2023-2024-2《密码学》期中测试试题

一．选择题（共 10 小题，每小题 2 分，共 20 分）

1. 一个密码系统至少由明文、密文、加密算法和解密算法、密钥五部分组成，在算法确定的情况下，其安全性是由（ D ）决定的。

A．加密算法

B．解密算法

C．加密算法和解密算法

D．密钥

2．利用已有的最好的方法破译密码系统所需要的努力超出了破译者的破译能力（诸如时间、空间、资金等资源），那么上述密码系统的安全性是（ D ）。

A．无条件安全

B．实际上的安全

C．可证明的安全

D．计算上的安全

3. 字母频率分析法对下面哪种密码算法最有效。（ B ）

A．置换密码

B．单表代换密码

C．多表代换密码

D．序列密码

4. 维吉尼亚密码（Vigenere）以密钥为 crypto 对明文消息 goodluck 的加密结果是（ C ）。

A．cryptoab

B．krrgoxfn

C．ifmsdieb

D．faaeuctf

5. 以下哪种运算是 DES 算法中唯一的非线性变换操作？（ C ）

A．初始置换

B．循环移位

C．S 盒变换

D．异或运算

6. 关于 SPN 结构描述错误的是：（ C ）。

A. AES 算法采用了 SPN 结构

B. 加解密不一致

C. P 层主要起混淆作用

D. SPN 结构比 Feistel 结构扩散更快

7. 下列那种分组密码工作模式用于图片的加密可能会产生信息泄露（ B ）。

A. CBC

B. ECB

C. CFB

D. OFB

8. 线性分析是一种（ A ）攻击

A. 已知明文

B. 选择明文

C. 选择密文

D. 唯密文

9. 关于 *n* 级反馈移位寄存器的说法错误的是（ D ）。

A. *n* 级线性反馈移位寄存器生成序列的最大周期为 2^n-1

B. *n* 级非线性反馈移位寄存器生成序列的最大周期为 2^n

C. 对于任意 *n* 总是存在线性反馈函数使得其生成序列是 m 序列

D. 线性反馈移位寄存器的输出可以直接用作密钥流加密消息

10. 下列哪一个算法是我国商用 4G 移动通信密码标准：（ A ）。

A. ZUC

B. SM4

C. DES

D. AES

二．填空题（共 7 小题，每空 1 分，共 20 分）

1. 密码学是研究通信安全保密的科学，根据加解密密钥是否相同可分为：对称密码和非对称密码。

2. 香农（Claude Shannon）在遵循柯克霍夫（Kerckhoff）原则前提下，提出了设计密码系统的两个基本方法 混淆 和 扩散 。

3. 密码体制不仅涉及到加密和解密消息，还涉及到解决现实世界对信息安全的要求问题，密码体制的主要目标是保障信息的机密性、完整性、真实性和不可否认性。

4. AES 一轮加密涉及到 4 种操作：字节替代、行移位、列混合和轮密钥加。

5. 分组密码工作模式中，需要使用解密算法的模式是 ECB 模式和 CBC 模式。

6. 设计序列密码的关键是要设计一种产生密钥流的方法，具体可分为同步序列密码和自同步序列密码。

7. ZUC 算法和 Trivium 算法都是典型的同步序列密码，两种算法在工作阶段前都需要进行初始化，其中 Trivium 是一种面向硬件实现的序列密码。

三．计算题（共 4 小题，共 36 分）

1. (4 分)一个仿射密码的加密函数为 $c = 17m + 2 (\mathrm{mod}\ 26)$，求解密函数。

$$m = 23c + 6 (\mathrm{mod}\ 26)$$

2. (8 分)设英文字母 a，b，c，……，z 分别编码为 0，1，2，3，4，……，25，已知 Hill 密码中的明文分组长度为 2，密钥 K=$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ 是 Z_{26} 上的一个二阶可逆方阵。假设密文为 XIYJ，试求所对应的明文。

解：设 n=2，密钥 K=$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ 容易计算 $K^{-1}=\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

而密文为：XIYJ，则相应的密文向量为（23，8）和（24，9），

于是，c=$\begin{pmatrix} 23 & 8 \\ 24 & 9 \end{pmatrix}$

相应的明文矩阵为：$m= c K^{-1} \mathrm{mod} 26=\begin{pmatrix} 23 & 8 \\ 24 & 9 \end{pmatrix}\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}=\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$,

从而所求的明文为：Hill。

3. (16 分)令 GF（2^8）表示 AES 算法中使用的包含 256 个元素的有限域（其使用的不可约多项式为$x^8 + x^4 + x^3 + x + 1$），

(1) $a = 0xe2, b = 0x3a,$ 求 ab 的值；(4 分)

(2)令 $a = 0x2,$ 求 a 的乘法逆元。 (6 分)

(3)AES 中一个重要步骤涉及四字节多项式乘法可化简为矩阵乘法，即

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

若$(x_1, x_2, x_3, x_4)^T = (87, 6E, 46, A6)^T$试求 y_4(6 分)

解：ED

4. (8 分) 一个 GF(2)上的 4 阶 LFSR，其特征多项式为$g(x) = x^4 + x + 1$，若初始状态为（s_0, s_1, s_2, s_3）=（1001），请画出该 LFSR 的逻辑图，并写出输出序列及状态变迁。

四．论述题（共 2 小题，共 24 分）

1. (12 分)在 DES 的 ECB 模式中，如果密文的一个分组在传输中出现了错误，解密后仅相应的明文分组受到影响。

(1) 试画出分组密码 CBC 工作模式的加解密流程图；（6 分）

(2) 在 CBC 模式中，密文分组 C1 在传输中出现了一个错误，解密时将会影响几个分组？ (3 分)

P1,P2 错误，其他无影响。

(3) 在 CBC 模式中，明文分组 P1 在加密前出现了 1 bit 错误，这一错误将在多少个密文分组中传播？接受者解密后多少组明文是错误的？ (3 分)

错误传播至所有密文分组；解密后只 P1 错误，其他均正确。

2. (12 分) 论述 DES 算法和 AES 算法的异同点，并详细阐述 DES 算法和 AES 算法的轮变换算法（可图示说明）。