**计算机科学与技术学院2014-2015学年第2学期 参考答案**

密码学基础 A卷 闭卷

姓名\_\_\_\_\_\_\_\_\_\_\_\_班级\_\_\_\_\_\_\_\_\_\_\_\_学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_考试日期 2015-6-30

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 五 | 总分 | 核对人 |
| 题分 | 10 | 10 | 45 | 20 | 15 | 100 |  |
| 得分 |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **名词解释(本大题5小题，共10分)** |
|  |  |

1、秘密共享 ：也称秘密分享，将秘密分解成多个子秘密，使用超过阈值数目的子秘密才能恢复该秘密的机制。

2、唯密文攻击 ：一种密码分析者只拥有密文进行密码攻击的方法。

3、字典攻击 ：一种由可能的密钥或口令组成字典，遍历字典中的所有条目以猜测密钥或口令的攻击方法。

4、差分能量分析 ：一种密码分析方法，使用统计方法和纠错技术等对密码设备功耗的变化进行分析，以提取密钥的有关信息。

5、单点登录 ：用户一次性进行身份鉴别之后就能够访问多个授权应用的登录机制。

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **判断题(本大题5小题，共10分)** |
|  |  |

请在题后的方框内填上“正确”或“错误”。

1. ，密钥等概率分布，则密文一定等概率分布。 [错误]
2. ，明文等概率分布，则密文一定等概率分布。 [正确]
3. 在任何完善密码体制中。 [正确]
4. 采用PKCS#5进行短块处理，若明文长度恰为分组整数倍，则密文将与明文长度一致。 [错误 ]
5. 随机数在认证协议中可以起到防止数据重用的作用。 [正确]

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **计算题(本大题5小题，共45分)** |
|  |  |

1. 已知K=(5,12)是定义在上仿射密码的加密密钥，如果密文是字符串‘ABC’，试求对应明文（用小写字母字符串表示）。（5分）



1. 考虑一个密码体制，其中。假设加密矩阵如下：

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

若，试判断该密码体制是否为完善保密的。（10分）



1. 假设有一个同步流密码的密钥流是由3级LFSR产生的，已知密文串“101011”和相应的明文串“010\*10”，其中“\*”为未知比特，试求出产生密钥流的递推公式。（10分）

解: 先通过明密文异或得到密钥为：“111\*01”，有如下方程成立：

，得到，\*=0，所以递推公式为：



1. 假设RSA公钥密码体制中，加密密钥，若密文为95，试求明文。（10分）



1. AES算法的S盒是建立在有限域上的，其算法描述如下：



现在已知，

1. 求的值（用16进制表示）。（4分）
2. 求的值。（6分）



|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **简答题(本大题2小题，共20分)** |
|  |  |

1. 试描述用差分密码分析方法分析SPN密码的过程。（10分）



1. 试简述CCM加密、解密以及数据认证的过程。（10分）



|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **设计题(本大题1小题，共15分)** |
|  |  |

1、已知系统中定义了如下密码算法：（1）H（X）：散列函数；（2）EP（X，Key）：RSA加密函数，DP（Y，Key）：RSA解密函数，密钥为Key；（3）Z（X）：快速压缩函数，Z-1（Y）：对应的解压缩函数；（4）EC（X,Key）：对称加密函数，DC（Y，Key）：对应的对称解密函数，密钥为Key。

Alice想传一个文件给Bob，文件内容为M，试设计一个安全、高效的文件传输方案，并分析方案设计的合理性。

解：如图所示：

