现代密码学作业——第五讲

1、

|  |  |
| --- | --- |
| 状态 | 输出 |
| 1000 | 0 |
| 1100 | 0 |
| 1110 | 0 |
| 1111 | 1 |
| 0111 | 1 |
| 1011 | 1 |
| 0101 | 1 |
| 1010 | 0 |
| 1101 | 1 |
| 0110 | 0 |
| 0011 | 1 |
| 1001 | 1 |
| 0100 | 0 |
| 0010 | 0 |
| 0001 | 1 |
| 1000 | 0 |

输出为：000111101011001

2、

|  |  |
| --- | --- |
| 状态 | 输出 |
| 1011 | 1 |
| 1101 | 1 |
| 1110 | 0 |
| 1111 | 1 |
| 0111 | 1 |
| 1011 | 1 |

输出：11011

周期：5

3、

初始化：

S: 0 1 2 3

K: 1 2 3 1

KSA：

i=0, j=0+s[0]+k[0] mod 4 = 1 , swap(s[0],s[1]) => S: 1 0 2 3

i=1, j=1+s[1]+k[1] mod 4 = 3 , swap(s[1],s[3]) => S: 1 3 2 0

i=2, j=2+s[2]+k[2] mod 4 = 3 , swap(s[2],s[3]) => S: 1 3 0 2

i=3, j=3+s[3]+k[3] mod 4 = 2 , swap(s[3],s[2]) => S: 1 3 2 0

PRGA:

i=0, j=0:

i=(i+1) mod 4=1

j=(j+s[i]) mod 4=3

swap(s[i],s[j])=swap(s[1],s[3])

=>S: 1 0 2 3

t=(s[i]+s[j])=(s[1]+s[3]) mod 4=3

k=s[t]=s[3]=3

=>key:11

重复上述过程，可得密钥key:1100110111

明文p=OK=14,10=01110 01010

密文c=pkey=10111 11101=XE

4、

5级本原多项式P(x)=x5+x3+1

对应的反馈函数为bi+6=bi+3bi+1

5、











