中国海洋大学　2017 年 春季学期
《现代密码学理论与实践》复习范围

一 题型

单选题(共 20 题，每题 1 分，共 20 分)
判断题(共 10 题，每题 1 分，共 10 分)
简答题(共 5 题，每题 6 分，共 30 分)
综合题(共 4 题，每题 10 分，共 40 分)

二 复习范围（仅限于简答题和综合题）

1 欧拉函数、欧拉定理、费马小定理：会计算
2 分组密码的工作模式： 工作原理、差错传播、特性、适用场合
3 一次一密：工作原理、优缺点
4 两军问题、《庄子·盗跖》：故事描述、说明的道理
5 PKI 四个信任模型：自己上网查详细工作原理
6 MAC 算法：给定一个简单的 MAC 算法，会证明其是不安全的
7 RSA：加密算法、签名算法的描述、存在性伪造、Hash 函数在数字签名中的作用
8 ElGamal 签名：卷面给出算法的描述后，会证明算法的正确性；卷面给出存在性伪造的方法后，会证明该方法的正确性
9 双线性映射：卷面给出两个双线性映射的式子后，会利用第八章 ppt 第 25 页的双线性映射的性质证明两个式子相等。
10 Lamport 协议、Needham 协议：描述、优缺点
11 实验内容：卷面给出 RSAREF 中的函数定义，会根据题目要求进行填空，将程序补充完整

三 单选、判断题

范围：各章 PPT 后的练习题、以及上课时提到的重点

四 惊喜题

范围：为了活跃场子，出了几道惊喜题，分不多，也不难，都是上课提到的内容

最后，祝大家端午节愉快，考试过关，开心放假，假期悠哉！