**计算机科学与技术学院2016-2017学年第2学期 考试试卷**

密码学原理 A卷 闭卷

姓名\_\_\_\_\_\_\_\_\_\_\_\_班级\_\_\_\_\_\_\_\_\_\_\_\_学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_考试日期 2017-06-21

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 九 | 总分 | 核对人 |
| 题分 | 8 | 10 | 11 | 15 | 14 | 12 | 10 | 10 | 10 | 100 |  |
| 得分 |  |  |  |  |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| 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)

|  |  |
| --- | --- |
| 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)

|  |  |
| --- | --- |
| 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）

|  |  |
| --- | --- |
| 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）

|  |  |
| --- | --- |
| 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）

|  |  |
| --- | --- |
| 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）

|  |  |
| --- | --- |
| 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）

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

八、简述CCM模式的工作过程（10分）

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

九、简述差分密码分析的基本原理。（10分）