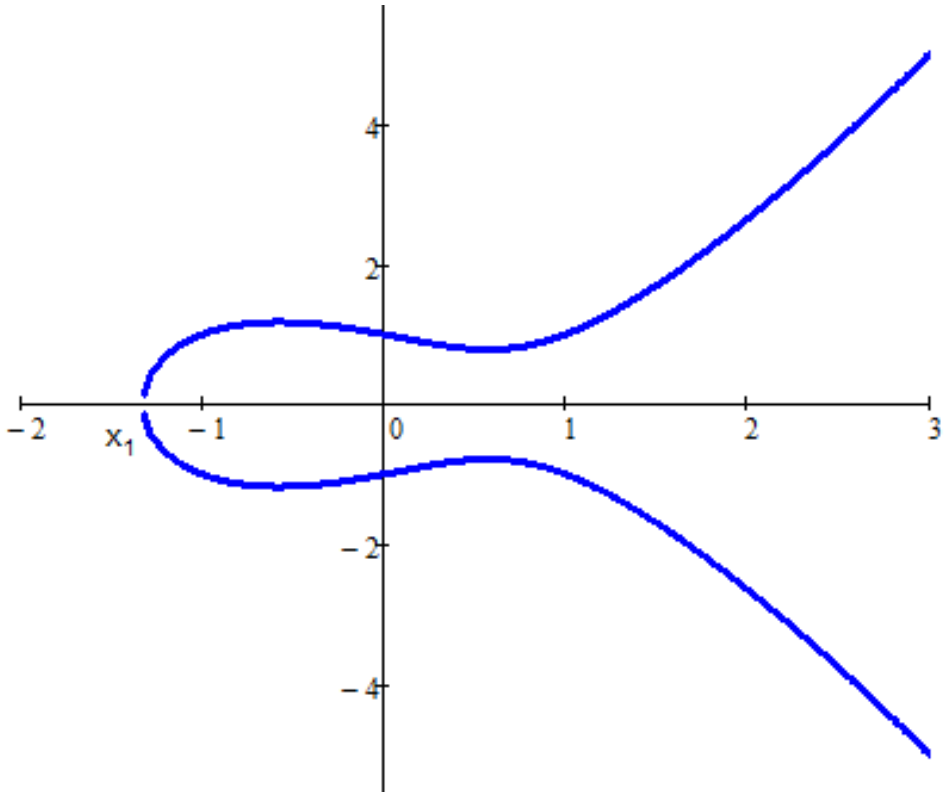

Рис. 1: Кривая $y^2 = x^3 - x + 1$

Шифрованный текст имеет вид $C_m = \{kG, P_m + k \cdot P_b\}$.
Для нахождения kG используем правила сложения точек эллиптической кривой.

$$x_3 = \lambda^2 - x_1 - x_2 \pmod{p}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p}$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, & P = Q \end{cases}$$

Вычисляем 2G:

$$\lambda = \frac{3 \cdot 0^2 + (-1)}{2 \cdot 1} = \frac{-1}{2} = -1 \cdot 2^{-1} = 750 \cdot 376 \mod 751 = 375 \mod 751$$

$$x = 375^2 - 0 - 0 \mod 751 = 188 \mod 751$$

$$y = 375 \cdot (0 - 188) - 1 \mod 751 = 93 \mod 751$$

2G = (188, 93)

Вычисляем 3G:

$$\lambda = \frac{1 - 93}{0 - 188} = \frac{-92}{-188} = 92 \cdot 188^{-1} \mod 751 = 92 \cdot 4 \mod 751$$

$$x = 368^2 - 188 - 0 \mod 751 = 56 \mod 751$$

$$y = 368 \cdot (188 - 56) - 93 \mod 751 = 419 \mod 751$$

3G = (56, 419)

Вычисляем 4G:

$$\lambda = \frac{3 \cdot 188^2 + (-1)}{2 \cdot 93} = \frac{106031}{186} = 106031 \cdot 186^{-1} = 140 \cdot 214 \mod 751 = 671 \mod 751$$

$$x = 671^2 - 188 - 188 \mod 751 = 16 \mod 751$$

$$y = 671 \cdot (188 - 16) - 93 \mod 751 = 416 \mod 751$$

4G = (16, 416)

Вычисляем 5G:

$$\lambda = \frac{93 - 419}{188 - 56} = \frac{-326}{132} = -326 \cdot 132^{-1} \mod 751 = 425 \cdot 165 \mod 751$$

$$x = 282^2 - 56 - 188 \mod 751 = 425 \mod 751$$

$$y = 282 \cdot (56 - 425) - 419 \mod 751 = 663 \mod 751$$

5G = (425, 663)

