电子科技大学 2023-2024 学年第二学期期中考试卷

课程名称：密码学 考试形式：闭卷 使用教师：汪小芬

学院：_____ 姓名：_____学号：_____

一，填空题（每空 2 分，共 20 分）

1，科尔霍夫原则中提到，系统保密性不依赖于加密体制或者算法的保密，而依赖于_____。

2，分组密码的迭代方式分为 _____ 和 _____ 两种。

3，一次一密每次加密的密钥是随机产生且使用一次的，它的安全性是 _____ 安全。

4，DES 的操作模式分别有 ECB 模式、CBC 模式、_____ 、_____四种模式，AES 除了拥有以上四种模式，还有 _____模式。

5，DES 分组加密算法中的“S 盒代替”，是将“子密钥异或”的输出结果_____bit 作为 S 盒代替的输入，经过变换得到_____bit 的输出。若 S1 盒输入为 111000（二进制），输出为_____（转换为二进制）。

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

图 1 S1 表

二，选择题（每小题 3 分，共 15 分）

1，以下哪种算法是流密码（ ）。

A.MD5 B.IDEA C.SHA1 D.RC4

2，若已知破译 DES 算法的时间复杂度为2^{56}，那么破译二重-DES 的时间复杂度大约为（ ）。

A.2^{56} B. 2^{112} C. 2^{168} D. 2^{60}

3,分组密码的操作模式 ECB 模式提供了（ ）安全性保证。

A.无安全性 B.CPA 安全 C.CCA 安全 D.无条件安全

4，字母频率分析法对下列哪种密码算法最有效（ ）。

A.置换密码 B.单表代换密码 C.多表代换密码 D.序列密码

5，一个 LFSR 的初始状态为 101，其反馈多项式为$[x^3 + x^2 + 1]$。如果按照时钟周期依次输出 10 个比特，则输出的序列为（ ）。

A. 1011011011 B. 1101101101 C. 1001011011 D.0110110110

三，计算题（每小题 15 分，共 45 分）

（注意：计算题需要给出详细解答过程，只给出答案不计分）

1， 设仿射变换的加密函数为$c = E(m) = 7m + 21(mod\ 26)$

1)写出该加密函数对应的解密函数

2)对“teacher”进行加密。

3)对“rxjfkzyh”进行解密。

2，已知流密码的密文串为 1010110110 和相应明文串 0100010001，而且还已知密钥流是使用 3 级线性反馈移位寄存器产生的，试破译该密码系统。（即写出该密码系统对应的初始状态和反馈函数）。

3，给定不可约多项式$p(x) = x^8 + x^5 + x^3 + x + 1$，写出多项式$A(x) = x^7 + x^5 + x^3 + x^2 + x + 1, B(x) = x^6 + x^4 + x^3 + x + 1$的二进制表示，并求出$A(x) + B(x)\ mod\ p(x)$和$A(x) \cdot B(x)\ mod\ p(x)$

四，简答题（20 分）

考虑一个使用 AES 算法和 CBC 模式加密的场景，密钥长度为 128 位。给定以下信息：

明文： "Hello, CBC!"

初始向量（IV）： 0x0123456789ABCDEF0123456789ABCDEF

密文（十六进制表示）： 0x6A59DDE9072E97A8D85FAFE9769FAC11

请回答以下问题：

1)请画出 CBC 模式示意图，并且给出加密和解密函数。

2)CBC 模式中初始向量（IV）的作用是什么？为什么 IV 需要是随机且唯一的？

3)CBC 模式中的填充是什么？在加密过程中，为什么需要填充？

4)CBC 模式是否具有完全抵抗选择明文攻击（Chosen-Plaintext Attack）的能力？简要说明理由。