应用密码学练习和复习习题集

第一题　填空（说明：请把答案填在题目中的横线上。）

1、根据对明文和密文掌握的程度，密码分析者通常可以在下述五种情况下对密码体制进行攻击：唯密文攻击，_____，选择明文攻击，选择密文攻击，选择文本攻击。

2、美国国家标准局在 2000 年 9 月发布的“信息保障技术框架（IATF）3.0”版本中将攻击形式分为被动攻击、_____、物理临近攻击、内部人员攻击和软硬件配装攻击等 5 类。

3、在 DES 密钥长度为 64bits，则明文分组长度为_____bits。

4、一个消息经过 SHA-512 处理后，生成_____bits 的消息摘要 。

5、美国在 NIST-SP800 中定义了五种运行模式，ECB、CBC、CTR、_____、OFB。

6、在序列密码中，假设当前的明文字为 01101011，加解密均为按位异或运算，若密文字为 11011100，则当前密钥串为_____。

7、在网络中，有 1000 个用户使用 RSA 公钥密码算法进行两两保密通信，则至少需要生成 _____对密钥。

8、AES 算法中，每一轮基本运算为字节替代、行移位、_____、轮密钥加四种运算。

9、认证协议从对认证实体认证来看，主要有单向认证和_____ 两种。

10、工作密钥，也称为_____或者会话密钥，是在一次通信或数据交换中，用户之间所使用的密钥，它可由通信用户之间进行协商得到。它一般是动态地、仅在需要进行会话数据加密时产生。

11. 一个密码体制或密码算法通常由以下 5 个部分构成：明文空间、密文空间、_____、加密算法和_____。

12. 从收发双方使用的密钥是否相同，密码体制可以分为对称密码体制和_____。

13. AES 算法的明文分组长度为_____，密钥长度有 128/192/256bits 三种选择。

14. 美国在 NIST-SP800 标准中定义了五种运行模式，包括 ECB、CBC、_____ 、_____、CFB 等。

15. 在序列密码中，根据状态函数是否独立于明文或密文，可以将序列密码

分为_____和自同步序列密码两类。

16. 杂凑算法 SHA-1 生成消息摘要值的长度为_____。

17. 已知一个 RSA 数字签名算法以{e,n}为公开密钥，{d,n}为秘密密钥。H( )是公开的安全哈希算法。如果签名算法为：$s \equiv H(m)^d \bmod n$，则验证算法为：_____。

18. 工作密钥，也称为数据加密密钥或者_____，是在一次通信或数据交换中，用户之间所使用的密钥，它可由通信用户之间进行协商得到。它一般是动态地、仅在需要进行会话数据加密时产生。

19、根据对明文和密文掌握的程度，密码分析者通常可以在下述五种情况下对密码体制进行攻击：唯密文攻击，_____，选择明文攻击，选择密文攻击，选择文本攻击。

20、已知构造有限域时使用的不可约多项式为 $x^8+x^4+x^3+x+1$，请使用有限域 $GF(2^8)$上的字节运算方法计算 *16* 进制的*"E0"*与*"09"*的加法，即计算*"E0+09"*的值=_____(十六进制表示)。

21、一个消息经过 SHA-256 处理后，生成_____比特的消息摘要 。

22、在 DES 算法的各种变形中，DES-EEE3 模式的有效密钥长度为_____比特。

23、信息安全根据其本质的界定，应具有以下基本属性：保密性、_____、_____、不可否认性、可控性、可审查性。

24、美国在 FIPS 中定义了五种运行模式，电子码本（ECB）、_____、_____、密码反馈（CFB）、输出反馈（OFB）

25、DES 和 RC4 从明文分组角度划分，DES 属于分组密码，RC4 属于流密码（序列密码），若从密钥角度，DES 属于对称密码体制，RC4 属于_____密码体制。

