《密码学》期末复习提纲

一． 密码学概述

密码五元组、保密通信模型

对称密码体制、非对称密码体制的区别、各自优缺点

安全性定义：无条件安全、计算安全、可证明安全

密码攻击分类：唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击

二． 古典密码

1. 单表替代密码：移位密码、**仿射密码**、密钥短语密码

2. 多元替代密码：Hill 密码

3. 多表替代密码：Vigenère 密码

4. 置换密码：了解倒置密码、换位密码

三．分组密码

分组密码设计原则、Feistel 结构及特点、SPN 结构及特点

DES 算法：基本了解发展历史；熟悉掌握算法整体框架、算法使用的结构、分组长度、密钥长度、迭代轮数、密钥扩展算法、加解密算法以及轮函数的细节，会画流程图；理解 DES 算法的互补对称性，理解 DES 算法的加解密一致性，了解 DES 的弱密钥，以及 2-DES、3-DES 算法；

AES 算法：基本了解发展历史；熟悉掌握算法整体框架、算法使用的结构、分组长度、密钥长度、迭代轮数、密钥扩展算法、加解密算法以及轮函数的细节，会画流程图；掌握**有限域上的乘法和求逆运算**；

了解 AES 算法加解密操作的区别。

SM4 算法：熟悉掌握算法整体框架、算法使用的结构、分组长度、密钥长度、迭代轮数、密钥扩展算法、加解密算法以及轮函数的细节，会画流程图；了解 SM4 算法的加解密一致性，了解 SM4 算法与 AES 和 DES 算法的异同点

分组密码工作模式：熟悉 ECB、CBC、CFB、OFB、CTR 模式，会画加解密流程图，熟悉掌握几种模式的加解密过程是否可并行，是否使用解密算法，会分析错误传播情况；

分组密码分析方法：了解差分分析、线性分析大致思想和所属攻击的类别。

四．流密码

基本概念：一次一密、流密码、同步流密码、自同步流密码；流密码与分组密码的区别，优缺点及应用场景；会根据 LFSR、NFSR 的反馈函数**计算输出序列和周期**，了解 m 序列和 M 序列的基本概念；

序列密码算法：ZUC 算法的大致流程和应用背景，能区分线性和非线性部分；了解 Trivium 算法的大致流程以及与 ZUC 算法的区别。

五．公钥密码

数学基础：**快速指数算法、扩展欧几里得算法**、中国剩余定理、欧拉函数、素性检测算法；

RSA 算法：理解算法的底层数学问题；熟练掌握 RSA 算法的密钥生成、加解密流程以及正确性证明；了解 RSA 算法的参数选择以及对应的安全性问题；给出具体参数和明文能计算密文；给定密文能计算明文，

并能用中国剩余定理加速解密过程。

ElGamal 算法：理解算法的底层数学问题；熟练掌握 ElGamal 算法的密钥生成和加解密流程；给出具体参数和明文能计算密文；给定密文能还原明文。

ECC 算法：理解**有限域上椭圆曲线的计算**，给定椭圆曲线能计算曲线上所有的点；给定椭圆曲线和基点能通过公式进行点之间的加法运算以及倍点运算；理解 ECC 算法的底层数学问题，熟练掌握 ECC 算法的密钥生成和加解密流程；给出具体参数和明文能计算密文；给定密文能还原明文。

SM2 算法：理解算法的底层数学问题，大致了解 SM2 算法的加解密流程和特点，能比较其与 ECC 算法及其他公钥算法的异同点。

六．哈希函数

基本概念：哈希函数的定义、哈希函数的基本结构、哈希函数的安全性要求、生日攻击、哈希函数的应用场景、消息认证码与 HMAC；对于具体问题能构造或分析哈希函数的碰撞；

MD5 算法：基本了解发展历史和 MD5 算法的基本框架，掌握分组长度、输出长度、迭代轮数、填充和存储规则；了解 MD5 的安全性问题；了解 MD 5 算法与 SHA 算法的异同点；

SM3 算法：基本了解发展历史和 SM3 算法的基本框架，掌握分组长度、输出长度、迭代轮数、填充和存储规则和扩展方式；了解 SM3 算法在 SM2 中的应用；能比较 SM3 算法与 MD5 以及 SHA 算法的异同点；

七. 数字签名

基本概念：数字签名的定义与意义、数字签名的特点、数字签名的五元组、哈希函数在数字签名中的应用；

RSA 算法：熟练掌握 RSA 签名算法的密钥生成、签名和验签过程会画流程图，能理解哈希函数在签名算法中的作用；了解 RSA 签名算法的应用 PGP 混合加密系统；

DSS 算法：基本了解 DSS 算法发展历史，了解 DSS 签名算法的大概框架及特点；理解算法的安全性与底层数学问题的关系，理解使用的随机数 K 的泄露或重用对算法安全性的影响；

SM2 算法：了解 SM2 签名算法的大概框架以及特点；理解算法的安全性与底层数学问题的关系，理解使用的随机数 K 的泄露或重用对算法安全性的影响；

七. 密钥管理

密钥的分层次管理：主密钥、加密会话密钥的密钥、会话密钥；

公钥管理：公开广播、公钥管理机构、公钥证书；

对称密钥管理：密钥中心分配、点对点分配、D-H 密钥交换协议；

主密钥管理：秘密分割、Shamir 门限分割方案