Вычисляем 6G:

$$\lambda = \frac{3 \cdot 56^2 + (-1)}{2 \cdot 419} = \frac{9407}{838} = 9407 \cdot 838^{-1} = 395 \cdot 587 \mod 751 = 557 \mod 751$$

$$x = 557^2 - 56 - 56 \mod 751 = 725 \mod 751$$

$$y = 557 \cdot (56 - 725) - 419 \mod 751 = 195 \mod 751$$

6G = (725, 195)

Вычисляем 7G:

$$\lambda = \frac{419 - 416}{56 - 16} = \frac{3}{40} = 3 \cdot 40^{-1} \mod 751 = 3 \cdot 169 \mod 751$$

$$x = 507^2 - 16 - 56 \mod 751 = 135 \mod 751$$

$$y = 507 \cdot (16 - 135) - 416 \mod 751 = 82 \mod 751$$

7G = (135, 82)

Вычисляем 8G:

$$\lambda = \frac{3 \cdot 16^2 + (-1)}{2 \cdot 416} = \frac{767}{832} = 767 \cdot 832^{-1} = 16 \cdot 102 \mod 751 = 130 \mod 751$$

$$x = 130^2 - 16 - 16 \mod 751 = 346 \mod 751$$

$$y = 130 \cdot (16 - 346) - 416 \mod 751 = 242 \mod 751$$

8G = (346, 242)

Вычисляем 9G:

$$\lambda = \frac{416 - 663}{16 - 425} = \frac{-247}{-409} = 247 \cdot 409^{-1} \mod 751 = 247 \cdot 213 \mod 751$$

$$x = 41^2 - 425 - 16 \mod 751 = 489 \mod 751$$

$$y = 41 \cdot (425 - 489) - 663 \mod 751 = 468 \mod 751$$

9G = (489, 468)

Вычисляем 10G:

$$\lambda = \frac{3 \cdot 425^2 + (-1)}{2 \cdot 663} = \frac{541874}{1326} = 541874 \cdot 1326^{-1} = 403 \cdot 64 \mod 751 = 258 \mod 751$$

$$x = 258^2 - 425 - 425 \mod 751 = 377 \mod 751$$

$$y = 258 \cdot (425 - 377) - 663 \mod 751 = 456 \mod 751$$

10G = (377, 456)

Вычисляем 11G:

$$\lambda = \frac{1 - 456}{0 - 377} = \frac{-455}{-377} = 455 \cdot 377^{-1} \mod 751 = 455 \cdot 251 \mod 751$$

$$x = 53^2 - 377 - 0 \mod 751 = 179 \mod 751$$

$$y = 53 \cdot (377 - 179) - 456 \mod 751 = 275 \mod 751$$

11G = (179, 275)

Вычисляем 12G:

$$\lambda = \frac{3 \cdot 725^2 + (-1)}{2 \cdot 195} = \frac{1576874}{390} = 1576874 \cdot 390^{-1} = 525 \cdot 518 \mod 751 = 88 \mod 751$$

$$x = 88^2 - 725 - 725 \mod 751 = 286 \mod 751$$

$$y = 88 \cdot (725 - 286) - 195 \mod 751 = 136 \mod 751$$

12G = (286, 136)

Вычисляем 13G:

$$\lambda = \frac{195 - 82}{725 - 135} = \frac{113}{590} = 113 \cdot 590^{-1} \mod 751 = 113 \cdot 737 \mod 751$$

$$x = 671^2 - 135 - 725 \mod 751 = 283 \mod 751$$

$$y = 671 \cdot (135 - 283) - 82 \mod 751 = 493 \mod 751$$

13G = (283, 493)

Вычисляем 14G:

$$\lambda = \frac{3 \cdot 135^2 + (-1)}{2 \cdot 82} = \frac{54674}{164} = 54674 \cdot 164^{-1} = 602 \cdot 664 \mod 751 = 196 \mod 751$$

$$x = 196^2 - 135 - 135 \mod 751 = 596 \mod 751$$

$$y = 196 \cdot (135 - 596) - 82 \mod 751 = 433 \mod 751$$

14G = (596, 433)

Вычисляем 15G:

$$\lambda = \frac{82 - 242}{135 - 346} = \frac{-160}{-211} = 160 \cdot 211^{-1} \mod 751 = 160 \cdot 210 \mod 751$$

$$x = 556^2 - 346 - 135 \mod 751 = 745 \mod 751$$

$$y = 556 \cdot (346 - 745) - 242 \mod 751 = 210 \mod 751$$

15G = (745, 210)

Вычисляем 16G:

$$\lambda = \frac{3 \cdot 346^2 + (-1)}{2 \cdot 242} = \frac{359147}{484} = 359147 \cdot 484^{-1} = 169 \cdot 45 \mod 751 = 95 \mod 751$$

$$x = 95^2 - 346 - 346 \mod 751 = 72 \mod 751$$

$$y = 95 \cdot (346 - 72) - 242 \mod 751 = 254 \mod 751$$

16G = (72, 254)