26、-2 mod 11 =_____。

27、一个消息经过 SHA-512 处理后，生成_____比特的消息摘要 。

28、在 DES 算法的各种变形中，DES-EDE2 模式的有效密钥长度为_____比特。

29、4 级线性反馈移位寄存器产生的序列$\{a_i\}$的周期达到最大值_____时，称$\{a_i\}$为 m 序列 。

30、AES 算法明文分组长度是_____比特，密钥长度有三种分别为

128bits、_____、_____。

31、在一般的密码系统中，密钥一般以层次化结构进行分成，按照密钥作用分，从下到上一般为会话密钥（数据加密密钥），_____ 和主密钥。

第二题　判断题（说明：判断正误。把你的判断填在题目后边的括号中。对的打“√”，错的打“×”。）

1、3DES 的 EDE 模式中，加密过程为加密-解密-加密，其解密过程则为解密-加密-解密。（　）

2、AES 算法采用暴力破解，明文搜索空间和密钥搜索空间完全一样，搜索空间为 2^{128}。（　）

3、在 ECB 模式加密下，在同一密钥作用下，内容相同的明文分组，一定会被转换为内容相同的密文分组。（　　）

4、在序列密码中，根据状态函数是否独立于明文或密文可分为同步序列密码和自同步序列密码。若密钥流是独立于消息流而产生，则为自同步序列密码。（　　）

5、RSA 算法的安全性是基于大数分解困难性问题。（　　）

6、使用 SHA-1 算法对消息进行哈希，10MB 的消息得到的哈希值比 100GB 的消息的哈希值要短。（　　）

7、SHA-1 算法中，若消息仅改写 1 比特，则哈希值也仅发生 1 比特改写。（　　）

8、要找出和某条消息具备相同哈希值的另外一条消息是非常困难的。（　　）

9、 RSA 可提供数字签名。（　　）

10、按照层次化密钥结构，若分成三层，从第一层到第三层，分别为主密钥、密钥加密密钥、会话密钥，则三种密钥中，生命周期最短的是第一层主密钥。（　　）

11. 维吉尼亚密码是一种单字符单表替换密码技术。　（　　）

12. DES 算法被弃用的原因，不是因为算法不安全，而是因为有效密钥太短，抵御不了穷尽搜索攻击。　（　　）

13. 即使有了安全的分组密码算法，也需要采用适当的工作模式来隐蔽明文的统计特性、数据的格式等，以提高整体的安全性，降低删除、重放、插入和伪造成功的机会。　（　　）

14. 序列密码算法安全性依赖于产生密钥流的算法的保密。（　　）

15. 20 世纪 70 年代，Diffie 和 Hellman 发表了非对称密码的奠基性的论文“密码学的新方向”，建立了公钥密码的概念，引起了广泛关注。（　　）

16. RSA 算法能抵御已知明文攻击，不能抵御选择明文攻击。（　　）

17. 哈希值是不可逆的，消息认证码是可逆的。（　　）

18. 中华人民共和国电子签名法已经施行多年。（　　）

19. QQ 登录过程中，用户通过的 QQ 号码和对应的口令对 QQ 服务器进行了认证。（　　）

20. 密码系统的安全强度由系统中最薄弱的环节决定的。（　　）

21、MD5 哈希算法可以处理任意长度的消息。（　　）

22、 若采用穷举搜索的方法破解 AES 和 DES，破解 AES 的代价要高于 DES。（　　）

23、RSA 算法的安全性是基于离散对数求解的困难性问题。（　　）

24、按照层次化密钥分结构，若分成三层，从第一层到第三层，分别为主密钥、密钥加密密钥、会话密钥，则三种密钥中，要求会话密钥必须密文保存，并且生命周期最长。（　　）

25、对于一个指定的哈希函数（散列算法），要求不论消息输入长短，得到的消息摘要值的长度都是相同的。（　　）

26、AES 密码算法，明文分组长度有三种情况 128bits、256bits、192bits（　　）

27、数字签名算法中，得到签名的长度必定远远小于被签消息的长度（　　）。

28、RSA 公钥密码算法是由 Ron Rivest、Adi Shami 和 Leonard Adleman 一起提出的。（　　）

29、n 级线性反馈移位寄存器，若特征多项式是本原多项式，则产生的密钥流是 m 序列（　　）

30、DES 算法和 AES 是典型的 Feistel 结构算法（　　）

31、古典密钥 “滚筒密码”则是属于替代密码（　　）

32、常采用哈希算法和公钥密码算法共同设计数字签名算法（　　）

33、AES 算法是美国研究者设计提出的（　　）

34、RSA 算法的安全性，是基于大整数分解困难性问题。（　　）

35、在公钥密码体制应用中，为了消息保密性，发送方利用发送方公钥对消息加密，然后发送给接收方（　　）。

36、哈希算法只能应用在数字签名中，不能用于设计消息认证（　　）

第三题　单项选择（说明：在每小题所给的四个选项中，选择一个最符合题意的选项，填在题目的括号中）。

1、下列有关古典密码体制叙述**错误**的是（　）

A、凯撒密码体制和维吉尼亚密码体制都属于对称密码算法；

B、凯撒密码体制和仿射密码体制都属于替代密码；

C、仿射密码体制不能抵抗穷举攻击（暴力破解）；

D、仿射密码体制是一种非对称密码算法。

2、假设 AES 的密钥长度为 128bits，进行密钥扩展，需要 RoteWord（字循环移位），SubBytes（字节替代），Rcons（常量值）运算，则把上述 3 运算分别填入图中，完成密钥扩展的示意图。

