**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 B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 | 12 | 13 | 11 | 8 | 15 | 9 | 100 |  |
| 得分 |  |  |  |  |  |  |  |  |  |  |  |

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

一、在一个密码体制中，如果一个加密函数和一个解密函数相同，我们将这样的密钥称为对合密钥。试找出定义在上的移位密码体制中的所有对合密钥。(10分)

解：x+k+k=x，则k=0或者13

|  |  |
| --- | --- |
| 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“0110010101”和相应的明文串“1011011101”，试求出产生密钥流的递推公式。(12分)

解：密钥为0110010101+1011011101=1101001000，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 | 3 | 1 | 2 |
| *K*3 | 2 | 3 | 1 |

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：，

，故不是完善保密的。

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

四、Alice和Bob采用D-H算法进行密钥交换，双方协商n=17,g=3，现截获到Alice发给Bob的X=5以及Bob发给Alice的Y=10，试分析Alice和Bob所协商的密钥。（12分）

解：Alice根据shanks算法，有L1：（0,1）（1,13）（2,16）（3，4），L2：（0,5）（1,13）（2,10）（3,9），故有1\*4+1=5，则协商的密钥为105 mod 17=6

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

五、假设RSA公钥密码体制中，签名密钥，试对明文进行加密，给出加密过程。（13分）

解：根据，且，则根据欧几里得扩展算法可得，加密过程为

|  |  |
| --- | --- |
| 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。（11分）

解：，故输出为

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

七、证明密钥等概率选取的移位密码是幂等的。（8分）

证明：乘积的密钥k=（k1，k2），则x+k1+k2依然是移位密码，则，则依然是一个等概的移位密码。

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

八、试述ECB、CBC和计数器模式的基本原理和优缺点。（15分）

答：ECB：给定明文分组序列，每一个都是用同一个密钥加密，产生密文分组序列 ，优点是简单快速，可并行实现，无误差传递，缺点是相同明文会产生相同密文，暴露明文模式。

CBC：，优点是初始向量不同相同明文分组会得到不同密文分组，可以用于认证，缺点是不能并行，一个密文块的传输错误会影响两块明文块的解密

计数器：，优点是快速，可并行

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

九、简述Hash函数需满足的安全特性。（9分）

答：单向性，第二原像稳固性和碰撞稳固性。