Вычисляем 17G:

$$\lambda = \frac{242 - 468}{346 - 489} = \frac{-226}{-143} = 226 \cdot 143^{-1} \mod 751 = 226 \cdot 730 \mod 751$$

$$x = 511^2 - 489 - 346 \mod 751 = 440 \mod 751$$

$$y = 511 \cdot (489 - 440) - 468 \mod 751 = 539 \mod 751$$

17G = (440, 539)

Вычисляем 18G:

$$\lambda = \frac{3 \cdot 489^2 + (-1)}{2 \cdot 468} = \frac{717362}{936} = 717362 \cdot 936^{-1} = 157 \cdot 341 \mod 751 = 216 \mod 751$$

$$x = 216^2 - 489 - 489 \mod 751 = 618 \mod 751$$

$$y = 216 \cdot (489 - 618) - 468 \mod 751 = 206 \mod 751$$

18G = (618, 206)

Вычисляем 19G:

$$\lambda = \frac{468 - 456}{489 - 377} = \frac{12}{112} = 12 \cdot 112^{-1} \mod 751 = 12 \cdot 114 \mod 751$$

$$x = 617^2 - 377 - 489 \mod 751 = 568 \mod 751$$

$$y = 617 \cdot (377 - 568) - 456 \mod 751 = 355 \mod 751$$

19G = (568, 355)

Вычисляем $Pm + kPb$ для каждой буквы в слове.

$Pm(\mathbf{т}) + k \cdot Pb = (247, 266) + 17 \cdot (725, 195) = (247, 266) + (179, 275) = (663, 275)$

$$\lambda = \frac{275 - 266}{179 - 247} = \frac{9}{-68} = 9 \cdot -68^{-1} \mod 751 = 9 \cdot 254 \mod 751$$

$$x = 33^2 - 247 - 179 \mod 751 = 663 \mod 751$$

$$y = 33 \cdot (247 - 663) - 266 \mod 751 = 275 \mod 751$$

$Pm(\mathbf{е}) + k \cdot Pb = (234, 587) + 5 \cdot (725, 195) = (234, 587) + (1, 1) = (638, 131)$

$$\lambda = \frac{1 - 587}{1 - 234} = \frac{-586}{-233} = 586 \cdot 233^{-1} \mod 751 = 586 \cdot 361 \mod 751$$

$$x = 515^2 - 234 - 1 \mod 751 = 638 \mod 751$$

$$y = 515 \cdot (234 - 638) - 587 \mod 751 = 131 \mod 751$$

$Pm(\mathbf{р}) + k \cdot Pb = (243, 87) + 4 \cdot (725, 195) = (243, 87) + (327, 108) = (228, 480)$

$$\lambda = \frac{108 - 87}{327 - 243} = \frac{21}{84} = 21 \cdot 84^{-1} \mod 751 = 21 \cdot 152 \mod 751$$

$$x = 188^2 - 243 - 327 \mod 751 = 228 \mod 751$$

$$y = 188 \cdot (243 - 228) - 87 \mod 751 = 480 \mod 751$$

$$Pm(\textbf{п}) + k \cdot Pb = (240, 442) + 17 \cdot (725, 195) = (240, 442) + (179, 275) = (329, 447)$$

$$\lambda = \frac{275 - 442}{179 - 240} = \frac{-167}{-61} = 167 \cdot 61^{-1} \mod 751 = 167 \cdot 197 \mod 751$$

$$x = 606^2 - 240 - 179 \mod 751 = 329 \mod 751$$

$$y = 606 \cdot (240 - 329) - 442 \mod 751 = 447 \mod 751$$

$$Pm(\textbf{е}) + k \cdot Pb = (234, 587) + 13 \cdot (725, 195) = (234, 587) + (283, 258) = (463, 736)$$

$$\lambda = \frac{258 - 587}{283 - 234} = \frac{-329}{49} = -329 \cdot 49^{-1} \mod 751 = 422 \cdot 46 \mod 751$$

$$x = 637^2 - 234 - 283 \mod 751 = 463 \mod 751$$

$$y = 637 \cdot (234 - 463) - 587 \mod 751 = 736 \mod 751$$

$$Pm(\textbf{л}) + k \cdot Pb = (237, 454) + 2 \cdot (725, 195) = (237, 454) + (286, 136) = (688, 741)$$

$$\lambda = \frac{136 - 454}{286 - 237} = \frac{-318}{49} = -318 \cdot 49^{-1} \mod 751 = 433 \cdot 46 \mod 751$$

$$x = 392^2 - 237 - 286 \mod 751 = 688 \mod 751$$

$$y = 392 \cdot (237 - 688) - 454 \mod 751 = 741 \mod 751$$

$$Pm(\textbf{и}) + k \cdot Pb = (236, 39) + 17 \cdot (725, 195) = (236, 39) + (179, 275) = (407, 669)$$