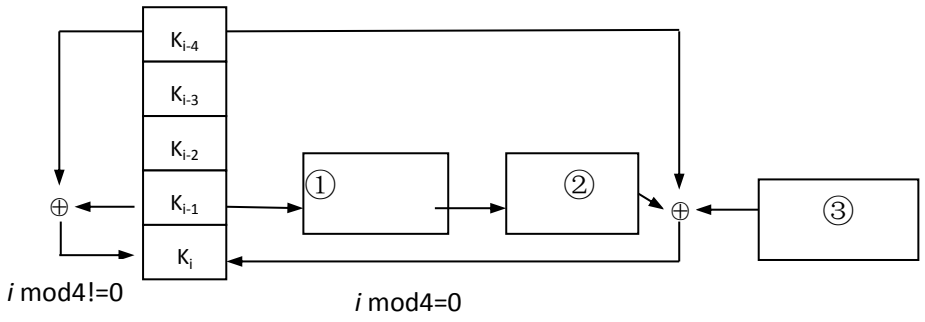


图 1　AES-128 比特密钥的扩展规则示意图

则①，②，③填完顺序为（　　）

A、RoteWord，SubBytes，　Rcons；

B、RoteWord，　Rcons , SubBytes；

C、Rcons　，SubBytes，RoteWord　；

D、SubBytes, Rcons , RoteWord。

3、关于线性反馈移位寄存器，描述**正确**的是（　）

A、n 级线性反馈移位寄存器的状态周期小于 2^n-1；

B、n 级线性反馈移位寄存器的状态周期等于 2^n-1；

C、 n 级线性反馈移位寄存器，每一状态对应于 GF(2)上的一个 n 维向量，共有 2^n-1 种可能的状态；

D、n 级线性反馈移位寄存器产生序列$\{a_i\}$为 n 级 m 序列，则周期达到最大值 2^n-1 。

4、下面关于 RSA 算法，说法**错误**的是（　　）

A、RSA 算法密钥生成过程中，私钥的产生需要采用欧几里得扩展算法求逆；

B、RSA 算法密钥生成过程中，需要产生大素数，而通过米勒罗宾素性检测算法检测的数不能保证百分之百为素数；

C、若两用户采用 RSA 算法进行通信，发送者发送信息给接收者，则发送者使用自己公钥加密信息，然后发送给接收者；

D、RSA 的加密和解密过程都需要模幂运算，为了提高模幂运算效率，可采用模重复平方和平方乘算法来实现模幂运算。

5、下面关于 RSA 算法安全性，说法**错误**的是（　）

A、不同的用户不能用相同的模数 n；

B、RSA 算法能抵御共模攻击，不能抵御选择明文攻击；

C、在密钥生成中，两素数 p 和 q 的差值要大；

D、在密钥生成中两素数 p 和 q，　p-1 和 q-1 都应有大的素因子。

6、下面关于 Hash 算法说法**正确**的是（　）

A、MD5 能够将任意长度的消息变换为 128 bits 的输出，也能够把 128bits 的输出还原回原始输入消息；

B、要找出具有相同哈希值但互不相同的两条消息是非常困难的；

C、SHA-1 算法中，输入消息长度变化，哈希值长度也跟着变化；

D、如果消息仅被改写 1 bit，则哈希值也仅改变 1 bit。

7、下面关于消息认证码说法**正确**的是（　）

A、使用消息认证码无法保证消息的机密性；

B、使用消息认证码无法识别出篡改行为；

C、使用消息认证码不需要发送者和接收者之间共享密钥；

D、使用消息认证码能够防止否认。

8、有关消息认证码和数字签名区别，说法**错误**的是（　）

A、数字签名用签名者的私钥签名，签名者的公钥验证；

B、数字签名和消息认证都能提供消息完整性；

C、数字签名可以保证消息的机密性，不用担心被窃听；

D、数字签名可以防止否认。

9、在下面的协议中，A 和 B 表示两用户，KDC 为密钥分配中心，ID_a，ID_b 分别为 A 和 B 的用户 ID 号，K_a 为用户 A 和 KDC 共享密钥，K_b 为用户 B 和 KDC 共享密钥，K_s 为临时会话密钥，N_1 为随机数，则协议步骤如下：

① $A \rightarrow KDC$：$ID_a \| ID_b \| N_1$

② $KDC \rightarrow A$：$E_{K_a}[K_S \| ID_b \| N_1 \| E_{K_b}[K_S \| ID_a]]$

③ $A \rightarrow B$：$E_{K_b}[K_S \| ID_a] \| E_{K_S}[M]$

则关于上述协议描述说法**错误**的是（　）

A、该协议实现了对 B 的身份认证；

B、该协议实现了对 A 的身份认证；

C、该协议的目的是协商 A 和 B 的临时会话密钥 K_s；

D、协议无法防止重放攻击。

10、关于密钥管理，下面描述**正确**的是（　）

A、由于密钥由随机数发生器产生，是随机的比特序列，因此别人知道也没有关系；

B、公钥密钥算法中，私钥可以公开；

C、密钥必须定期更换；

D、会话密钥是整个密钥管理系统的核心。

11. 关于密码分析，下面说法**错误**的是：(　　)

A. 通常来说，一个密码系统的密码算法是公开的。

B. 惟密文攻击攻击由于只知道算法和密文，因而这种攻击是最难的。

C. 仿射密码技术能够抵御选择明文攻击。

D. 高级加密算法（AES）能够抵御已知明文攻击。

12. 关于数据加密标准 DES 算法，下面说法**错误**的是：(　　)

A. DES 算法的变型之一 3DES-EDE2 模式的有效密钥长度为 112bits。

B. DES 算法加密一组明文，要执行 16 次轮结构。

C. DES 算法中一共有 8 个不同的 S 盒。

D. DES 算法的轮子密钥长度为 56bits。

13. 同步密钥流生成器模型**不具有**的特点是：(　　)

A. 密钥流的产生不是独立于明文流和密文流的，与种子密钥和其前面已产生若干密文字有关。

B. 在传输期间，一个密文字（或位）被改变只能影响该密文字（或位）的恢复，不会对后续密文字（或位）产生影响。

C. 一个主动攻击对密文进行插入、删除或重放操作都会立即破坏其同步，从而可能被解密器检测出来。

D. 在一个同步序列中，发送方和接收方必须是同步的，即用同样的密钥且该密钥操作在同样的位置，才能保证正确的解密。

14. 下面选项中，哪一个**不是**实用的非对称密码体制应该满足如下的性质：(　　)

