华南农业大学期末考试试卷（A 卷）

2018-2019 学年第 2 学期 **考试科目：** 现代密码学

考试类型：（闭卷） 考试 **考试时间：** 120 **分钟**

学号_____姓名_____班级_____年级专业_____

装

订

线

题号	一	二	三	四	总分
得分					
评阅人					

得分	

一、名词解释（本大题共8小题，每小题 3 分，共 24 分）

1. 古典密码
2. 仿射密码
3. 百万富翁问题
4. 消息认证码
5. 欧拉函数
6. DES算法
7. 哈希函数
8. 秘密分割

得分	

1.5CM

二、简答题（本大题共4小题，每小题6分，共24分）

1. 对称密码和非对称密码分别有什么特点，请举例说明。
2. 流密码与分组密码各有什么特点？流密码有哪些设计原则？
3. 为什么Diffie-Hellman密钥交换获得的会话密钥是安全的？
4. 在没有第三方参加的情况下，两方怎样公平的进行掷硬币的游戏？

得分	

1.5CM

三、流程分析题（本大题共3小题，每小题10分，共30分）

1. 写出RC4加密和解密算法的基本流程。

2. 单钥体制下，如何进行安全的会话密钥分配，写出基本流程。

3. 写出公钥密码体制下的认证流程，画出认证框图。

得分	

四、论述题（本大题共2小题，每小题11分，共22分）

1. 写出 RSA 加密算法的基本步骤，并说明其安全性所在。
2. 写出 DSA 签名算法的基本步骤，并说明其正确性和安全性。