$$\lambda = \frac{275 - 39}{179 - 236} = \frac{236}{-57} = 236 \cdot -57^{-1} \mod 751 = 236 \cdot 527 \mod 751$$

$$x = 457^2 - 236 - 179 \mod 751 = 407 \mod 751$$

$$y = 457 \cdot (236 - 407) - 39 \mod 751 = 669 \mod 751$$

$$Pm(\textbf{в}) + k \cdot Pb = (229, 151) + 14 \cdot (725, 195) = (229, 151) + (135, 669) = (6, 218)$$

$$\lambda = \frac{669 - 151}{135 - 229} = \frac{518}{-94} = 518 \cdot -94^{-1} \mod 751 = 518 \cdot 743 \mod 751$$

$$x = 362^2 - 229 - 135 \mod 751 = 6 \mod 751$$

$$y = 362 \cdot (229 - 6) - 151 \mod 751 = 218 \mod 751$$

$$Pm(\textbf{о}) + k \cdot Pb = (240, 309) + 19 \cdot (725, 195) = (240, 309) + (591, 555) = (561, 140)$$

$$\lambda = \frac{555 - 309}{591 - 240} = \frac{246}{351} = 246 \cdot 351^{-1} \mod 751 = 246 \cdot 659 \mod 751$$

$$x = 649^2 - 240 - 591 \mod 751 = 561 \mod 751$$

$$y = 649 \cdot (240 - 561) - 309 \mod 751 = 140 \mod 751$$

Итог шифрования:

Cm(т) = ((440, 539), (663, 275))
Cm(е) = ((425, 663), (638, 131))
Cm(р) = ((16, 416), (228, 480))
Cm(п) = ((440, 539), (329, 447))
Cm(е) = ((283, 493), (463, 736))
Cm(л) = ((188, 93), (688, 741))

Cm(и) = ((440, 539), (407, 669))

Cm(в) = ((596, 433), (6, 218))

Cm(о) = ((568, 355), (561, 140))

2 Расшифрование криптограммы на основе эллиптических кривых

Цель работы - дан шифртекст, используя алфавит, приведённый в учебно-методическо пособии к выполнению лабораторного практикума по дисциплине «Криптография» в подразделе «Задачи к лабораторным работам по криптографии на эллиптических кривых (используется кривая $E751(-1,1)$ и генерирующая точка $G = (0,1)$» и зная секретный ключ n_b, найти открытый текст.

Номер варианта	7
Секретный ключ	12
Шифртекст	{(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)}

$$P_m + k \cdot P_b - n_b \cdot (kG) = (128, 672) - 12 \cdot (16, 416) = (128, 672) + (519, 38) = (236, 39)$$

$$\lambda = \frac{38 - 672}{519 - 128} = \frac{-634}{391} = -634 \cdot 391^{-1} \mod 751 = 117 \cdot 315 \mod 751 = 56 \mod 751$$

$$x = 56^2 - 128 - 519 \mod 751 = 236 \mod 751$$

$$y = 56 \cdot (128 - 236) - 672 \mod 751 = 39 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (59, 386) - 12 \cdot (56, 419) = (59, 386) + (499, 595) = (235, 732)$$

$$\lambda = \frac{595 - 386}{499 - 59} = \frac{209}{440} = 209 \cdot 440^{-1} \mod 751 = 209 \cdot 425 \mod 751 = 207 \mod 751$$

$$x = 207^2 - 59 - 499 \mod 751 = 235 \mod 751$$

$$y = 207 \cdot (59 - 235) - 386 \mod 751 = 732 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (106, 24) - 12 \cdot (425, 663) = (106, 24) + (750, 750) = (229, 600)$$

$$\lambda = \frac{750 - 24}{750 - 106} = \frac{726}{644} = 726 \cdot 644^{-1} \mod 751 = 726 \cdot 379 \mod 751 = 288 \mod 751$$
$$x = 288^2 - 106 - 750 \mod 751 = 229 \mod 751$$
$$y = 288 \cdot (106 - 229) - 24 \mod 751 = 600 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (145, 608) - 12 \cdot (568, 355) = (145, 608) + (406, 397) = (240, 309)$$

$$\lambda = \frac{397 - 608}{406 - 145} = \frac{-211}{261} = -211 \cdot 261^{-1} \mod 751 = 540 \cdot 446 \mod 751 = 520 \mod 75$$
$$x = 520^2 - 145 - 406 \mod 751 = 240 \mod 751$$
$$y = 520 \cdot (145 - 240) - 608 \mod 751 = 309 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (279, 398) - 12 \cdot (188, 93) = (279, 398) + (327, 643) = (247, 266)$$

