# 第8章 SM2公钥密码算法

**1．已知点G=(2，7)在椭圆曲线E11(1，6)上，求2G和3G。**

答案：这里*a*=1,*b*=6,*p*=11,则对于2G=G+G，可首先计算

利用公式和可得：

2G=G+G=（2，7）+（2，7）=（5，2）。同样得3G=2G+G=（5，2）+（2，7）=（8，3）。

**2．有限域上一条椭圆曲线E19(1,1) 表示*y*2=*x*3+*x*+1 ，求其上的所有点。**

答案：

|  |  |  |  |
| --- | --- | --- | --- |
| *x* | *x*3+*x*+1 mod19 | 是否为模19的平方剩余 | *y* |
| 0 | 1 | 是 | （1，18） |
| 1 | 3 | 不是 |  |
| 2 | 11 | 不是 |  |
| 3 | 12 | 不是 |  |
| 4 | 12 | 不是 |  |
| 5 | 17 | 不是 |  |
| 6 | 14 | 不是 |  |
| 7 | 9 | 是 | （3，16） |
| 8 | 8 | 不是 |  |
| 9 | 17 | 不是 |  |
| 10 | 4 | 是 | （2，17） |
| 11 | 13 | 不是 |  |
| 12 | 12 | 不是 |  |
| 13 | 7 | 不是 |  |
| 14 | 4 | 是 | （2，17） |
| 15 | 9 | 是 | （3，16） |
| 16 | 9 | 是 | （3，16） |
| 17 | 10 | 不是 |  |
| 18 | 18 | 不是 |  |

所以由表可知上椭圆曲线上的点为：（0，1），（0，18），（7，3），（7，16），（10，2）（10，17），（14，2），（14，17），（15，3），（15，16），（16，3），（16，16）

**3．若选用输出长度为256位的国密算法SM3作为杂凑函数，则当密钥派生函数中的len为544时，密钥派生函数共进行几次Hash运算，输出的比特串K中包含最后一次Hash运算结果的多少位？**

答案： 由题意知，在SM2中的密钥派生函数选用了SM3，SM3输出的函数值长度为*v*=256, 当派生函数的输出长度为len=544时，，因此派生函数共使用了3次Hash运算。

最后一次Hash运算结果的有位输出在K中。

**4．SM2算法的基础是什么，与RSA公钥密码体制相比有什么优点？**

答案：SM2算法是一种椭圆曲线公钥密码算法，它有基于素域和二元域的椭圆曲线。

相对于RSA算法，SM2算法具有以下优点：

（1）安全性高。192位的SM2密码强度已经比RSA 2048位密码强度要高。

（2）存储空间小。SM2算法的密码一般使用192－256位，RSA算法密码一般需要使用2048－4096位。

（3）签名速度快。SM2在私钥运算上，速度远比RSA快得多。

5.设素域F5=｛0，1，2，3，4｝。参照本章例8.5构造加法、乘法示例，生成元及由生成元方幂表示素域中的元素。

答案：椭圆曲线方程为：*y*2=*x*3+*x*+6mod5，首先构造*E*5(1,6)的元素。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *y* | 0 | 1 | 2 | 3 | 4 |
| *y*2 | 0 | 1 | 4 | 9 | 16 |
| *y*2mod5 | 0 | 1 | 4 | 4 | 1 |

从上表可以看出，在GF(5) 中，元素0、1、4是平方剩余，而元素2、3不是平方剩余。（可用欧拉平方剩余定理来判断。上表很明显有这样的结果）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *x* | 0 | 1 | 2 | 3 | 4 |
| *x*2+*x*+6 | 6 | 8 | 16 | 36 | 74 |
| *x*2+*x*+6mod5 | 1 | 3 | 1 | 1 | 4 |
| *y* | [1,4] | 无 | [1,4] | [1,4] | [2,3] |

