**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A卷 闭卷

姓名\_\_\_\_\_\_\_\_\_\_\_\_班级\_\_\_\_\_\_\_\_\_\_\_\_学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_考试日期 2016-06-22

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 九 | 总分 | 核对人 |
| 题分 | 8 | 10 | 8 | 14 | 14 | 10 | 12 | 10 | 14 | 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 | 9 |
| π(x) | 3 | 8 | 6 | 9 | 7 | 1 | 5 | 4 | 2 |

（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：

WHEOWNHTOEHTAHLRAENGAUNDLEOEHDETANAGMDOSRSWEA。(4分)

解：（1）逆置换π-1为

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 6 | 9 | 1 | 8 | 7 | 3 | 5 | 2 | 4 |

（2）NOWTHEWHOLEEARTHHADONELANGUAGEANDTHESAMEWORDS

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

**二、**假设明文behold利用2阶希尔密码加密得到密文RZZPMH，试求该希尔密码的加密密钥。(10分)

解：K=X-1Y，（1,4）K=（17,25），（7,14）K=（25,15），（11,3）K=（12,7）

，而gcd（12,26）=2，故该矩阵不存在逆



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

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

**三、**考虑一个密码体制，其中。加密矩阵如下：

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ElGamal算法进行通信加密，Alice的公开密钥是(n=17,g=5,b=14)，Bob的公开密钥是(n=17,g=5,b=11)，现截获到Alice发给Bob的密文(3,5)，试利用shanks算法求解离散对数并破译该密文。（14分）

解：根据shanks算法，n=17，所以阶为16，m=4，



|  |  |
| --- | --- |
| 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=18。（14分）

解：

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

六、已知AES的当前状态第一列为，试计算其经过列混合之后的输出。（10分）

解：（03x3+01x2+01x+02)(D8x3+4Ax2+90x+4D)=46x3+3Ax2+70x+A3

所以输出为（A3,70,3A，46）

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

七、设明文分组序列x1…xn产生的密文分组序列为y1…yn。假设一个密文分组yi在传输时出现错误，试问在应用ECB、CBC、OFB和CFB模式下不能正确解密的明文分组数分别是多少，并用各种模式的基本原理证明你的结论。（12分）

解：ECB和OFB不能正确解密1个分组，CBC和CFB不能正确解密2个分组

ECB：

CBC: 

OFB: 

CFB: 

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

八、证明Solovay-Strassen算法对于合数问题是一个偏是的Monte Carlo算法。（10分）

算法描述：随机选取a，使之 



if x=0 return ("n is compisite")

else y=a(n-1)/2

if x=y mod n return ("n is prime")

else return ("n is composite")

证明：如果n是素数，则

所以不会输出为合数，可证。

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

九、试利用RSA、AES和SHA-1设计一个可以提供认证、机密性、完整性的文件传输系统方案，并分析方案的合理性。（14分）