A. 接收方 Alice 产生密钥对（公钥 PK_A 和私钥 SK_A）在计算上是容易的。

B. 消息发送方 Bob 用接收方 Alice 的公钥对消息 m 加密以产生密文 c 是容易的。

C. 接收方 Alice 用自己的私钥 SK_A 对 c 解密是容易的。

D. 计算能力强的机构如 Google 公司可以通过穷举搜索的方式解密非对称密码算法加密得到的密文。

15. 对比 AES 算法和 RSA 算法，下面说法**错误**的是：(　　)

A. RSA 出现在 1978 年，而 AES 算法在出现 2002 年，因而使用 AES 算法加密消息比使用 RSA 算法更安全。

B. 在对消息进行同等强度的保密时，AES 算法比 RSA 算法的加解密速度更快。

C. AES 是对称密码算法，用于加密的密钥也可以用于解密。

D. RSA 是非对称密码算法，知道加密密钥不能去解密对应的密文。

16. 对于哈希函数的描述，下面说法**错误**的是：(　　)

A. 算法 SHA-256 生成的消息摘要值的长度为 256bits。

B. 中国的消息摘要算法是 SM3。

C. 算法 MD5 的消息摘要长度为 160bits。

D. 杂凑算法 SHA-1 把消息分成 64 字节一块进行消息摘要值的计算。

17. 下面对哈希函数的描述，**错误**的是：(　　)

A. Hash 函数是一公开函数，可以将任意长的消息 m 映射为较短的、固定长度的一个值，记为 $H(m)$，经常称函数值 $H(m)$为散列值。

B. 对任何消息输入都能够容易和快速地以相同的时间计算出哈希值。

C. 给定消息 m 和 $H(m)$，找到另外一个消息 $m \neq m'$，使 $H(m)= H(m')$在计算上是不可能的。

D. 给定 $H(m)$，恢复消息 m 在计算上是不可行的。

18.关于数字签名算法，下面描述**错误**的是：(　　)

A. 通常会使用哈希函数。

B. 如果使用公钥密码算法，则应该采用“私钥签名，公钥认证”模式。

C. 用户使用方便，可以把一个电子文档的签名复制给另一个文档。

D. 对签名者而言，不可以事后否认所完成的签名。

19. 在下面的协议中，M 是消息，H( )是公开的安全哈希算法。Alice 用自己的私钥 SK_A 实现了对 M 的摘要值的签名，并把相关信息发送给 Bob。

$$Alice \rightarrow Bob: M \,||\, E_{SK_A}[H(M)]$$

下面描述**错误**的是：(　　)

A. 该协议实现了对 Alice 的身份认证。

B. 该协议中消息实现了对 M 的保密功能。

C. Alice 事后不能否认发送过消息 M。

D. 该协议实现了对消息 M 的完整性验证。

20. 关于密钥管理，下面描述**错误**的是：(　　)

A. 表示用户身份的用户密钥和用于数据加密的数据加密密钥的生命周期一般相同。

B. 层次化的密钥结构可以实现最底层密钥每加密一份报文就更换一次。

C. 密钥必须定期更换。

D. 主密钥是整个密钥管理系统的核心。

21、下列有关古典密码体制叙述**错误**的是（　）

A、凯撒密码算法是一种对称密码算法

B、维吉尼亚密码算法是一种非对称密码算法

C、凯撒密码算法和维吉尼亚密码算法都属于替代密码

D、古代“滚筒密码”则是属于换位（置换）密码。

22、下面有个流密码体制叙述叙述**正确**的是（　）

A、n 级线性反馈移位寄存器，若特征多项式是本原多项式，只要寄存器的初始值不全为 0，则产生的密钥流是 m 序列。

B、计数器模式（CRT）中密钥流的产生属于自同步密钥流方式。

C、密码反馈（CFB）中密钥流产生属于同步密钥流方式。

D、线性反馈移位寄存器的特征多项式必须是本原多项式。

23、假设 AES 的密钥长度为 128 比特，进行密钥扩展的示意图如图 1 所示，

在空格中选择合适的变换，完成密钥扩展的示意图。

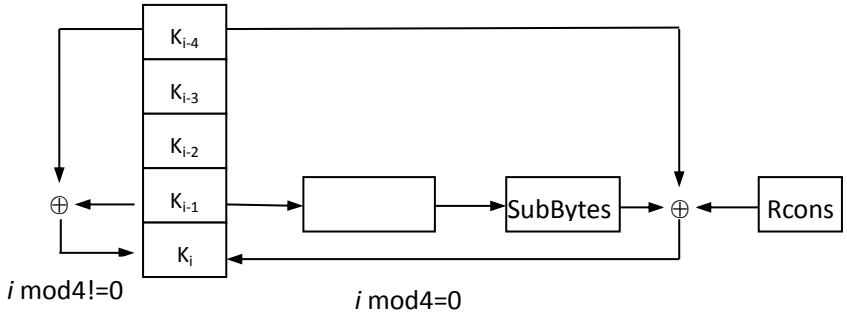


图 1 AES-128 比特密钥的扩展规则示意图

A、MixColumns ；　　B、ShiftRows；

C、RoteWord；　　D、AddRoundKey.

