Контрольная работа по дисциплине
„Методы алгебраической геометрии в криптографии"
Студентки 531 группы Швецовой Елизаветы. Вариант 18

Задана эл. кривая $E: y^2 = x^3 + ax + b$ над полем $F_{11}$, где
$a = b \pmod 9) + 1 = 18 \pmod 9) + 1 = 1$, $b = 18 \equiv 7 \pmod{11})$

т. о. $E: y^2 = x^3 + x + 7$

1) Найти порядок $N$ эл. кривой $E$, а также все её точки

| $y$ | $y^2$ |
|---|---|
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 3 | 9 |
| 4 | 5 |
| 5 | 3 |
| 6 | 3 |
| 7 | 5 |
| 8 | 9 |
| 9 | 4 |
| 10 | 1 |

| $x$ | $x^3+x+7$ | $y$ | $\frac{x^3+x+7}{11}$ |
|---|---|---|---|
| 0 | 7 | – | −1 |
| 1 | 9 | 3,8 | 1 |
| 2 | 6 | – | −1 |
| 3 | 4 | 2,9 | 1 |
| 4 | 9 | 3,8 | 1 |
| 5 | 5 | 4,7 | 1 |
| 6 | 9 | 3,8 | 1 |
| 7 | 5 | 4,7 | 1 |
| 8 | 10 | – | −1 |
| 9 | 8 | – | −1 |
| 10 | 5 | 4,7 | 1 |

Получ. т-ки эл. кр.:

$\theta$, (1,3), (1,8), (3,2), (3,9), (4,3), (4,8), (5,4), (5,7), (6,3), (6,8), (7,4), (7,7), (10,4), (10,7)

$N = 0+2+0+2+2+2+2+2+0+0+2+1 = 15$

2) Для эл. кривой вычисл. $kP$, $1 < k < 5$, где $P$ – $N \pmod 9$ точка. $N \pmod 9) = 15 \pmod 9) = 6 \Rightarrow P = (4,3)$

По следствию из теоремы 1.15 будем исп-ть ф-лы:

$$\begin{cases} \lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1}, & \text{если } x_1 = x_2 \\ \dfrac{y_1 - y_2}{x_1 - x_2}, & \text{если } x_1 \neq x_2 \end{cases} \\ x_3 = -x_1 - x_2 + \lambda^2 \\ y_3 = -y_1 + \lambda(x_1 - x_3) \end{cases}$$

$2P = P + P = (4,3) + (4,3)$ $\quad \lambda = \frac{3 \cdot 4^2 + 1}{2 \cdot 3} = \frac{49}{6} \pmod{11} = 10$

$x_3 = -4 - 4 + 10^2 = 92 \pmod{11} = 4$

$y_3 = -3 + 10(4-4) = 8$

$2P = (4,8)$

$3P = 2P + P = (4,8) + (4,3) \overset{*}{=}$ $\quad \lambda = \frac{8-3}{4-4}$ – знаменатель 0 $\Rightarrow$

$\Rightarrow 3P = \theta$

* так же по св-во 3 из т-мы 1.15 * $-P + P = \theta$

$2P+2P = 3P+P$

$3P+P = \mathcal{O}+P = P = (4,3)$

$2P+2P = (4,8)+(4,8)$ $\quad \lambda = \frac{3\cdot 4^2+1}{2\cdot 8} = \frac{49}{16} \pmod{11} = 1$

$x_3 = -4-4+1 = -7 \pmod{11} = 4$

$y_3 = -8+1(4-4) = -8 \pmod{11} = 3$ $\quad 2P+2P = (4,3)$

$4P = (4,3)$

3) Для эл кривой E и миним порожд т. B найдите публичный ключ для криптосист Эль-Гамаля, зная что секр кл $a_k = 4$.

Для нахожд B рассчитаем порядки точек, т.е. такое миним n, что $n\cdot P = \mathcal{O}$

• $P=(1,3)$: $\quad 2(1,3) = (1,3)+(1,3)$ $\quad \lambda = \frac{3\cdot 1^2+1}{2\cdot 3} = \frac{4}{6} \pmod{11} = 8$

$x_3 = -1-1+8^2 = 62 \pmod{11} = 7$ $\quad 2P = (7,4)$

$y_3 = -3+8(\overset{-6}{1-7}) = -51 \pmod{11} = 4$

$3P = 2P+P = (7,4)+(1,3)$ $\quad \lambda = \frac{4-3}{7-1} = \frac{1}{6} \pmod{11} = 2$

$x_3 = -7-1+4 = -4 \pmod{11} = 7$ $\quad 3P = (7,7)$

$y_3 = -4+2(\overset{0}{7-7}) = 7$

$4P = 3P+P = (7,7)+(1,3)$ $\quad \lambda = \frac{7-3}{7-1} = \frac{4}{6} \pmod{11} = 8$

