**计算机科学与技术学院2015-2016学年第2学期 考试答案**

密码学基础 B卷 闭卷

姓名\_\_\_\_\_\_\_\_\_\_\_班级\_\_\_\_\_\_\_\_\_\_\_\_学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_考试日期 \_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 九 | 总分 | 核对人 |
| 题分 | 8 | 10 | 8 | 12 | 12 | 12 | 10 | 13 | 15 | 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) | 5 | 8 | 1 | 3 | 7 | 4 | 2 | 6 |

（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：VALNCGOAIYTOMNISREFVTOAI。(4分)

解：（1）逆置换π-1为

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

（2）LONGVACATIONISMYFAVORITE

|  |  |
| --- | --- |
| 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“0110011010”和相应的明文串“1101011101”，试求出产生密钥流的递推公式。(10分)

密钥为0110011010+1101011101=1011000111，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 | 2 | 1 |

若，试判断该密码体制是否为完善保密的，给出判断过程。（8分）

解：



故不是完善保密的。

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

四、Alice和Bob采用D-H算法进行密钥协商，协商n=37和原根g=2，Alice发送X=31给Bob，Bob发送Y=26给Alice，试求二人协商的密钥。（12分）

解：根据shanks算法，n=37，所以阶为36，m=6，



|  |  |
| --- | --- |
| 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。（12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（53）。（12分）

解：，



53-1=CA，则SubBytes（53）=ED

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

七、设（P,C,K,E,D)是一个密码体制，试证明

。（10分）

证明：

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

八、证明Miller-Rabinn算法对于合数问题是一个偏是的Monte Carlo算法。（13分）

证明：通过反证法，当n为素数时不能返回为合数的回答。

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

九、试利用公钥密码算法、对称密码算法和Hash函数设计一个安全的邮件传输系统方案，并分析方案的合理性。（15分）