24、下面有关分组密码叙述错误的（　　）

A、DES 算法和 AES 是典型的 Feistel 结构算法。

B、NIST 已经建议停止使用 DES 算法作为标准。

C、AES 算法可以看作是 Rijndael 算法的子集。

D、序列密码中的密钥流生成器可以用 DES 算法或 AES 算法来设计产生。

25、对于数字签名，下列描述**错误**的是 （　　）

A、常采用哈希算法和公钥密码算法共同设计数字签名算法

B、RSA 签名算法中，被签消息采用私钥签名，公钥验证

C、数字签名算法，当发生纠纷时，要求可由第三方验证签名真实性

D、常用哈希算法和对称密码算法共同设计数字签名算法

26、下面不是 25 的本原元 （　　）

A、2　　B、3　C、4　　D、8

27、下列有关密码攻击**错误**的是（　）

A、唯密文攻击的难度要高于选择明文攻击

B、仿射密码能抵抗穷举攻击

C、仿射密码不能抵抗唯密文攻击

D、古典密码中，置换密码（换位）不能抵抗穷举攻击

28、已知仿射密码加密过程可以定义为 c=k*m+b(mod 26)，其中 c 为密文，m 为明文，密钥为(k,b)，下面哪个选项密钥参数不满足仿射密码对密钥的要求。（　）

A、k=5，b=4；B、k=7，b=7；　C、k=11，b=5；D、k=13，b=7

29、下图 1 是 S 盒中的 S1，如果输入为（111010），则输出应为（　）

S_i		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	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　DES 算法 S 盒

A、3 ；　B、10；　C、5；D、0

30、下面有关哈希算法叙述错误的（　　）

A、MD5 哈希算法中，消息长度可以大于 2^{64}bits。

B、SHA-1 哈希算法中，消息长度不能大于 2^{64}bits。

C、大小为 64Mbits 的消息，经过 MD5 哈希之后，哈希摘要值的长度为 512bits。

D、大小为 64Mbits 的消息，经过 SHA-1 哈希之后，哈希摘要值的长度为 160bits。

31、下列描述**错误**的是 （　　）

A、密码工作模式中，ECB（电码本）模式中，若两组明文相同，则输出的密文是不同的。

B、RSA 公钥密码算法是由 Ron Rivest、Adi Shami 和 Leonard Adleman 一起提出的。

C、DH 密钥协商协议易遭受中间人攻击。

D、数字签名算法中，得到签名的长度不一定小于被签消息的长度。

32、在 RSA 算法中，取 p=3，q=11，e=7，则私钥参数 d 等于（　　）

A、7　　B、1　　C、3　　D、5

第四题　综合问答题

1、此题是关于维吉尼亚密码的考查）

记 Z_{26}={0,1,2,3,…,25}分别表示 26 个字母，即 a 对应 0，b 对应 1，…。则密钥 k=(k_1, k_2, …, k_n)，明文 m=(m_1, m_2, …, m_n)，密文 c=（c_1, c_2, …, c_n)，其中 c_i,m_i,k_i ∈Z_{26}。则维吉尼亚密码加密函数如下：

$E_k(m_1, m_2, \ldots, m_n)=((m_1+k_1) \bmod 26, (m_2+k_2) \bmod 26, \ldots, (m_n+k_n) \bmod 26$

= $c_1, c_2, \ldots, c_n$。

（1）写出维吉尼亚密码的解密函数。

（2）若密钥 k=(5, 2, 1)，明文为 bye，求密文。

2、此题是对 DES 算法的考查，共 2 题。

（1）图 2 给出了 DES 算法的轮结构，其中 F 变换主要包括 P 盒置换、E 盒扩展、S 盒压缩 3 个变换。把上述 3 个变换按照正确顺序分别填入图中，完成轮结构图。

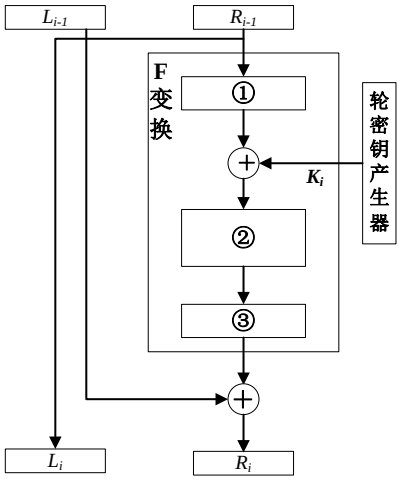


图 2　DES 算法轮结构

（1）完成题目中的填空；

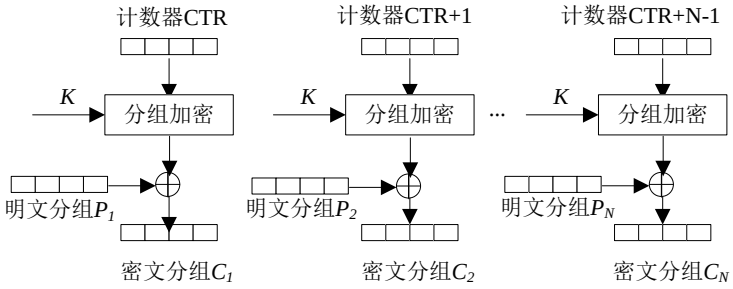
①_____；　②_____；③_____。

（2）下图 3 是 S 盒中的 S_1，如果输入为（111011），则输出应为_____　。

S_i		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	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 3　DES 算法 S 盒

