查看成绩

期中考试（一）

题目编号及标记说明

正确 错误 主观题

一、选择题

1 2 3 4

5 6 7 8

9 10

二、填空题

1 2 3 4

5 6 7 8

三、简答题

1 2

四、计算题

1 2

测验得分: **96.0** 分

期中考试（一）_2025

试卷描述 期中考试（一）

总题数: 22

总分: 100.0

第一部分: 选择题（共10道题）

1.从重合指数的定义可知，一个完全随机的文本其重合指数约为0.0385，而一个有意义的英文文本其重合指数却是( )左右 ✓

A.0.0185

B.0.0365

C.0.065

D.0.0385

2.AES轮函数由以下4个不同的模块组成，其中（）是非线性模块。 ×

A.字节代换

B.行位移

C.列混淆

D.轮密钥加

3.下列哪个是密码分组链接模式（） ✓

A.CBC

B.OFB

C.CTR

D.ECB

4.AES是一个分组长度为（）位分组加密算法 ✓

A. 56

B. 80

C. 128

D. 256

5.在相同的密钥下，相同的明文会得到相同的密文，而且能够实现明密文分组的并行处理，主要用于发送少量数据，这种分组密码的操作模式是指（ ） ✓

A.ECB

B.CBC

C.CFB

D.OFB

6.假设某一个仿射密码中，$P = C = Z_{26}, n = 26,$ 如果其加密变换为$E_k(x) = 7x + 3$，则其解密变换为 ( )。

A.$D_k(y) = 15y - 19$

B.$D_k(y) = 7y + 3$

C.$D_k(y) = 7y - 3$

D.$D_k(y) = 15y + 19$

7.计算复杂性是密码分析技术中分析计算量和研究破译密码的固有难度的基础，下列算法中，（）的运行时间是难解的。

A. $O(1)$

B.$O(n)$

C.$O(n^2)$

D.$O(2^n)$

8.一般来说，密码系统至少经得起的攻击是()

A.惟密文攻击

B.已知明文攻击

C.选择明文攻击

D.选择密文攻击

9.现代密码算法的设计中，真正保密的是()

A.明文

B.密文

C.密钥

D.公钥

10.维吉尼亚密码是（）

A.序列密码

B.置换密码

C.单表代换密码

D.多表代换密码

第二部分: 填空题（共8道题）

1.分组密码主要采用__原则和__原则来抵抗攻击者对该密码体制的统计分析

该生答案
扩散
，
混乱

教师反馈

请输入您对这道题的反馈信息. . .

2. 关于DES算法，密钥的长度（即有效位数）是__位，又其互补性使DES 在选择明文攻击下所需的工作量减半

该生答案
56

教师反馈

请输入您对这道题的反馈信息. . .

3.我国的商用分组密码标准是__算法

该生答案
SM4

教师反馈

请输入您对这道题的反馈信息. . .

4. DES算法中每一轮都有S盒运算，其中的一个S盒如下表所示，

	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

假设现有六位二进制数101110，经过上面的S盒映射后，输出的四位二进制数是____。

该生答案
1011

教师反馈

请输入您对这道题的反馈信息...

5.信息安全的主要目标是指__、__、__、和__、可用性

该生答案
机密性
，
完整性
，
认证性
，
不可否认性

教师反馈

请输入您对这道题的反馈信息...

6.一个保密系统一般是明文、密文__、__和解密算法组成。

该生答案
密钥
，
加密算法

教师反馈

请输入您对这道题的反馈信息...

7.1949年，香农发表题为__的论文，标志着密码学成为一门科学

该生答案
保密系统的通信理论

教师反馈

请输入您对这道题的反馈信息...

8.DES 的轮函数 F 是由四个部分： _____、密钥加、S盒和_____ 组成的。

该生答案
扩展置换（E盒）
，
置换运算（P盒）

教师反馈

请输入您对这道题的反馈信息...

第三部分: 简答题（共2道题）

1.简述DES与AES的至少三处相同点

该生答案
1.都是分组密码，都运用了扩散与混乱的设计思想
2.实现时都有使用S盒进行代换
3.都对密钥进行扩展
4.加解密过程中都有相同的轮密钥加的操作

教师反馈

请输入您对这道题的反馈信息...

