# 武汉大学国家网络安全学院

# 2023-2024 学年度第二学期

# 《密码学》期末考试试卷（A 卷）（回忆版）（开卷）

**本卷依据网安试验班 24 年试卷回忆而成，以方便复习 — by xyz**

**专业：** _____ **学号：** _____ **姓名：** _____

说明：答案请全部写在答题纸上，写在试卷上无效。

考试试卷、答题纸、草稿纸均不得带离考场，否则视为违规。

| 题号 | 一 | 二 | 三 | 四 | 总分 |
|---|---|---|---|---|---|
| 分值 | 30 | 20 | 20 | 30 | 100 |

*忘了具体多少分值了，看看就好*

**一、 计算题（共 30 分）**

1. AES-128，ECB 工作模式，仅计算第一轮第一个字节的加密结果。
   明文：`0x0102030405060708090A0B0C0D0F`，密钥为全 `0`。（数据是这样的）

**二、 算法题（共 2 小题，每小题 10 分，共 20 分）**

1. RSA 算法，n=55，e=7，M1=5，求密文。（数据是这样的）
2. 已知$g(x) = x^4 + x^3 + 1$为 GF(2)上的多项式，以其为连接多项式组成线性移位寄存器（LFSR）。

（1）画出 LFSR 的**逻辑框图**，并求出**反馈函数**；

（2）试穷举其**所有状态**，给出**状态变迁过程**并求出其**周期**和**输出序列**；

（3）判断输出序列是否为 **m 序列**。

**三、 简答题（共 2 小题，每小题 10 分，共 20 分）**

1. 请写出**对称密码**中**填充（padding）**的作用，并举出一种**应用**实例。

2. 请写出**三种分组密码的工作模式**，说明它们的**流程和作用**。

**四、 设计题（共 30 分）**

请针对一种**电子支付系统**，进行安全性分析与设计。分析设计时主要包括：

（1）应用**问题描述**；

（2）你认为其中的**主要安全问题**有哪些；

（3）你觉得可以采用什么样的**安全协议**或**密码学技术**可以**提供解决方案**；若现有技术无法有效解决，请提出你的观点。（差不多是这样吧，具体反正跟着题目要求写）