3、此题是对分组密码的工作模式考查，共 2 题。（1）图 4 是某分组密码算法的 CTR 工作模式的加密过程，参照加密过程，请画出 CTR 工作模式的解密过程示意图。



(a) 加密

图 4 CTR 工作模式加密过程

（2）某密码算法采用 CBC 工作模式，则解密过程中，若密文分组第 2 组，第 3 组同时出错，会影响几组密文分组无法正常解密？

4、此题是对 RSA 算法考查，共 2 题。

为了更好理解 RSA 算法， 把 RSA 算法放入保密通信，如图 5 所示。假设 RSA 算法的公钥 e=7，模数 n=143，私钥 d=103。则私钥{d=103，n=143}和公钥参数{e=7，n=143}。

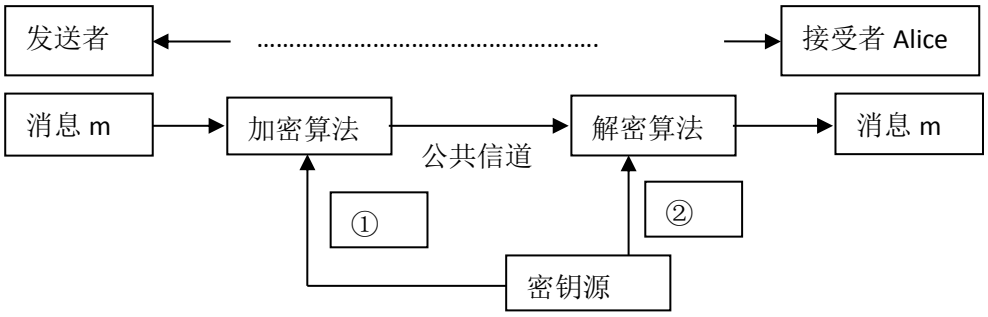


图 5 保密通信示意图

（1）完成题目中的填空；

①_____；　②_____；

（2）假设发送的消息 m=4，求接收者 Alice 接收到密文 c。（给出详细求解过程）

5、此题是对 SHA-1 算法考查，包含了 2 个小题。

采用 SHA-1 算法，完成消息的填充，填充之后数据格式如图 6 所示，包含三部分：原始消息，填充消息，数据长度。

原始消息	填充消息	数据长度

图 6　SHA-1 填充之后消息格式

（1）假设输入消息为 ASCII 码字符“abcd0123”，给出第二部分填充消息的比特位长度和第三部分数据长度的比特位长度。

（2）消息填充之后，输出第 0 组 W[0]，第 1 组 W[1]，第 2 组 W[2]。（十六进制表示）

注：①其中字符'a'对应的 ASCII 序号为十进制的 97，字符'0'对应的 ASCII 序号为十进制的 48。

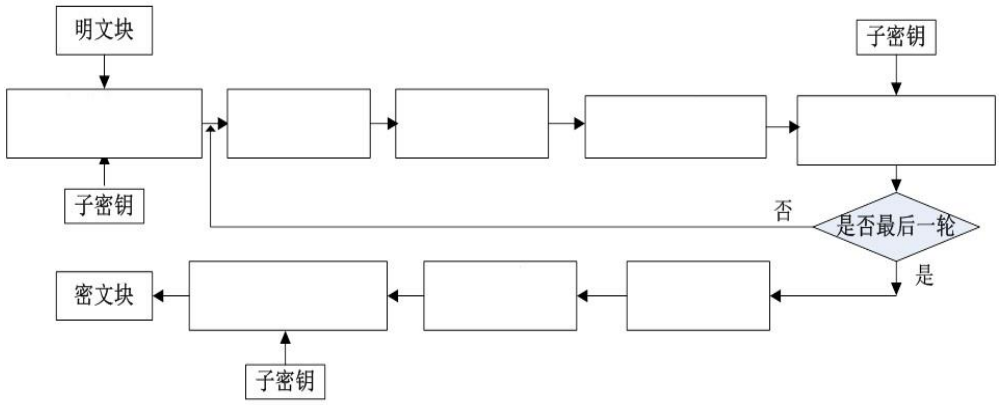
6. 记 Z_{26}={0,1,2,3,…,25}分别表示 26 个字母，即 a 对应 0，b 对应 1，……。选择整数 k 和 $b \in Z_{26}$ 组成密钥(k, b)，其中 gcd(k，26)=1。加密算法为：$y \equiv kx + b \pmod{26}$，其中 $x \in Z_{26}$ 为明文。