$$\lambda = \frac{643 - 398}{327 - 279} = \frac{245}{48} = 245 \cdot 48^{-1} \mod 751 = 245 \cdot 266 \mod 751 = 584 \mod 751$$
$$x = 584^2 - 279 - 327 \mod 751 = 247 \mod 751$$
$$y = 584 \cdot (279 - 247) - 398 \mod 751 = 266 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (99, 295) - 12 \cdot (425, 663) = (99, 295) + (750, 750) = (240, 309)$$

$$\lambda = \frac{750 - 295}{750 - 99} = \frac{455}{651} = 455 \cdot 651^{-1} \mod 751 = 455 \cdot 383 \mod 751 = 33 \mod 751$$
$$x = 33^2 - 99 - 750 \mod 751 = 240 \mod 751$$
$$y = 33 \cdot (99 - 240) - 295 \mod 751 = 309 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (269, 187) - 12 \cdot (179, 275) = (269, 187) + (116, 659) = (229, 151)$$

$$\lambda = \frac{659 - 187}{116 - 269} = \frac{472}{-153} = 472 \cdot -153^{-1} \mod 751 = 472 \cdot 697 \mod 751 = 46 \mod 751$$
$$x = 46^2 - 269 - 116 \mod 751 = 229 \mod 751$$
$$y = 46 \cdot (269 - 229) - 187 \mod 751 = 151 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (395, 337) - 12 \cdot (188, 93) = (395, 337) + (327, 643) = (237, 454)$$

$$\lambda = \frac{643 - 337}{327 - 395} = \frac{306}{-68} = 306 \cdot -68^{-1} \mod 751 = 306 \cdot 254 \mod 751 = 371 \mod 751$$
$$x = 371^2 - 395 - 327 \mod 751 = 237 \mod 751$$
$$y = 371 \cdot (395 - 237) - 337 \mod 751 = 454 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (311, 68) - 12 \cdot (188, 93) = (311, 68) + (327, 643) = (234, 587)$$

$$\lambda = \frac{643 - 68}{327 - 311} = \frac{575}{16} = 575 \cdot 16^{-1} \mod 751 = 575 \cdot 47 \mod 751 = 740 \mod 751$$
$$x = 740^2 - 311 - 327 \mod 751 = 234 \mod 751$$
$$y = 740 \cdot (311 - 234) - 68 \mod 751 = 587 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (556, 484) - 12 \cdot (135, 82) = (556, 484) + (135, 82) = (238, 576)$$

$$\lambda = \frac{82 - 484}{135 - 556} = \frac{-402}{-421} = 402 \cdot 421^{-1} \mod 751 = 402 \cdot 685 \mod 751 = 504 \mod 751$$
$$x = 504^2 - 556 - 135 \mod 751 = 238 \mod 751$$
$$y = 504 \cdot (556 - 238) - 484 \mod 751 = 576 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (106, 727) - 12 \cdot (56, 419) = (106, 727) + (499, 595) = (236, 39)$$

$$\lambda = \frac{595 - 727}{499 - 106} = \frac{-132}{393} = -132 \cdot 393^{-1} \mod 751 = 619 \cdot 279 \mod 751 = 722 \mod 75$$
$$x = 722^2 - 106 - 499 \mod 751 = 236 \mod 751$$
$$y = 722 \cdot (106 - 236) - 727 \mod 751 = 39 \mod 751$$

$$P_m + k \cdot P_b - n_b \cdot (kG) = (307, 693) - 12 \cdot (16, 416) = (307, 693) + (519, 38) = (234, 587)$$

$$\lambda = \frac{38 - 693}{519 - 307} = \frac{-655}{212} = -655 \cdot 212^{-1} \mod 751 = 96 \cdot 542 \mod 751 = 213 \mod 751$$
$$x = 213^2 - 307 - 519 \mod 751 = 234 \mod 751$$
$$y = 213 \cdot (307 - 234) - 693 \mod 751 = 587 \mod 751$$

Точка	Буква
(236, 39)	и
(235, 732)	з
(229, 600)	г
(240, 309)	о
(247, 266)	т
(240, 309)	о
(229, 151)	в
(237, 454)	л
(234, 587)	е
(238, 576)	н
(236, 39)	и
(234, 587)	е

3 Расчёт точки 2P + 3Q – R на эллиптической кривой

Цель работы: Даны точки P,Q, R на эллиптической кривой $E751(-1,1)$. Найти точку $2P + 3Q–R$.