$x_3 = -7-1+8^2 = 56 \pmod{11} = 1$ $\quad 4P = (1,8)$

$y_3 = -7+8(\overset{6}{7-1}) = 41 \pmod{11} = 8$

$5P = 4P+P = (1,8)+(1,3) \overset{св}{=} \mathcal{O}$

Порядок (1,3) равен 5

• $P=(1,8)$: $\quad 2(1,8) = (1,8)+(1,8)$ $\quad \lambda = \frac{3\cdot 1^2+1}{2\cdot 8} = \frac{4}{16} \pmod{11} = 3$

$x^3 = -1-1+3^2 = 7$ $\quad 2P = (7,7)$

$y^3 = -8+3(1-7) = 7$

$3P = 2P+P = (7,7)+(1,8)$ $\quad \lambda = \frac{7-8}{7-1} = \frac{-1}{6} \pmod{11} = 9$

$x^3 = -7-1+9^2 = 73 \pmod{11} = 7$ $\quad 3P = (7,4)$

$y^3 = -7+9(7-7) = -7 \pmod{11} = 4$

$4P = 3P+P = (7,4)+(1,8)$ $\quad \lambda = \frac{4-8}{7-1} = \frac{-4}{6} \pmod{11} = 3$

$x^3 = -7-1+9 = 1$ $\quad y^3 = -4+3(7-1) = 14 \pmod{11} = 3$ $\quad 4P = (1,3)$

$5P = (1,3) + (1,8) \overset{\text{св}}{=} O$

Порядок $(1,8)$ равен 5

- $P = (3,2)$: $2P = (3,2) + (3,2)$ $\quad \lambda = \frac{3 \cdot 3^2 + 1}{2 \cdot 2} = \frac{28}{4} \pmod{11}$

$x_3 = -3 - 3 + 7^2 = 43 \pmod{11} = 10$

$y_3 = -2 + 7(3 - 10) = -51 \pmod{11} = 4$ $\quad \underline{2P = (10,4)}$

$3P = 2P + P = (10,4) + (3,2)$ $\quad \lambda = \frac{4-2}{10-3} = \frac{2}{7} \pmod{11} = 5$

$x_3 = -10 - 3 + 5^2 = 12 \pmod{11} = 1$

$y_3 = -4 + 5(10 - 1) = 41 \pmod{11} = 8$ $\quad \underline{3P = (1,8)}$

$4P = 3P + P = (1,8) + (3,2)$ $\quad \lambda = \frac{8-2}{1-3} = \frac{6}{-2} \pmod{11} = 8$

$x_3 = -1 - 3 + 8^2 = 60 \pmod{11} = 5$

$y_3 = -8 + 8(1 - 5) = -40 \pmod{11} = 4$ $\quad \underline{4P = (5,4)}$

$5P = 4P + P = (5,4) + (3,2)$ $\quad \lambda = \frac{4-2}{5-3} = \frac{2}{2} \pmod{11} = 1$

