Построение эллиптических кривых

Уравнение: $y^2 = x^3 + ax + b$

Пусть a = 2, b = 4

Пусть p = 5 => $Z_p = Z_5$

Тогда уравнение будет $y^2 = x^3 + 2x + 4$

Проверим:

$(4a^3 + 27b^2) \pmod p = (4 * 2^3 + 27 * 4^2) \pmod 5 = (4 * 8 + 27 * 16) \pmod 5 = 4$
4 != 0 => у кривой нет самопересечений и острых углов

Вычисляем точки E:

X = 0 => $z = x^3 + 2x + 4 \pmod 5 = 4 \bmod 5 = 4$

X = 1 => $z = x^3 + 2x + 4 \pmod 5 = 1 + 2 + 4 \bmod 5 = 7 \bmod 5 = 2$

X = 2 => $z = x^3 + 2x + 4 \pmod 5 = 8 + 4 + 4 \bmod 5 = 16 \bmod 5 = 1$

X = 3 => $z = x^3 + 2x + 4 \pmod 5 = 27 + 6 + 4 \bmod 5 = 37 \bmod 5 = 2$

X = 4 => $z = x^3 + 2x + 4 \pmod 5 = 64 + 8 + 4 \bmod 5 = 76 \bmod 5 = 1$

Находим такие x, что $y^2 = z \bmod 5$

Для z = 4, $y^2 = 4 \bmod 5$

$0^2 \bmod 5 = 0$

$1^2 \bmod 5 = 1$

$2^2 \bmod 5 = 4$

$3^2 \bmod 5 = 4$

$4^2 \bmod 5 = 1$

Решения: 2, 3

Для $z = 2$, $y^2 = 2 \bmod 5$

Решения: ~~0~~

Для $z = 1$, $y^2 = 1 \bmod 5$

Решения: 1, 4

X	Z	Y
0	4	2, 3
1	2	-
2	1	1, 4
3	2	-
4	1	1, 4

Получаем 6 точек: (0, 2), (0, 3), (2, 1), (2, 4), (4, 1), (4, 4)

Вычисляем степени a

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{dacă } P \neq Q \\[2ex] \dfrac{3 * x_1^2 + a}{2 * y_1}, & \text{dacă } P = Q \end{cases}$$

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda (x_1 - x_3) - y_1$

где λ это угол наклона прямой, соединяющей две точки

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \mod p.$$

Если P = Q, то вычисляем

$$\lambda = \frac{3x_1^2 + a}{2y_1} \mod p$$

Вычисление степеней α для (0, 2)

1. 2α = α + α = (0, 2) + (0, 2) => P = Q => берём формулу 2

   $\lambda = (3 * 0^2 + 2) / (2 * 2) = 2/ 4 \pmod 5 \Rightarrow \lambda = 3$

   $x_3 = 3^2 – 0 – 0 = 9 \pmod 5 = 4$

   $y_3 = 3 * (0 - 4) – 2 = -14 \pmod 5 = 1$

   Получаем точку (4, 1)

2. 3α = 2α + α = (4, 1) + (0, 2) => P != Q => берём формулу 1

   $\lambda = (2 – 1) / (0 - 4) = 1 / (-4) = 1$

   $x_4 = 1^2 – 4 – 0 = -3 \pmod 5 = 2$

   $y_4 = 1 * (4 - 2) - 1 = 1 \pmod 5 = 1$

   Получаем точку (2, 1)

3. 4α = 2α + 2α = (4, 1) + (4, 1) => P = Q => берём формулу 2

   $\lambda = (3 * 4^2 + 2) / (2 * 1) = 50 / 2 = 25 \pmod 5 \Rightarrow \lambda = 0$

   $x_5 = -2 * 4 = -8 \pmod 5 = 2$

   $y_5 = -1 = -1 \pmod 5 = 4$

   Получаем точку (2, 4)

4. 5α = 4α + α = (2, 4) + (0, 2)

