**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 B卷 闭卷

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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、电子印章 ：一种由制作者签名的包括持有者信息和图形化内容的数据，可用于签署电子文件。

2、动态口令 ：基于时间、事件等方式动态生成的一次性口令。

3、公钥基础设施 ：基于公钥密码技术实施的具有普适性的基础设施，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务。

4、链路逐段加密 ：数据在节点之间链路层加密传输，从一个节点发出的加密数据，在下一个节点解密。

5、密钥加密密钥 ：用于对密钥进行加密或解密的密钥。

|  |  |  |
| --- | --- | --- |
| 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. 完善密码体制中，。 [ 正确 ]
2. 一般而言，公钥加密算法比对称加密算法更难破译。 [ 错误 ]
3. 在任何密码体制中。 [ 正确 ]
4. 消息鉴别码MAC可以防止抵赖。 [ 错误 ]
5. 生日攻击不能应用于HMAC模式。 [ 错误 ]

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

1. 已知K=(7,13)是定义在上仿射密码的加密密钥，如果密文是字符串‘XYZ’，试求对应明文。（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 |
| *K*3 | 1 | 2 | 3 |

若，试判断该密码体制是否为完善保密的。（10分）



1. 假设明文“loop”用2阶希尔密码加密后得到“FELL”，试求该希尔密码的加密密钥。（10分）



1. 假设RSA公钥密码体制中，加密密钥，若密文为30，试求明文。（10分）



1. AES算法的S盒是建立在有限域上的，试在该有限域中，求‘37’所代表的元素的乘法逆元。（10分）



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

1. 试描述用线性密码分析方法分析SPN密码的过程。（10分）



1. 试简述生日攻击法寻找HASH函数碰撞的原理与方法。（10分）



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

1、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、高效的文件传输方案，并分析方案设计的合理性。

