密码学第八次作业

1.ECC基础知识

(1)： Z_p $GF(2^p)$

(2)：3 p、a、b $y^2 = x^3 + ax + b \bmod p$ 0 2

(3)：$i: P$ $ii: (x_p, -y_p)$ iii：$x_R = \Delta^2 - x_P - x_Q$，$y_R = -y_P + \Delta(x_P - x_R)$
$\Delta = \frac{y_Q - y_P}{x_Q - x_P} \bmod p$

iv：椭圆曲线对数问题

(4)：$y_m = y_n$ 或 $y_m + y_n = 0$ $M - N$

(5)：0

2.ECC计算

(1) Z_p上的椭圆曲线

曲线方程：$y^2 = x^3 + x + 6 \bmod 11$ 点集如下：

$(0,0), (5,2), (5,9), (7,2), (7,9), (8,3), (8,8), (10,2), (10,9)$

$G = (5,2)$ $2G = (10,2)$ $3G = (7,9)$

$x_{2G} = (\frac{3x_p^2+a}{2y_p})^2-2x_p = (\frac{3*5^2 + 1}{2*2})^2 - 2*5 = -1 = 10 \bmod 11$

$y_{2G} = (\frac{3x_p^2+a}{2y_p})(x_p - x_R) - y_p = (\frac{3*5^2+1}{2*2})(5 - 10) - 2 = 2 \bmod 11$

$\therefore 2G = (10,2)$

利用点加公式：$x_R = \Delta^2 - x_P - x_Q$，$y_R = -y_P + \Delta(x_P - x_R)$ $\Delta = \frac{y_Q - y_P}{x_Q - x_P} \bmod p$

也可以计算得到$3G = (7,9)$

(2) $GF(2^m)$上的椭圆曲线

方程：$y^2 + xy = x^3 + g^2x + g^2$ 有限域中所有元素：$0, g^0, g^1, g^2$

$x = 0$时，$y^2 = g^2 \rightarrow y = g \rightarrow (0, g)$

$x = g^0$时，$y^2 + g^0y = g^0 + g^2 + g^2 = g^0 \rightarrow y = g^2 \rightarrow (g^0, g^2)$

$x = g^1$时，$y^2 + gy = g^3 + g^3 + g^2 \rightarrow y = g^0 \rightarrow (g^1, g^0)$

$x = g^2$时，$y^2 + g^2y = g^6 + g^4 + g^2 = g^0 + g^1 + g^2 = 0 \rightarrow y = g^2 \rightarrow (g^2, g^2)$

所有点：$(0, g), (g^0, g^2), (g, g^0), (g^2, g^2)$

3.基于ECC的公钥密码体制

（1）DH密钥交换

$K_{AB} = n_A n_B G = 6G = (125, 152)$

$K_{AD} = n_A n_D G = 8G = (174, 163)$

$K_{BD} = n_B n_D G = 12G = (155, 95)$

（2）ElGamal加解密

i.

$P_B = n_B G = 7G = (7, 2)$

ii.

$C_m = (kG, P_m + kn_A G) = ((8, 3), (10, 2))$

iii.

- Bob受到密文后，把密文分解$C_1 = (8, 3), C_2 = (10, 2)$
- 计算$n_B C_1 = (3, 5)$
- $msg = C_2 - n_B C_1 = (10, 9)$