Алексеев А.

Контрольная работа

Вариант 1

Задана эллиптическая кривая $E: y^2 \equiv x^3 + ax + b$ над полем F_{11}, где $a = b \pmod{10} + 1 = 2$, $b = 1$

№1

Найти порядок N эл. кривой $E: y^2 \equiv x^3 + 2x + 1$, а также все ее точки.

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

Для того, чтобы точка принадлежала эл. кривой, необходимо, чтобы символ Лежандра $\left(\frac{y^2}{p}\right) = (y^2)^{\frac{p-1}{2}} \pmod{p} \neq -1$.

x	$y^2 \equiv x^3 + 2x + 1$	$\left(\frac{y^2}{p}\right)$	y
0	1	1	1,10
1	4	1	2,9
2	2	-1	—
3	1	1	1,10
4	7	-1	—
5	4	1	2,9
6	9	1	3,8
7	6	-1	—
8	1	1	1,10
9	0	0	0
10	9	1	3,8

Получили точки эл. кривой: $\{O; (0,1); (0,10); (1,2); (1,9); (3,1); (3,10); (5,2); (5,9); (6,3); (6,8); (8,1); (8,10); (10,3); (10,8); (9,0)\}$.

Порядок эл. кривой N = кол-во точек = 16.

№2

Для эл. кривой $E: y^2 = x^3 + 2x + 1$ вычислить kP, $1 < k < 5$, где $P = 16 \pmod{10} = 6$-я точка

Отсортированные точки: $\{O; (0,1); (0,10); (1,2); (1,9); (3,1); (3,10); (5,2); (5,9); (6,3); (6,8); (8,1); (8,10); (9,0); (10,3); (10,8)\}$.

$= 16 \pmod{10}$

Для сложения точек используем следующие ф-лы:

$$\begin{cases} \lambda = \begin{cases} (3x_1^2 + a)(2y_1)^{-1} \pmod{11}, & \text{если } x_1 = x_2 \text{ и } y_1 = y_2 \\ (y_1 - y_2)(x_1 - x_2)^{-1} \pmod{11}, & \text{если } x_1 \neq x_2 \end{cases} \\ x_3 = \lambda^2 - x_1 - x_2 \pmod{11} \\ y_3 = \lambda(x_1 - x_3) - y_1 \pmod{11} \end{cases}$$

$P = (3,1)$

$2P = P + P = (3,1) + (3,1) = (9,0)$

т.к. $x_1 = x_2$: $\lambda = (3 \cdot 3^2 + 2)(2 \cdot 1)^{-1} \pmod{11} = 29 \cdot 6 \pmod{11} = 9$

$x_3 = 9^2 - 3 - 3 = 75 \pmod{11} = 9$

$y_3 = 9(3 - 9) - 1 = 44 \pmod{11} = 0$

$3P = 2P + P = (9,0) + (3,1) = (3,10)$

т.к. $x_1 \neq x_2$: $\lambda = (0-1)(9-3)^{-1} \pmod{11} = 10 \cdot 2 \pmod{11} = 9$

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

$y_3 = 9(9-3) - 0 = 54 \pmod{11} = 10$

$4P = 3P + P = (3,10) + (3,1) = O$

т.к. $x_1 = x_2$ и $y_1 \neq y_2$, то получаем O

$5P = 4P + P = O + (3,1) = (3,1)$

№3

Для эл. кривой $E: y^2 = x^3 + 2x + 1$ и минимальной порождающей точки B найдите публичный ключ для криптосистемы Эль-Гамаля, зная, что секретный ключ $a_k = 5$

Найдем минимально порождающую точку (т.е. точку B: $n \cdot B = O$ и $n = N = 16$):

$P = (0,1)$

$2P = (0,1) + (0,1) = (1,9)$

т.к. $x_1 = x_2$: $\lambda = (3 \cdot 0^2 + 2) \cdot (2 \cdot 1)^{-1} \pmod{11} = 2 \cdot 6 \pmod{11} = 1$

