2023-2024学年《密码学》

判断题：TF

- SM2 对称加密与否（连着考了两年了，记得回忆！）
- Z3 上的 2*2 可逆矩阵数目
- 扩展欧几里得算法时间复杂度（PPT 原结论）等
- 哈希只考察了书中的一个定理结论，即可以通过抗碰撞的 compress 函数迭代构造。

填空题：

- 仿射密码密钥空间（PPT 原结论）
- 条件概率计算（贝叶斯）

大题：

- LFSR 周期（1 和 15）
- 作业题
- 置换密码求逆置换后解密
- AES 差分攻击分析差分工具表的最大值。（10 分，很难。。。）
- 倍加和算法伪代码，如何提高效率（NAF）
- 中国剩余定理求二次同余方程（就是数基）。BBS 生成器，及其安全性的分析
- ECDSA 安全性的计算推导与证明。固定 K 值会存在线性方程组可求解，容易被破解密钥。（10 分）

总体来说，80 分的正常分数，20 分的思考题难度较大。。。几乎所有密钥体制都会直接给出来，不要浪费时间背一些复杂的！关注于一些 PPT 中结论和作业计算题。可以用去年数基的题练习一下。最后苏明老师也不会划重点，但是哈希几乎不考，古典密码有一些，难题集中在椭圆曲线加密和 AES 分组加密那几个章节。伪代码需要准备一些！密码学上一届考察的是 Miller Rabin 伪代码。下一届可能还要出。关注 OJ 上的题。