**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 A卷 闭卷

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

一、设下列的π是集合{1,2，…，9}上的置换，

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| X | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| π(x) | 5 | 8 | 1 | 7 | 2 | 4 | 6 | 3 |

（1）求出逆置换π-1；（4分）

（2）解密使用该置换密码加密的密文：VOIFNOELSWLLLIAYWTAEYSES。 (4分)

解：（1）逆置换为

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| X | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| π-1 | 3 | 5 | 8 | 6 | 1 | 7 | 4 | 2 |

（2）In love folly is always sweet.

|  |  |
| --- | --- |
| 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“01101011”和相应的明文串“11011001”，试求出产生密钥流的递推公式。(10分)

密钥为01101011+11011001=10110010，则

，则，则有



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

|  |  |  |  |
| --- | --- | --- | --- |
|  | *a* | *b* | *c* |
| *K*1 | 1 | 2 | 3 |
| *K*2 | 3 | 2 | 1 |
| *K*3 | 2 | 1 | 3 |
| *K*4 | 1 | 3 | 2 |

**三、**考虑一个密码体制，其中。加密矩阵如下：

若

（1）计算P(C)和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）

**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采用如下定义的签名算法进行数字签名，密钥，公开选定的公钥（79,13，8，18）和签名算法：选择秘密的随机数k，，定义



（1）试给出该签名算法对应的验证算法；（3分）

（2）给定消息x的散列值H(x)=2和随机数k=4，对于敌手Bob，试使用shanks算法根据公钥计算出私钥a，利用a伪造签名并给出验证过程。（12分）

**解：（1）**

**（2）**

签名：

**验证过程略**

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

五、假设RSA公钥密码体制中，加密密钥，试利用中国剩余定理解密密文C=25。（14分）

**解：**

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

六、给出Feistel结构图并描述加解密过程和特点。（12分）

**解：结构图和加解密过程略。**

**特点：结构本身可以保证过程还原；非线性替代过程可以不需要可逆**

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

七、AES算法的S盒是建立在有限域上的，其算法描述如下：



求Subbytes（'6A'）的值。（10分）

解：（'6A'）-1='91'，Subbytes（'6A'）='02'

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

八、简述CCM模式的工作过程（10分）

解：CTR加密+CBC\_MAC鉴别。

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

九、简述差分密码分析的基本原理。（10分）

解：一种选择明文攻击方法，对于给定固定输入差分的明文对及其对应的密文对，寻找大扩散率的差分特征及其差分链，当给定的明密文对数量足够，能够区别正确的候选密钥。