Номер варианта	7
P	(74, 170)
Q	(53, 277)
R	(86, 25)

Вычисляем $2P$

$$\lambda = \frac{3 \cdot 74^2 + (-1)}{2 \cdot 170} = \frac{16427}{340} = 16427 \cdot 340^{-1} = 656 \cdot 550 \mod 751 = 320 \mod 751$$
$$x = 320^2 - 74 - 74 \mod 751 = 116 \mod 751$$
$$y = 320 \cdot (74 - 116) - 170 \mod 751 = 659 \mod 751$$

$$2P = (116, 659)$$

Вычисляем $2Q$

$$\lambda = \frac{3 \cdot 53^2 + (-1)}{2 \cdot 277} = \frac{8426}{554} = 8426 \cdot 554^{-1} = 165 \cdot 690 \mod 751 = 449 \mod 751$$
$$x = 449^2 - 53 - 53 \mod 751 = 227 \mod 751$$
$$y = 449 \cdot (53 - 227) - 277 \mod 751 = 452 \mod 751$$

$$2Q = (227, 452)$$

Вычисляем $3Q$

$$\lambda = \frac{277 - 452}{53 - 227} = \frac{-175}{-174} = 175 \cdot 174^{-1} \mod 751 = 175 \cdot 669 \mod 751 = 670 \mod 751$$
$$x = 670^2 - 227 - 53 \mod 751 = 273 \mod 751$$
$$y = 670 \cdot (227 - 273) - 452 \mod 751 = 270 \mod 751$$

$$3Q = (273, 270)$$

Вычисляем $2P + 3Q$

$$\lambda = \frac{270 - 659}{273 - 116} = \frac{-389}{157} = -389 \cdot 157^{-1} \mod 751 = 362 \cdot 464 \mod 751 = 495 \mod 75$$
$$x = 495^2 - 116 - 273 \mod 751 = 561 \mod 751$$
$$y = 495 \cdot (116 - 561) - 659 \mod 751 = 611 \mod 751$$

$$2P + 3Q = (561, 611)$$

Вычисляем $2P + 3Q - R$

$$\lambda = \frac{726 - 611}{86 - 561} = \frac{115}{-475} = 115 \cdot -475^{-1} \mod 751 = 115 \cdot 634 \mod 751 = 63 \mod 751$$
$$x = 63^2 - 561 - 86 \mod 751 = 318 \mod 751$$
$$y = 63 \cdot (561 - 318) - 611 \mod 751 = 429 \mod 751$$

$$2P + 3Q - R = (318, 429)$$

4 Расчет точки nP на эллиптической кривой

Цель работы: дана точка P на эллиптической кривой $E751(-1,1)$ и натуральное число n. Найти точку nP.

Вариант	7
P	(39, 580)
n	109

$$109_{10} = 1101101_2$$

$$n \cdot P = 109 \cdot P = p + 4 \cdot P + 8 \cdot P + 32 \cdot P + 64 \cdot P$$

Найдём $2P$

$2 \cdot P = 1 \cdot P + 1 \cdot P = (39, 580) + (39, 580) = (156, 704) \mod 751$

$$\lambda = \frac{3 \cdot 39^2 + (-1)}{2 \cdot 580} = \frac{4562}{1160} = 4562 \cdot 1160^{-1} = 56 \cdot 213 \mod 751 = 663 \mod 751$$

$$x = 663^2 - 39 - 39 \mod 751 = 156 \mod 751$$

$$y = 663 \cdot (39 - 156) - 580 \mod 751 = 704 \mod 751$$

Найдём $4P$

$4 \cdot P = 2 \cdot P + 2 \cdot P = (156, 704) + (156, 704) = (157, 576) \mod 751$

$$\lambda = \frac{3 \cdot 156^2 + (-1)}{2 \cdot 704} = \frac{73007}{1408} = 73007 \cdot 1408^{-1} = 160 \cdot 743 \mod 751 = 222 \mod 751$$

$$x = 222^2 - 156 - 156 \mod 751 = 157 \mod 751$$

$$y = 222 \cdot (156 - 157) - 704 \mod 751 = 576 \mod 751$$

Найдём $8P$

$8 \cdot P = 4 \cdot P + 4 \cdot P = (157, 576) + (157, 576) = (327, 108) \mod 751$

$$\lambda = \frac{3 \cdot 157^2 + (-1)}{2 \cdot 576} = \frac{73946}{1152} = 73946 \cdot 1152^{-1} = 348 \cdot 324 \mod 751 = 102 \mod 751$$

$$x = 102^2 - 157 - 157 \mod 751 = 327 \mod 751$$

$$y = 102 \cdot (157 - 327) - 576 \mod 751 = 108 \mod 751$$

Найдём $16P$

$16 \cdot P = 8 \cdot P + 8 \cdot P = (327, 108) + (327, 108) = (519, 713) \mod 751$

$$\lambda = \frac{3 \cdot 327^2 + (-1)}{2 \cdot 108} = \frac{320786}{216} = 320786 \cdot 216^{-1} = 109 \cdot 226 \mod 751 = 602 \mod 751$$
$$x = 602^2 - 327 - 327 \mod 751 = 519 \mod 751$$
$$y = 602 \cdot (327 - 519) - 108 \mod 751 = 713 \mod 751$$