$x_3 = 1^2 - 0 - 0 \pmod{11} = 1$

$y_3 = 1(0-1) - 1 \pmod{11} = 9$

$3P = 2P + P = (1,9) + (0,1) = (8,1)$

т.к. $x_1 \neq x_2$: $\lambda = (9-1)(1-0)^{-1} \pmod{11} = 8 \cdot 1 \pmod{11} = 8$

$x_3 = 8^2 - 1 - 0 = 63 \pmod{11} = 8$

$y_3 = 8(1-8) - 9 \pmod{11} = 23 \pmod{11} = 1$

$4P = 3P + P = (8,1) + (0,1) = (3,10)$

т.к. $x_1 \neq x_2$: $\lambda = (1-1)(8-0)^{-1} \pmod{11} = 0$

$x_3 = 0^2 - 8 - 0 = -8 \pmod{11} = 3$

$y_3 = 0(8-3) - 1 \pmod{11} = 10$

$5P = 4P + P = (3,10) + (0,1) = (6,3)$

т.к. $x_1 \neq x_2$: $\lambda = (10-1)(3-0)^{-1} \pmod{11} = 9 \cdot 4 \pmod{11} = 3$

$x_3 = 3^2 - 3 - 0 = 6 \pmod{11} = 6$

$y_3 = 3(3-6) - 10 \pmod{11} = -8 \pmod{11} = 3$

$6P = 5P + P = (6,3) + (0,1) = (10,3)$

т.к. $x_1 \neq x_2$: $\lambda = (3-1)(6-0)^{-1} \pmod{11} = 4 \pmod{11} = 4$

$x_3 = 4^2 - 6 - 0 \pmod{11} = 10$

$y_3 = 4(6-10) - 3 \pmod{11} = 3$

$7P = 6P + P = (10,3) + (0,1) = (5,9)$

т.к. $x_1 \neq x_2$: $\lambda = (3-1)(10-0)^{-1} \pmod{11} = 2 \cdot 10 \pmod{11} = 9$

$x_3 = 9^2 - 10 - 0 \pmod{11} = 5$

$y_3 = 9(10-5) - 3 \pmod{11} = 9$

$8P = 7P + P = (5,9) + (0,1) = (9,0)$

т.к. $x_1 \neq x_2$: $\lambda = (9-1)(5-0)^{-1} \pmod{11} = 9$

$x_3 = 6^2 - 5 - 0 \pmod{11} = 9$

$y_3 = 6(5-9) - 9 \pmod{11} = 0$

Далее по теореме Лагранжа: если G конеч. группа и H подгруппа G, то $|H|$ делит $|G|$. Т.к. порядок эл. кривой $N=16$, а порядок $P > 8 \Rightarrow$ порядок $P=16$ и данная точка является порождающей.

Публичный ключ для Эль-Гамаля равен $a_k \cdot B$, где a_k – секретный ключ, B – мин. порождающий эл-т $\Rightarrow$ публичный ключ $= 5 \cdot (0,1) = (6,3)$

№4

Используя эл. кривую $E: y^2 = x^3 + 2x + 1$, точку $B = \overset{(0,1)}{\cancel{(6,3)}}$ из пункта 3), секретный ключ $a=5$, случайное число $k=9$

а) зашифруйте сообщение $M=6$:

1) представим сообщение $M=6$ в виде точки эл. кривой: пусть $M=(6,3)$;

2) найдём $a \cdot B = 5 \cdot (0,1) = (6,3)$;

3) вычислим $k \cdot aB = 9 \cdot (6,3)$:

$2P = P + P = (6,3) + (6,3) = (10,8)$

т.к. $x_1 = x_2$: $\lambda = (3 \cdot 6^2 + 2)(2 \cdot 3)^{-1} \pmod{11} = 0 \cdot 2 \pmod{11} = 0$

$x_3 = 0^2 - 6 - 6 \pmod{11} = 10$

$y_3 = 0(6-1) - 3 \pmod{11} = 8$

$4P = 2P + 2P = (10,8) + (10,8) = (3,10)$

т.к. $x_1 = x_2$: $\lambda = (3 \cdot 10^2 + 2)(2 \cdot 8)^{-1} \pmod{11} = 5 \cdot 9 \pmod{11} = 1$