   $\lambda = 2 – 4 / 0 – 2 = -2 / -2 = 1 \pmod 5 = 1$

   $x_6 = 1 – 2 – 0 = -1 \pmod 5 = 4$

   $y_6 = 1 * (2 - 4) – 4 = -2 -4 = -6 \pmod 5 = 4$

   Получаем точку (4, 4)

5. $6\alpha = 5\alpha + \alpha = (4, 4) + (0, 2)$

   $\lambda = 2 – 4 / 0 – 4 = 2 / 4 \pmod 5 = 3$

   $x_7 = 9 – 4 – 0 = 5 \pmod 5 = 0$

   $y_7 = 3 * (4 - 0) – 4 = -12 - 4 = 8 \pmod 5 = 3$

   Получаем точку (0, 3)

6. $7\alpha = 6\alpha + \alpha = (0, 3) + (0, 2)$

   Т.к $y_1 = 3$, $y_2 = 2$, $y_1 + y_2 \pmod 5 = 0$ => 7α это точка О (точка бесконечности) => $\alpha = 7$ это нулевой элемент группы

Подпись Эль Гамаль

Коэффиценты будут вычисляться по модулю, равному количеству точек (Mod 7)

$P = 5$, $\alpha = (0, 2)$

Выберем произвольную a (Секретный ключ), от 1 до 7 (7 – степень α)

Пусть $a = 3$

Тогда публичный ключ $\beta = a \cdot \alpha = 3\alpha$

Начало шифрования

$e_K(M, k) = (k * \alpha , M + k * \beta)$, где M принадлежит кривой E, $0 \le k \le$ число точек минус 1 => $\mathbf{0 \le k \le 6}$

Выбираем сообщение для шифрования (Например $(2, 4) = 4\alpha$)

Выбираем k

Пусть $k = 4$

$y_1 = k * \alpha = 4 * \alpha = 4\alpha$

$y_2 = k * \beta + M = 3\alpha * 4 + 4\alpha = 16\alpha \bmod 7 = 2\alpha$

Получаем точку $(4\alpha, 2\alpha)$

Начало дешифрования

$d_K(y_1, y_2) = y_2 - a * y_1, \quad a = 3$

$M = y_2 - 3 * y_1 = 2\alpha - 3*4\alpha = 2\alpha - 12\alpha = -10\alpha \bmod 7 = 4\alpha$

Создание подписи

$y^2 = x^3 + 2x + 4 \bmod 5$, $\alpha = (0, 2)$, $n = 7$

закрытый ключ $d = 3$, $Q = 3 \cdot \alpha = (2, 1)$

открытый ключ $(E, P, n, Q) = (y^2 = x^3 + 2x + 4, (0, 2), 7, (2, 1))$

Генерация подписи

Выберем случайное $k = 2$

Вычислим $k * p = 2 * \alpha = 2\alpha = (4, 1) = (x_1, x_2)$

Вычислим $r = x_1 \bmod n = 4 \bmod 7 = 4$ (Если $n = 0$, выбираем другое k)

Вычисляем $k^{-1} \bmod n = ½ \bmod 7 \Rightarrow k^{-1} = 4$

$S = k^{-1} \cdot (H(M) + d \cdot r) \bmod n = 4 * (H(M)) + 3 * 4) \Rightarrow$ Пусть $H(M) = 3$, тогда $S = 60 \bmod 7 = 4$ (Если $S = 0$, выбираем другое k)

Подпись – $(r, s) = (4, 4)$

Проверка подписи

Проверим, что [r и s] входят в интервал [1, n-1], иначе *подпись не верна.*

Вычисляем $w = s^{-1} \bmod n = 3^{-1} \bmod 7 = 5$

Пусть $H(M) = 3$

$u_1 = H(M) * w \pmod n = 3 * 3 \bmod 7 = 9 \bmod 7 = 2$

$u_2 = 4 * 3 \bmod n = 12 \bmod 7 = 5$

$u_1P + u_2Q = 2 * \alpha + 5 * 3\alpha = 2\alpha + 15\alpha = 17\alpha = (17 \bmod 7)\alpha = 3\alpha = (4, 1) = (x_0,y_0)$.

$x_0 = \mathbf{r} = 4$ —> **подпись валидна.**