**计算机科学与技术学院2016-2017学年第2学期 考试答案**

密码学原理 B卷 闭卷

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

一、已知K=(11,15)是定义在上的仿射密码的密钥。

（1）以的形式给出解密函数，这里； (6分) (2)证明对于任意的，都有。（4分）

解：（1）

（2）

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

**二、**假设有一个同步流密码的密钥流是由4级LFSR产生的，Oscar得到密文串“10110100”和相应的明文串“01100011”，试求出产生密钥流的递推公式。(10分)

解：根据明密文可得密钥为11010111，则有，

解得，所以递推公式为

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

**三、**考虑一个密码体制，其中。加密矩阵如下：

若

（1）计算密文的概率分布P(C)和条件概率P(M|C) ；（8分）

（2）判断密码体制是否具有完善保密性，给出理由。（3分）

|  |  |  |  |
| --- | --- | --- | --- |
|  | *a* | *b* | *c* |
| *K*1 | 1 | 2 | 3 |
| *K*2 | 3 | 2 | 1 |
| *K*3 | 2 | 1 | 3 |

解：**（1）**

****

**（2）不具有完善保密性，因为p(m|c)≠p(m)**

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

四、Alice和Bob采用D-H算法进行密钥协商，协商n=29和原根g=2，Alice发送X=2x=18给Bob，Bob发送Y=2y=21给Alice，试求：（1）x和y（使用shanks算法）；（9分）

（2）二人协商的密钥。（4分）

**解：（1）**

（2）

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

五、假设RSA公钥密码体制中，签名密钥，试签名消息M=28，并使用RSA的公钥对签名进行验证。（14分）

**解：**

验证：

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

六、证明解密一个Feistel密码相当于对密文使用加密算法，但密钥编排方案要逆序使用。（12分）

**证明：**

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

七、AES算法中的列混合是将每列元素看做一个系数定义在上的三次多项式，记为S(x)，列混合运算定义为,试求当前列列经过列混合之后的结果。（10分）

解：

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

八、简述CBC模式的工作过程（10分）

解：加密

解密

|  |  |
| --- | --- |
| 得分 | 评卷人 |
|  |  |

九、简述线性密码分析的基本原理。（10分）

解：一种已知明文攻击方法。分析明密文相关比特的线性关系，寻找大概率的线性链，选取足够的明密文对，最后一轮正确的密钥可以使得该线性特征显著。