《现代密码学》2019 复习范围

一、 题型

单选(20 分)、判断(10 分)、简答(30 分)、综合(40 分)

二、 复习范围

1、 **单选、判断：**老师放飞自我的地方

（PPT 中全部画五星的地方，题目有一定难度，考察大家综合思维能力）

记住：不要死记硬背！不要死记硬背！不要死记硬背！

2、 简答、综合：

一次一密

对称密码的工作模式

欧拉函数、欧拉定理、费马小定理 会计算

最大公约数、最小公倍数

RSA 加密、RSA 签名、ElGamal 数字签名

数字信封

椭圆曲线的画图（给出一个或两个点，会画点的相加）

双线性映射（特别是会用双线性进行计算）

Needham 口令认证协议

秘密共享

Shamir 的门限方案（参看 PPT 中的例题）

PS：以上范围包括 PPT 中涉及的每一页内容。