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

$y_3 = 1(10-3) - 8 \pmod{11} = 10$

$8P = 4P + 4P = (3,10) + (3,10) = (9,0)$

т.к. $x_1 = x_2$: $\lambda = (3 \cdot 3^2 + 2)(2 \cdot 10)^{-1} \pmod{11} = 7 \cdot 5 \pmod{11} = 2$

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

$y_3 = 2(3-9) - 10 \pmod{11} = 0$

$9P = 8P + P = (9,0) + (6,3) = (8,10)$

т.к. $x_1 \neq x_2$: $\lambda = (0-3)(9-6)^{-1} \pmod{11} = 8 \cdot 4 \pmod{11} = 10$

$x_3 = 10^2 - 9 - 6 \pmod{11} = 8$

$y_3 = 10(9-8) - 0 \pmod{11} = 10$

Таким образом, $k \cdot aB = 9 \cdot (6,3) = (8,10)$;

4) вычислим $R = M + k \cdot aB = (6,3) + (8,10) = (1,9)$

т.к. $x_1 \neq x_2$: $\lambda = (3-10)(6-8)^{-1} \pmod{11} = 4 \cdot 5 \pmod{11} = 9$

$x_3 = 9^2 - 6 - 8 \pmod{11} = 1$

$y_3 = 9(6-1) - 3 \pmod{11} = 9$

5) вычислим $kB = 9 \cdot (0,1) = (9,0) + (0,1) = (5,2)$

т.к. $x_1 \neq x_2$: $\lambda = (0-1)(9-0)^{-1} \pmod{11} = 10 \cdot 5 \pmod{11} = 6$

$x_3 = 6^2 - 9 - 0 \pmod{11} = 5$

$y_3 = 6(9-5) - 0 \pmod{11} = 2$

Таким образом, получили криптограмму $(kB; R) = ((5,2),(1,9))$;

б) расшифруйте полученную криптограмму

1) вычислим $a \cdot kB = 5 \cdot (5,2) = (8,10)$

$P = (5,2)$

$2P = P + P = (5,2) + (5,2) = (1,9)$

т.к. $x_1 = x_2$: $\lambda = (3 \cdot 5^2 + 2)(2 \cdot 2)^{-1} \pmod{11} = 0 \cdot 3 \pmod{11} = 0$

$x_3 = 0^2 - 5 - 5 \pmod{11} = 1$

$y_3 = 0(5-1) - 2 \pmod{11} = 9$

$4P = 2P + 2P = (1,9) + (1,9) = (3,10)$

т.к. $x_1 = x_2$: $\lambda = (3 \cdot 1^2 + 2) \cdot (2 \cdot 9)^{-1} \pmod{11} = 5 \cdot 8 \pmod{11} = 7$

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

$y_3 = 7(1-3) - 9 \pmod{11} = 10$

Продолжение на листке внутри...

Начало на листке снаружи

$5P = 4P + P = (3,10) + (5,2) = (8,10)$

т.к. $x_1 \neq x_2$: $\lambda = (10-2)(3-5)^{-1} \pmod{11} = 8 \cdot 5 \pmod{11} = 7$

$x_3 = 7^2 - 3 - 5 \pmod{11} = 8$

$y_3 = 7(3-8) - 10 \pmod{11} = 10$

2) вычтем результат из 2-й точки в паре:

$(1,9) - (8,10) = (1,9) + (8,-10) = (1,9) + (8,1) = (6,3)$

т.к. $x_1 \neq x_2$: $\lambda = (9-1)(1-8)^{-1} \pmod{11} = 8 \cdot 3 \pmod{11} = 2$

$x_3 = 2^2 - 1 - 8 \pmod{11} = 6$

$y_3 = 2(1-6) - 9 \pmod{11} = 3$

Таким образом, получили точку (6,3), которая соответствует сообщению $M = 6$.