*E*5(1,6)={O、(0,1)、(0,4)、(2,1)、(2,4)、(3,1)、(3,4)、(4,2)、(4,3) }

*||E*5(1,6)||=9

*E*5(1,6)的加法：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **加法** | **O** | **(0,1)** | **(0,4)** | **(2,1)** | **(2,4)** | **(3,1)** | **(3,4)** | **(4,2)** | **(4,3)** |
| **O** | O | (0,1) | (0,4) | (2,1) | (2,4) | (3,1) | (3,4) | (4,2) | (4,3) |
| **(0,1)** | (0,1) | (4,2) | O | (3,4) | (4,3) | (2,4) | (3,1) | (2,1) | (0,4) |
| **(0,4)** | (0,4) | O | (4,3) | (4,2) | (3,1) | (3,4) | (2,1) | (0,1) | (2,4) |
| **(2,1)** | (2,1) | (3,4) | (4,2) | (2,4) | O | (0,4) | (4,3) | (3,1) | (0,1) |
| **(2,4)** | (2,4) | (4,3) | (3,1) | O | (2,1) | (4,2) | (0,1) | (0,4) | (3,4) |
| **(3,1)** | (3,1) | (2,4) | (3,4) | (0,4) | (4,2) | (0,1) | O | (4,3) | (2,1) |
| **(3,4)** | (3,4) | (3,1) | (2,1) | (4,3) | (0,1) | O | (0,4) | (2,4) | (4,2) |
| **(4,2)** | (4,2) | (2,1) | (0,1) | (3,1) | (0,4) | (4,3) | (2,4) | (3,4) | O |
| **(4,3)** | (4,3) | (0,4) | (2,4) | (0,1) | (3,4) | (2,1) | (4,2) | O | (3,1) |

*E*5(1,6)的乘法：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **乘法** | **[1]** | **[2]** | **[3]** | **[4]** | **[5]** | **[6]** | **[7]** | **[8]** | **[9]** |
| **O** | O | O | O | O | O | O | O | O | O |
| **(0,1)** | (0,1) | (4,2) | (2,1) | (3,4) | (3,1) | (2,4) | (4,3) | (0,4) | O |
| **(0,4)** | (0,4) | (4,3) | (2,4) | (3,1) | (3,4) | (2,1) | (4,2) | (0,1) | O |
| **(2,1)** | (2,1) | (2,4) | O | (2,1) | (2,4) | O | (2,1) | (2,4) | O |
| **(2,4)** | (2,4) | (2,1) | O | (2,4) | (2,1) | O | (2,4) | (2,1) | O |
| **(3,1)** | (3,1) | (0,1) | (2,4) | (4,2) | (4,3) | (2,1) | (0,4) | (3,4) | O |
| **(3,4)** | (3,4) | (0,4) | (2,1) | (4,3) | (4,2) | (2,4) | (0,1) | (3,1) | O |
| **(4,2)** | (4,2) | (3,4) | (2,4) | (0,4) | (0,1) | (2,1) | (3,1) | (4,3) | O |
| **(4,3)** | (4,3) | (3,1) | (2,1) | (0,1) | (0,4) | (2,4) | (3,4) | (4,2) | O |

由上表可知，元素(0,1)、(0,4)、 (3,1)、(3,4)、(4,2)、(4,3)都为 *E*5(1,6) 的生成元，阶数都为9。元素(2,1)、(2,4)不是*E*5(1,6)的生成元，其阶数为3。

由上述表格，容易得到每个元素的方幂表示。

**6．利用椭圆曲线实现ECC密码体制，假设取*p*=23, *Ep*(1,1)椭圆曲线为：，*Ep*(1,1)的一个生成元是*G*=(6,4)，私钥*d*=3，明文*M*=(5,4) ，求ECC的加解密过程。**

答案：由题，公钥为*P*A=[*d*]*G*=[3]*G*=[3]（6，4）=（2，16）。

加密：用户B随机选取*k*=2，计算

*C*1=[2]*G*=（17，13）

*C*2=*M*+[*k*]*P*A=（5，4）+2（2，16）=（12，13）+（5，4）=（17，17）

得密文*C*=（*C*1,*C*2）=（（17，13），（17，17））

解密：*C*2-[*d*]*C*1=（17，17）- [2]（17，13）

=（17，17）-（12，13）

=（5，4）。