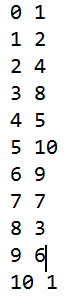
***10.2 Diffie-Hellman公钥中，q=11,α=2***

***a. 证明2是11的本原根。***





***b. YA=9,XA=?***

查一下a中求出来的表，可知XA=6

***c. YB=3,K=?***

根据Diffie-Hellman方法，K的表示方法如下：

在此处，当然是

***10.6题 q=71,α=7***

***a.***

密文为（49，57）

***b. lice发送密文为,***

首先知道

59

故

即

***10.10 ,P+Q=?,P+P=?***

即

1. 2P

直线方程为

即

***10.11 对于质数椭圆曲线给定点G(2,7)，计算2G到13G***

首先，为了计算简便，先写出逆元表来

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 6 | 4 | 3 | 9 | 2 | 8 | 7 | 5 | 10 |

1. 在点G(2,7)处，先求斜率

=13

,直线方程为y=8x+2

得到2G=(5,-9)=(5,2)

1. 对于直线G(2,7),2G(5,2)，先求斜率k

,直线方程为y=2x+3

得到3G=(8,-8)=(8,3)

1. 对于直线3G(8,3),G(2,7)，先求斜率

,直线方程为y=3x+1

得到4G=(10,-9)=(10,2)

1. 对于直线4G(10,2),G(2,7)，先求斜率

,直线方程为y=9x

得到5G=(3,-5)=(3,6)

1. 对于直线5G(3,6),G(2,7)，先求斜率

,直线方程为y=10x+9

得到6G=(7,-2)=(7,9)

1. 对于直线6G(7,9),G(2,7)，先求斜率

,直线方程为y=7x+4

得到7G=(7,-9)=(7,2)

1. 对于直线7G(7,2),G(2,7)，先求斜率

,直线方程为y=10x+9

得到8G=(3,-6)=(3,5)

1. 对于直线8G(3,5),G(2,7)，先求斜率

,直线方程为y=9x

得到9G=(10,-2)=(10,9)

1. 对于直线9G(10,9),G(2,7)，先求斜率

,直线方程为y=3x+1

得到10G=(8,-3)=(8,8)

1. 对于直线10G(8,8),G(2,7)，先求斜率

,直线方程为y=2x+3

得到11G=(5,-2)=(5,9)

1. 对于直线11G(5,9),G(2,7)，先求斜率

,直线方程为y=8x+2

得到12G=(2,-7)=(2,4)

1. 对于直线12G(2，4),G(2,7),因为关于x轴对称，所以13G=O