（1）写出解密算法。

（2）取 k=17，b=11，若明文 x 为字母 c，求加密后的密文。

7. 在 AES 算法加密过程中有 4 个步骤，分别是字节替代、行移位、列混合、轮密钥加。

（1）把这 4 个步骤填入下图中，完成加密过程。



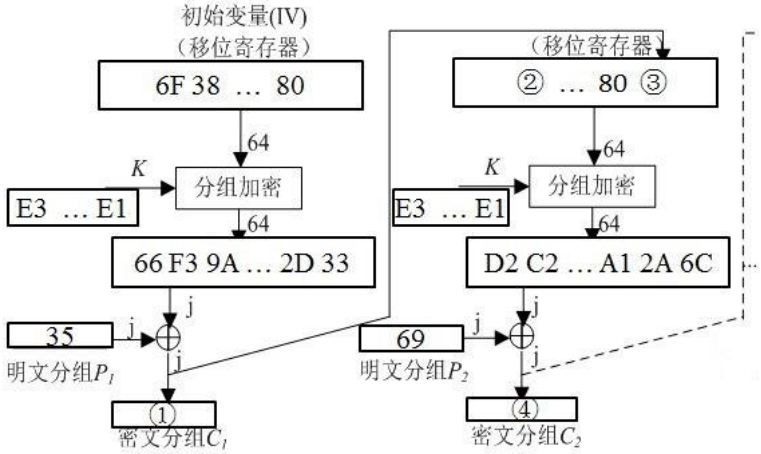
（2）加密一组明文时，若密钥长度为 128bits，则要执行 10 轮加密。那么执行字节替代、行移位、列混合、轮密钥加各多少次？

8. 下图是某分组密码算法的 CFB 模式加密过程，图中所有数据为 16 进制。假设消息的长度超过 100 个分组，反馈长度为 j=8bits。

（1）完成题目中的填空。

①_____；　②_____；③_____；④_____。

（2）画出对应的解密过程。



9. 已知 DES 的 E 盒如表所示，E 盒的输入为 16 进制的{EA09782C}，求经过 E 盒扩展后的输出。要求画出表格，写出转换的完成过程。

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

10. 已知 Diffie-Hellman 密钥交换算法的安全性是基于 Z_p^*上的离散对数问题。设 p 是一个素数，并且 $g(1<g<p)$是循环群 Z_p^*的生成元，g 和 p 公开。两个用户 A 与 B 通信时，通过分别选取随机数 r_A 和 r_B，通过执行 Diffie-Hellman 密钥交换算法协商通信所使用的密钥。

若 p=41, g=6，A 和 B 分别选 r_A=11，r_B=27，计算他们的共享密钥。

11、下题是对 DES 算法的考核，包含了 2 个小题。

（1）图 2 给出了 DES 算法的轮结构，请问轮结构 F 变换中，哪些变换的输出是 32bits，哪些变换的输出是 48bits？（4 分）

提示：有箭头指向的位置表示有输出，F 变换中有 4 个表示输出的箭头。

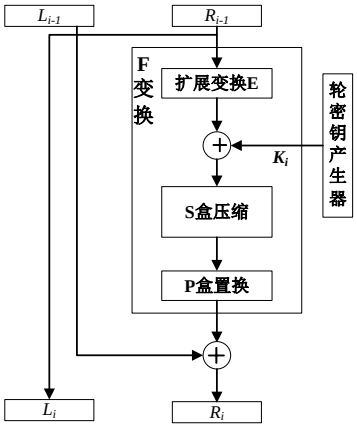


图 2　DES 算法轮结构

（2）图 3 是 S 盒中的 S1，如果输入为 101010，则输出应为_____。

S_i		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	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 3　DES 算法 S 盒