$x_3 = -5 - 3 + 1^2 = -7 \pmod{11} = 4$

$y_3 = -4 + 1(5 - 4) = -3 \pmod{11} = 8$ $\quad \underline{5P = (4,8)}$

$6P = 5P + P = (4,8) + (3,2)$ $\quad \lambda = \frac{6}{1} \pmod{11} = 6$

$x_3 = -4 - 3 + 6^2 = 29 \pmod{11} = 7$

$y_3 = -8 + 6(4 - 7) = -26 \pmod{11} = 7$ $\quad \underline{6P = (7,7)}$

$7P = 6P + P = (7,7) + (3,2)$ $\quad \lambda = \frac{5}{4} \pmod{11} = 4$

$x_3 = -7 - 3 + 4^2 = 6$

$y_3 = -7 + 4(7 - 6) = -3 \pmod{11} = 8$ $\quad \underline{7P = (6,8)}$

$8P = 7P + P = (6,8) + (3,2)$ $\quad \lambda = \frac{6}{3} = 2$

$x_3 = -6 - 3 + 4 = -5 \pmod{11} = 6$

$y_3 = -8 + 2(6 - 6) = -8 \pmod{11} = 3$ $\quad \underline{8P = (6,3)}$

$9P = 8P + P = (6,3) + (3,2)$ $\quad \lambda = \frac{1}{3} \pmod{11} = 4$

$x_3 = -6 - 3 + 4^2 = 7$

$y_3 = -3 + 4(6 - 7) = -7 \pmod{11} = 4$ $\quad \underline{9P = (7,4)}$

$10P = (7,4) + (3,2)$ $\quad \lambda = \frac{2}{4} \pmod{11} = 6$

$x_3 = -7 - 3 + 6^2 = 26 \pmod{11} = 4$

$y_3 = -4 + 6(7 - 4) = 14 \pmod{11} = 3$ $\quad \underline{10P = (4,3)}$

$10P+P=(4,3)+(3,2)$  $\lambda=\frac{1}{1}=1$

$x_3=-4-3+1=-6 \pmod{11}=5$

$y_3=-3+1(4-5)=-4 \pmod{11}=7$  $11P=(5,7)$

$P=11P+P=(5,7)+(3,2)$  $\lambda=\frac{5}{2} \pmod{11}=8$

$x_3=-5-3+8^2=56 \pmod{11}=1$  $12P=(1,3)$

$y_3=-7+8(5-1)=25 \pmod{11}=3$

$13P=12P+P=(1,3)+(3,2)$  $\lambda=\frac{1}{-2} \pmod{11}=5$

$x_3=-1-3+5^2=21 \pmod{11}=10$

$y_3=-3+5(1-10)=-48 \pmod{11}=7$  $13P=(10,7)$

$14P=13P+P=(10,7)+(3,2)$  $\lambda=\frac{5}{7} \pmod{11}=7$

$x_3=-10-3+7^2=3$  $14P=(3,9)$

$y_3=-7+7(10-3)=42 \pmod{11}=9$

$15P=14P+P=(3,9)+(3,2)=\theta$

Порядок точки (3,2) = 15 $\Rightarrow$ (3,2) – наименьшая пор. т.к. мы вычисляем т в отсортир порядке и при начали др порядок т. они будут не минимальны

Т.о. $B=(3,2)$

Публичн. ключом в криптосистеме Эль-Гамаля для базов т. $B$ кривой $E$ над полем $F_q$ явл. т. $a_k \cdot B$, где $a_k$ – секр кл

Т.о. $a_k \cdot B = 4\cdot(3,2)=(5,4)$ – публичный ключ.

4) Исп $E: y^2=x^3+x+7$, точку $B=(3,2)$, секр кл $a_k=4$, случ число $k=8$

а) Зашифруйте сообщ. $M=10$.

- Для зашифров. сопост. ему в соотв т. (6,3) кр $E$
- Выберем $a_k$ ($a_k=4$ по условию) и найдем $a_k B=(5,4)$ (зад 3)
- Для $k=8$ опр $k a_k B = 8(5,4)$

$2P=P+P=(5,4)+(5,4)$  $\lambda=\frac{3\cdot5^2+1}{2\cdot4}=\frac{76}{8} \pmod{11}=4$

$x_3=-5-5+4^2=6$

$y_3=-4+4(5-6)=-8 \pmod{11}=3$  $2P=(6,3)$

$4P=2P+2P=(6,3)+(6,3)=$  $\lambda=\frac{3\cdot6^2+1}{2\cdot3}=\frac{109}{6} \pmod{11}=9$

$x_3=-6-6+9^2=69 \pmod{11}=3$

$y_3=-3+9(6-3)=24 \pmod{11}=2$  $4P=(3,2)$

$8P = 4P + 4P = (3,2) + (3,2)$ $\quad \lambda = \frac{3 \cdot 3^2 + 1}{2 \cdot 2} = \frac{28}{4} \pmod{11}$

$x_3 = -3 - 3 + 7^2 = 43 \pmod{11} = 10$ $\quad 8P = (10,4)$

$y_4 = -2 + 7(3 - 10) = -51 \pmod{11} = 4$

$\Rightarrow kB = 8 \cdot (5,4) = (10,4)$

- Вычислим сумму $R = M + k \cdot a_k B = (6,3) + (10,4) = (4,3)$

$\lambda = \frac{3-4}{6-10} = \frac{-1}{-4} \pmod{11} = 3$

$x_3 = -6 - 10 + 3^2 = 4$

$y_3 = -3 + 3(6-4) = 3$

Определим $kB = 8 \cdot (3,2) = (6,3)$ (зад 3)

Криптограмма имеет вид $(kB; R) \Rightarrow ((6,3); (4,3))$

б) Расшифруйте получ. криптограмму

- Вычисляем $a_k kB = 4 \cdot (6,3) = (3,2) + (3,2) = (10,4)$

$2 \cdot (6,3) = (6,3) + (6,3)$ $\quad \lambda = 9$

$x_3 = -6 - 6 + 9^2 = 3$

$y_3 = -3 + 9(6-3) = 2$ $\quad 2 \cdot (6,3) = (3,2)$

- Найдем $R - a_k kB = (4,3) - (10,4) = (4,3) + (-(10,4)) = (4,3) + (10,7)$

$\lambda = \frac{3-7}{4-10} = \frac{-4}{-6} = 8$

$x_3 = -4 - 10 + 8^2 = 50 \pmod{11} = 6$

$y_3 = -3 + 8(4-6) = -19 \pmod{11} = 3$

т.о. $R - a_k kB = (6,3)$ – это и есть точка кот мы стави-
ли в соотв сообщ. $M - 10$ в а)