1．是非判断题

(1)在分组密码中，分组或密钥越长意味着安全性越高，因此，在实际应用中应选用分组和密钥都长的分组密码算法。(X) 注：一般密钥越长，加解密效率越低

(2)分组密码一般采用简单的、安全性弱的加密算法进行多轮迭代运算，使得安全性增强。一般来说，分组密码迭代轮数越多，密码分析越困难。(V)

(3)分组密码的实现往往需要多轮迭代运算，而每轮运算使用的密钥是相同的，即分组密码的初始密钥。(X) 注：子密钥，每轮不同

(4)在分组密码中，分组或密钥的长度应足够长，至少能够抵御穷举攻击。(V)

注：由于算法是公开的

(5)在分组密码中，分组长度、密文长度以及密钥长度都是一样长的。(X)

(6)DES 算法中，其初始置换和逆初始置换与 DES 算法的安全强度无关。(V) 注：因没有密钥参与

(7)DES 作为加密算法现很少直接使用,其主要原因是 DES 的算法已被破解,不安全了。(X)

注：因为密钥 56 位太短

(9)多重 DES 就是使用多个密钥利用 DES 对明文进行多次加密，然而总会找出一个多重 DES 密钥与一个单重 DES 密钥相对应。(X)

(10)多重 DES 使得密钥长度增加，同时分组长度也会发生相应改变。(X)

(11)在高级加密标准(AES)规范中，分组长度和密钥长度均能被独立指定为 128 位、192 位或 256 位。(X)

注：分组长度 128 位不变

(12)AES 同 DES 一样，其加密算法和解密算法是相同的。(X) 注：AES 不同

(13)在实际运用中，需要加密消息的数据量是不定的，数据格式可能是多种多样的，选取合适的分组密码操作模式能提高整体的安全性。(V)

2．选择题

(1)在(C)年，美国国家标准局 NBS 把 IBM 的 Lucifer 方案确定数据加密标准，即 DES。

A. 1949　　B. 1972　　C. 1977　　D. 2001

(2)在现代密码学发展史上，第一个广泛应用于商用数据保密的密码算法是(B)。

A. AES　　B. DES　　C. RSA　　D. RC4

(3)1977 年由美国国家标准局（NBS）批准的联邦数据加密标准 DES 的分组长度是 (B)。

A. 56 位　　B. 64 位　　C. 112 位　　D. 128 位

(4)在现有的计算能力条件下，对于对称密码算法，被认为是安全的密钥最小长度是(B)。

A. 64 位　　B. 128 位　　C. 512 位　　D. 1024 位

(5)分组密码算法主要解决信息安全存在的 (A) 问题。

A. 保密性　B. 完整性　C. 认证性　D. 不可否认性

(6)在分组密码算法中，如果分组长度过短，那么攻击者可利用(C)来破解。

A. 唯密文攻击　B. 已知明文的攻击　C. 选择明文攻击　D. 选择密文攻击

注：建立所有明密文对，然后根据明文就能找到对应密文了

(7)AES 算法具有很好的雪崩效应，在经过(B)轮变换后，所有的输出位均与所有的输入

位相关。

A. 1　　B. 2　　C. 3　　D. 4

注：字节代换使得字节与每位有关，列混淆使得字节与其它四字节有关，列位移使得列四字节扩散到不同列中，

(8) 密钥长度为 128 位的 AES 算法中，其轮函数迭代次数应为（ A ）。

A. 10　　B. 16　　C. 20　　D. 32

(9) AES 结构由以下四个不同的模块组成，其中（ A ）是非线性模块。

A. 字节代换　　B. 行位移　　C. 列混淆　　D. 轮密钥加

(10) 国家商用密码管理办公室制定了一系列密码标准，其中（ D ）是算法公开的且是分组算法。

A. SM1　　B. SM2　　C. SM3　　D. SM4

(11) 下面那种分组密码的操作模式主要用于内容较短且随机的报文的加解密处理。（ A ）

A. 电子密码本模式 B. 密码分组链接模式　C. 密码反馈模式 D. 输出反馈模式

(12) 下面那种分组密码的操作模式具有可预处理、可并行处理多块明(密)文、以及可随机访问任一块明(密)文。（ C ）

A. 电子密码本模式 B. 密码分组链接模式　C. 计数器模式　D. 密文反馈模式

3. 填空题

(1) 分组密码主要采用 混淆 原则和 扩散 原则来抵抗攻击者对该密码体制的统计分析。

(2) 轮函数是分组密码结构的核心，评价轮函数设计质量的三个主要指标是 非线性 、 高效 和 雪崩效应 。

(3) DES 的轮函数 F 是由三个部分： 选择扩展运算 、选择压缩运算 S 盒 和 置换运算 P 组成的。

(4) 就目前而言，DES 算法已经不再安全，其主要原因是 密钥(56 位)太短，在目前计算能力下，不能抵御穷举攻击 。

(5) 分组密码的加解密算法中最关键部分是非线性运算部分，那么，DES 加密算法的非线性运算部分是指 选择压缩运算 S 盒 ，AES 加密算法的非线性运算部分是指 字节代换 。

(6) 在高级加密标准 AES 规范中，分组长度只能是 128 位，密钥的长度可以是 128 位 、 192 位、 256 位中的任意一种。

(7) DES 与 AES 有许多相似之处，也有一些不同之处，请指出两处不同：（其实有很多不同）

譬如，DES 针对比特位处理，AES 针对字节处理；DES 密钥固定 56 位，AES 可有 128 位，192 位，256 位三种选择；DES 加密算法可用作解密算法，AES 加密算法和解密算法是不同的。

4. 思考题

(1) DES 算法具有互补性，而这个特性会使 DES 在选择明文攻击下所需的工作量减半。简要说明原因。

见教材 P81

(2)为什么二重 DES 并不像人们相像那样可提高密钥长度到 112 比特，而相当 57 比特？简要说明原因。

见教材 P84

(3)请了解国密 SM4 加解算法的实现过程，并简要说明 SM4 算法分别与 DES 算法、AES 算法的相似之处。

SM4 算法与 DES 算法、AES 算法所采用的设计原理相同，即扩散和混淆；

SM4 使用类似 DES 的 Feistel 的结构，每轮 DES 处理 1/2 分组，SM4 处理 1/4 分组；

SM4 加解密算法同 DES 是可复用的，即加密算法也可用于解密算法；

SM4 的非线性部分类似 AES 的字节代换；

SM4 的线性变换 L 中的移位类似 AES 的行移位；

SM4 的子密钥生成部分类似 AES 的子密钥生成部分，递归迭代并含有非线性部分；