2.简述密码学中的柯克霍夫原则

该生答案
秘密必须完全寓于密钥中，即加密和解密算法的安全性取决于密钥的安全性，而加密/解密的过程和细节（算法的实现）全的，攻击者就无法推导出明文。

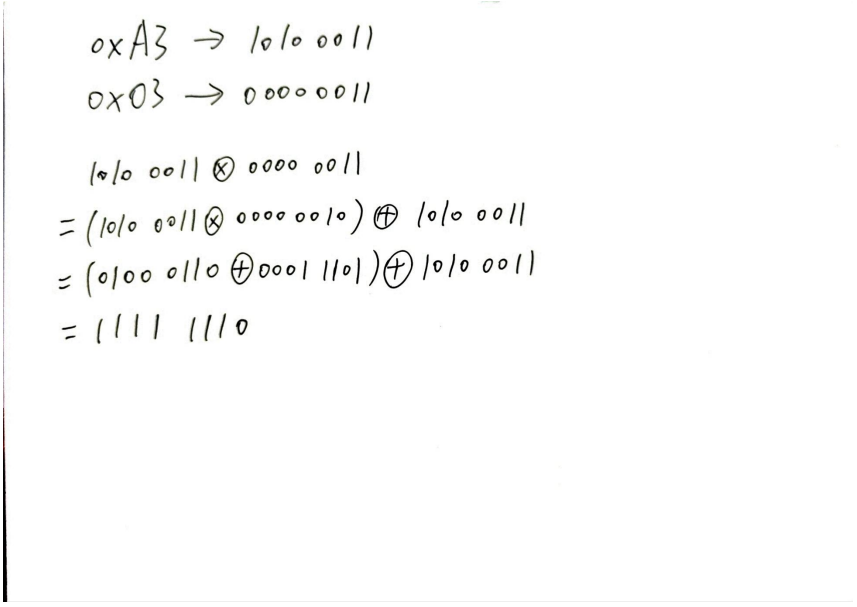
教师反馈

请输入您对这道题的反馈信息...

第四部分: 计算题（共2道题）

1.快速计算法，计算0xA3乘以0x03模m(x)= x8+x4+x3+x+1的值。

该生答案

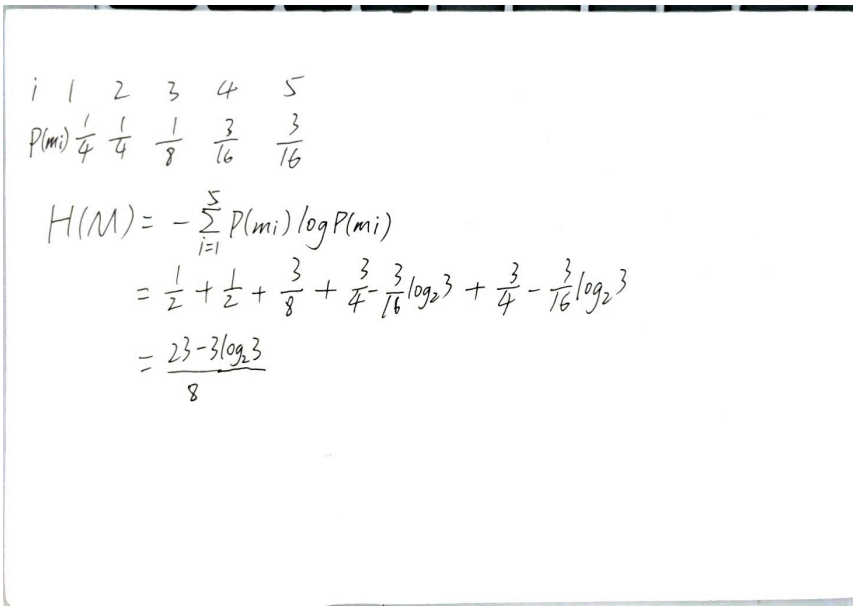


教师反馈

请输入您对这道题的反馈信息...

2.假设密文空间 M 共含有 5 个信息 $m_i(1 \le i \le 5)$ **,并且** $P(m_1) = P(m_2) = 1/4, P(m_3) = 1/8, P(m_4) = P(m_5)$ **,求 H(M)。**

该生答案



教师反馈

请输入您对这道题的反馈信息...