**计算机科学与技术学院2013-2014学年第2学期 考试答案**

密码学基础 A卷 闭卷

姓名\_\_\_\_\_\_\_\_\_\_\_\_班级\_\_\_\_\_\_\_\_\_\_\_\_学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_考试日期 2014-07-01

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 九 | 总分 | 核对人 |
| 题分 | 10 | 12 | 10 | 13 | 15 | 15 | 10 | 10 | 5 | 100 |  |
| 得分 |  |  |  |  |  |  |  |  |  |  |  |

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

一、设下列的π是集合{1,2，…，8}上的置换，

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

（1）求出逆置换π-1；（5分）

（2）解密使用该置换密码加密的密文：TMIIETFSUMOMERRSAIVTOONC。(5分)

解：（1）逆置换为

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

（2）明文为ITSTIMEFORSUMMERVOCATION

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

**二、**假设有一个同步流密码的密钥流是由5级LFSR产生的，Oscar得到密文串“0110100101”和相应的明文串“1010011101”，试求出产生密钥流的递推公式。(12分)

密钥为0110100101+1010011101=1100111000，则，则，则有



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

**三、**考虑一个密码体制，其中。假设加密矩阵如下：

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

若，试判断该密码体制是否为完善保密的，给出判断过程。（10分）

解：

，

同理对明文为b、c有同样结论，故是完善保密的。

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

四、Alice和Bob采用ElGamal算法进行通信加密，Alice的公开密钥是(n=17,g=3,b=13)，Bob的公开密钥是(n=23,g=7,b=11)，现截获到Alice发给Bob的密文(4,3)，试破译该密文。（13分）

解：Alice给Bob，故n=23,g=7,b=11，根据shanks算法，有L1：（0,1）（1,17）（2,13）（3，14），（4,8）L2：（0,11）（1,18）（2,19）（3,6），（4,14）故有3\*5+4=19，则解密过程为

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

五、假设RSA公钥密码体制中，加密密钥，试对明文进行数字签名，并验证数字签名的正确性。（15分）

解：根据，且，则根据欧几里得扩展算法可得，数字签名过程为

验证过程：，所以验证成功。

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

六、AES的字节替代操作SubBytes定义在有限域上，试求SubBytes（67）。（15分）

解：，



67-1=43，则SubBytes（67）=85

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

七、证明在任何密码体制中，。（10分）

证明：,

,而,,而，所以可证。

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

八、证明DES解密算法相当于对密文使用加密算法，但密钥编排方案要逆序使用。（10分）

证明：加密为

则解密，过程是一样的，只是密钥逆序使用，所以得证。

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

九、简述利用Hash函数提供数据完整性的原理。（5分）

答：Hash函数将任意长的明文摘要成固定长度的“指纹”，一旦数据改变，则指纹就不再正确，因此通过验证给定明文的指纹可以检测数据是否被篡改，提供数据完整性验证。