Найдём $32P$

$32 \cdot P = 16 \cdot P + 16 \cdot P = (519, 713) + (519, 713) = (425, 663) \mod 751$

$$\lambda = \frac{3 \cdot 519^2 + (-1)}{2 \cdot 713} = \frac{808082}{1426} = 808082 \cdot 1426^{-1} = 6 \cdot 583 \mod 751 = 494 \mod 751$$
$$x = 494^2 - 519 - 519 \mod 751 = 425 \mod 751$$
$$y = 494 \cdot (519 - 425) - 713 \mod 751 = 663 \mod 751$$

Найдём $64P$

$64 \cdot P = 32 \cdot P + 32 \cdot P = (425, 663) + (425, 663) = (377, 456) \mod 751$

$$\lambda = \frac{3 \cdot 425^2 + (-1)}{2 \cdot 663} = \frac{541874}{1326} = 541874 \cdot 1326^{-1} = 403 \cdot 64 \mod 751 = 258 \mod 751$$
$$x = 258^2 - 425 - 425 \mod 751 = 377 \mod 751$$
$$y = 258 \cdot (425 - 377) - 663 \mod 751 = 456 \mod 751$$

Найдём $64P + 32P = 96P$

$96 \cdot P = 64 \cdot P + 32 \cdot P = (377, 456) + (425, 663) = (745, 210) \mod 751$

$$\lambda = \frac{663 - 456}{425 - 377} = \frac{207}{48} = 207 \cdot 48^{-1} \mod 751 = 207 \cdot 266 \mod 751 = 239 \mod 751$$
$$x = 239^2 - 377 - 425 \mod 751 = 745 \mod 751$$
$$y = 239 \cdot (377 - 745) - 456 \mod 751 = 210 \mod 751$$

Найдём $96P + 8P = 104P$

$104 \cdot P = 96 \cdot P + 8 \cdot P = (745, 210) + (327, 108) = (616, 400) \mod 751$

$$\lambda = \frac{108 - 210}{327 - 745} = \frac{-102}{-418} = 102 \cdot 418^{-1} \mod 751 = 102 \cdot 645 \mod 751 = 453 \mod 751$$
$$x = 453^2 - 745 - 327 \mod 751 = 616 \mod 751$$
$$y = 453 \cdot (745 - 616) - 210 \mod 751 = 400 \mod 751$$

Найдём $104P + 4P = 108P$

$108 \cdot P = 104 \cdot P + 4 \cdot P = (616, 400) + (157, 576) = (589, 429) \mod 751$

$$\lambda = \frac{576 - 400}{157 - 616} = \frac{176}{-459} = 176 \cdot -459^{-1} \mod 751 = 176 \cdot 733 \mod 751 = 587 \mod 75$$
$$x = 587^2 - 616 - 157 \mod 751 = 589 \mod 751$$
$$y = 587 \cdot (616 - 589) - 400 \mod 751 = 429 \mod 751$$

Найдём $108P + 1P = 109P$

$109 \cdot P = 108 \cdot P + 1 \cdot P = (589, 429) + (39, 580) = (509, 341) \mod 751$

$$\lambda = \frac{580 - 429}{39 - 589} = \frac{151}{-550} = 151 \cdot -550^{-1} \mod 751 = 151 \cdot 411 \mod 751 = 479 \mod 75$$
$$x = 479^2 - 589 - 39 \mod 751 = 509 \mod 751$$
$$y = 479 \cdot (589 - 509) - 429 \mod 751 = 341 \mod 751$$

Результат $109P = (509, 341)$

5 Получение ЭЦП на основе эллиптических кривых

Цель работы: сгенерировать ЭЦП для сообщения с известным значением хэш-свертки e, зная секретный ключ подписи d при данном значении выбираемого случайным образом числа k. Используется эллиптическая кривая $E751(-1,1)$ и генерирующая точка $G = (416, 55)$ порядка $n = 13$.

Вариант	7
e	8
d	5
k	5

Найдём kG = 5*(416, 55).

Найдём 2G.

$2G = G + G = (416, 55) + (416, 55) = (384, 475)$

$$\lambda = \frac{3 \cdot 416^2 + (-1)}{2 \cdot 55} = \frac{519167}{110} = 519167 \cdot 110^{-1} = 226 \cdot 198 \mod 751 = 439 \mod 751$$

$$x = 439^2 - 416 - 416 \mod 751 = 384 \mod 751$$

$$y = 439 \cdot (416 - 384) - 55 \mod 751 = 475 \mod 751$$

Найдём 4G.

