电子科技大学 2024-2025 学年第二学期期中考试卷 A 卷

课程名称:密码学 考试形式:闭卷 使用教师:

学院:_____ 姓名:_____学号:_____

一、填空题(每空 2 分, 共 20 分)

1. DES 分组加密算法使用的密钥长度为____位，其中有效密钥为____位，另外_____位是奇偶校验位。

2. AES 分组加密的轮结构由四个不同的模块组成，其中_____是非线性模块。

3.凯撒密码是古典密码体制比较有代表性的一种密码, 其本质是一种_____密码。

4.设计分组密码系统的两个基本思想是_____和_____。

5. 分组密码主要有两种迭代结构，分别是_____和_____。

6. 明文或密钥的微小变化将对密文产生很大的影响，这是分组密码的_____效应。

二、选择题(每小题 4 分, 共 20 分)

1. 以下几种分组密码的操作模式中，密文接受错误会造成解密时错误传播的操作模式是( )。

A. ECB 模式 B. CRT 模式 C. OFB 模式 D. CFB 模式

2. 根据密码分析者所掌握的分析资料的不同，密码分析一般可为四类：惟密文攻击、已知明文攻击、选择明文攻击、选择密文攻击，其中破译难度最小的是 ( )。

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

3. 字母频率分析法对下面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

4. AES 算法以字节为单位对明文进行处理, 在处理的过程中的每一个状态均可表示为一个矩阵, 其密钥也按上述方法进行排列。如果密钥长度为 256 比特, 则密钥状态为( )的矩阵。

A. 4 行 6 列 B. 4 行 8 列 C. 4 行 10 列 D. 4 行 4 列

5.下列古典密码算法中最能抵抗统计分析的是 ( )。

A. 加法密码 B. 乘法密码 C. 仿射密码 D. 多表代换密码

三、计算问答题（每道题 20 分，共 60 分）

1. 设多表代换加密为$E_{A,B}(M) = A \cdot M + B \mod 26$，对明文 rsa 使用密钥

$$A = \begin{pmatrix} 2 & 11 & 19 \\ 23 & 5 & 25 \\ 7 & 20 & 17 \end{pmatrix}, B = \begin{pmatrix} 21 \\ 6 \\ 14 \end{pmatrix}$$

进行加密，并解密验证你的计算结果。(20 分)

2，设敌手得到密文串 11100110001011 和其对应的明文串 01011010101010，加密该密文的密钥流是由一个 5 级线性反馈移位寄存器得到，求该 5 级线性反馈移位寄存器的反馈函数并画出该 5 级线性反馈移位寄存器。（20 分）

3，请给出 AES 算法在不同密钥长度（128、192、256 位）下的加密解密的迭代轮数，并说明除最后一轮外，加密时和解密时分别包含哪四个函数运算。（20 分）