$4G = 2G + 2G = (384, 475) + (384, 475) = (455, 383)$

$$\lambda = \frac{3 \cdot 384^2 + (-1)}{2 \cdot 475} = \frac{442367}{950} = 442367 \cdot 950^{-1} = 28 \cdot 434 \mod 751 = 136 \mod 751$$

$$x = 136^2 - 384 - 384 \mod 751 = 455 \mod 751$$

$$y = 136 \cdot (384 - 455) - 475 \mod 751 = 383 \mod 751$$

Найдём 5G.

$5G = 4G + G = (455, 383) + (416, 55) = (562, 662)$

$$\lambda = \frac{55 - 383}{416 - 455} = \frac{-328}{-39} = 328 \cdot 39^{-1} \mod 751 = 328 \cdot 674 \mod 751 = 278 \mod 751$$

$$x = 278^2 - 455 - 416 \mod 751 = 562 \mod 751$$

$$y = 278 \cdot (455 - 562) - 383 \mod 751 = 662 \mod 751$$

Найдём $r = x \mod n = 562 \mod (13) = 3$.

Найдём $z = k^{-1} \mod (n) = 5^{-1} \mod (13) = 8$.

Найдём $s = z \cdot (e + d \cdot r) \mod (n) = 8 \cdot (3 + 5 \cdot 3) \mod (13) = 2$.

Цифровая подпись: $(r,s) = (3, 2)$

6 Проверка ЭЦП на основе эллиптических кривых

Цель работы: проверить подлинность ЭЦП (r,s) для сообщения с известным значением хэш-свертки e, зная открытый ключ проверки подписи Q. Используется эллиптическая кривая $E751(-1,1)$ и генерирующая точка $G = (562, 89)$ порядка $n = 13$.

Вариант	7
e	4
Q	(384, 475)
(r, s)	(11, 9)

Проверка подписи начинается с проверки условий $1 \leqslant r \leqslant n{-}1, 1 \leqslant s \leqslant n{-}1$.

$1 \leqslant 11 \leqslant 12, 1 \leqslant 9 \leqslant 12$.

Вычисляем $v = s^{-1} \mod (n) = 9^{-1} \mod (13) = 3$

Вычисляем $u_1 = e \cdot v \mod (n) = 4 \cdot 3 \mod (13) = 12$

Вычисляем $u_2 = s \cdot v \mod (n) = 9 \cdot 3 \mod (13) = 1$

Находим точку $X = u_1 \cdot G + u_2 \cdot Q = 12 \cdot (562, 89) + 1 \cdot (384, 475)$

Найдем $2G = 1 * G + 1 * G = (562, 89) + (562, 89) = (135, 669)$

$$\lambda = \frac{3 \cdot 562^2 + (-1)}{2 \cdot 89} = \frac{947531}{178} = 947531 \cdot 178^{-1} = 520 \cdot 308 \mod 751 = 197 \mod 751$$

$$x = 197^2 - 562 - 562 \mod 751 = 135 \mod 751$$

$$y = 197 \cdot (562 - 135) - 89 \mod 751 = 669 \mod 751$$

Найдем $4G = 2 * G + 2 * G = (135, 669) + (135, 669) = (596, 318)$

$$\lambda = \frac{3 \cdot 135^2 + (-1)}{2 \cdot 669} = \frac{54674}{1338} = 54674 \cdot 1338^{-1} = 602 \cdot 87 \mod 751 = 555 \mod 751$$

$$x = 555^2 - 135 - 135 \mod 751 = 596 \mod 751$$

$$y = 555 \cdot (135 - 596) - 669 \mod 751 = 318 \mod 751$$

Найдем $8G = 4 * G + 4 * G = (596, 318) + (596, 318) = (416, 696)$

$$\lambda = \frac{3 \cdot 596^2 + (-1)}{2 \cdot 318} = \frac{1065647}{636} = 1065647 \cdot 636^{-1} = 729 \cdot 431 \mod 751 = 281 \mod 75$$

$$x = 281^2 - 596 - 596 \mod 751 = 416 \mod 751$$

$$y = 281 \cdot (596 - 416) - 318 \mod 751 = 696 \mod 751$$

Найдем $12G = 4 * G + 8 * G = (596, 318) + (416, 696) = (562, 662)$

$$\lambda = \frac{696 - 318}{416 - 596} = \frac{378}{-180} = 378 \cdot -180^{-1} \mod 751 = 378 \cdot 630 \mod 751 = 73 \mod 751$$

$$x = 73^2 - 596 - 416 \mod 751 = 562 \mod 751$$

$$y = 73 \cdot (596 - 562) - 318 \mod 751 = 662 \mod 751$$

X = (596, 433)

Сравниваем значения r и $x \mod n$, если они совпадают, следовательно, подпись действительная.

$$r = 11$$

$$x \mod n = 11$$

Значия совпадают, следовательно, подпись действительная.