12、下题是对 AES 算法的考核，包含了 2 个小题。

（1）图 4 给出了 AES 的算法的解密过程，请在空白处补充完整 AES 的算法解密过程？

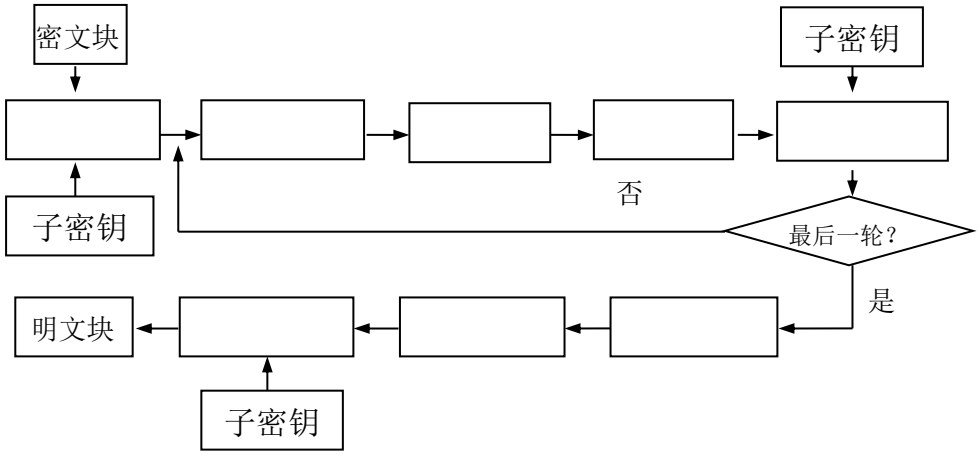


图 4 AES 算法解密结构

（2）AES 算法有三种密钥长度 128bits、192bits、256bits，请问加密 1 组明

文时，对于三种不同长度密钥，分别需要扩展多少 bit 的密钥？

13、下题是对分组密码工作模式的考查，包含了 2 个小题。

（1）图 5 以 DES 算法为例，给出了使用 OFB 工作模式时进行加密时的示意图，画出对应的解密示意图。

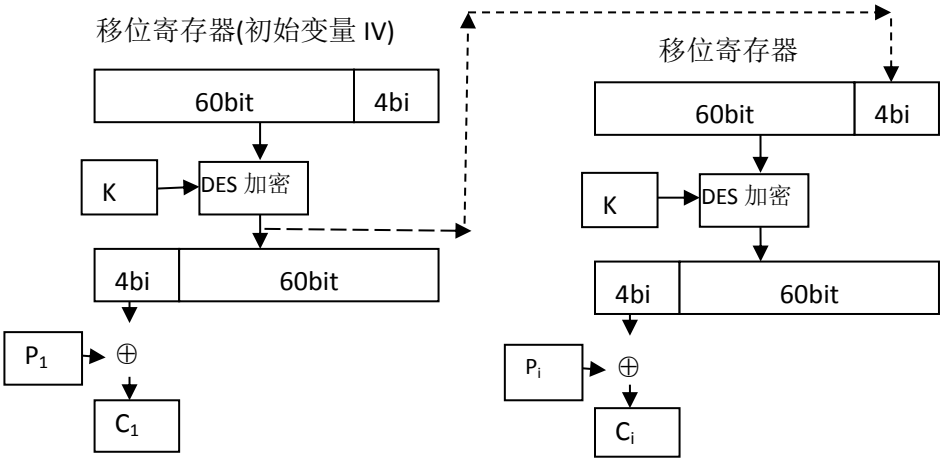


图 5 OFB 工作模式加密图

（2）OFB 工作模式中， DES 算法实际起到的是密钥流生成器的作用，问此密钥流生成器属于同步密钥流生成器还是自同步密钥生成器？该密钥流生成器有什么特性

14、设 4 级线性移位寄存器的反馈函数为 $f(a_1,a_2,a_3,a_4)=a_1\oplus a_2\oplus a_4$，完成下面题目（共 6 分）

（1）写出该 LFSR 的反馈函数的特征多项式，并求其周期

（2）画出 LFSR 反馈状态图

15、下题是对消息认证的考查，包含了 2 个小题。

（1）图 5 给出了基于明文的消息认证过程，请在空白 1-4 处补充完整消息认证过程？

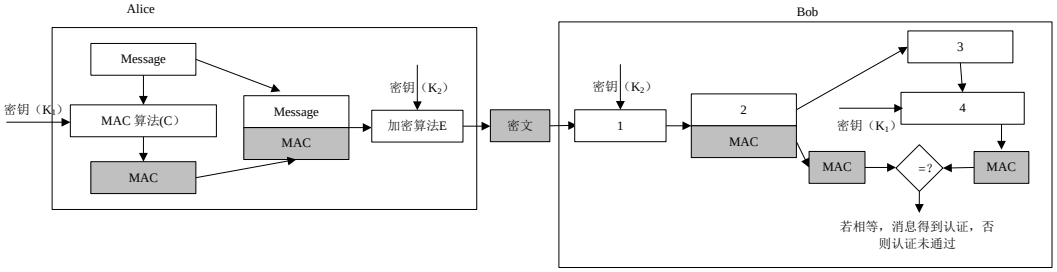


图 5 消息认证

1、_____ 2、_____

3、_____ 4、_____

（2）图 5 消息认证过程，能达到哪几个信息安全目标？

16 在 DES 加密算法中，第一步是初始置换，也称 IP 置换，该置换表如表所示。如果明文输入为字符的“itis2015”，求经过 IP 置换后的右边 32 个比特的值，以行优先的方式填入右边表格中，并写出对应的 16 进制表示。其中字符"i"的 ASCII 码为 105，字符"s"的 ASCII 码为 115，字符"0"的 ASCII 码为 48. 提示:先把每个字符的 ASCII 码转换为 8 位二进制, 然后再按置换表进行置换.

IP 置换表

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP 置换后的右边 32 个比特

输出的 16 进制为：_____

17、下面是对消息摘要算法 SHA-1 的考察，共 2 小题

（1）若消息的长度为 199 字节. 按照 SHA-1 算法，每次处理 512 比特长度的消息，则该消息应该分成几组，为什么？需要填充多少字节

（2）若消息的长度为 252 字节，按照 SHA-1 算法的规定，需要对消息进行分组和填充. 则为计算该消息的摘要值，需要运行多少次 SHA-1 压缩函数，为什么？

提示：（1）填充的消息长度是整个消息的长度；（2）注意比特和字节的换算关系。

18、下题是对 AES 算法的考核，包含了 2 个小题。

在 AES 算法中，已知构造有限域时使用的不可约多项式为 $x^8+x^4+x^3+x+1$，xtime 特指用位运算实现多项式 x 乘以一个普通的多项式 $b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x^1+b_0x^0$，因此有限域 $GF(2^8)$中，例如 16 进制“02”等价于多项式“x”，例如“05”等价于多项式“x^2+1”，使用有限域 $GF(2^8)$上的字节运算方法计算：

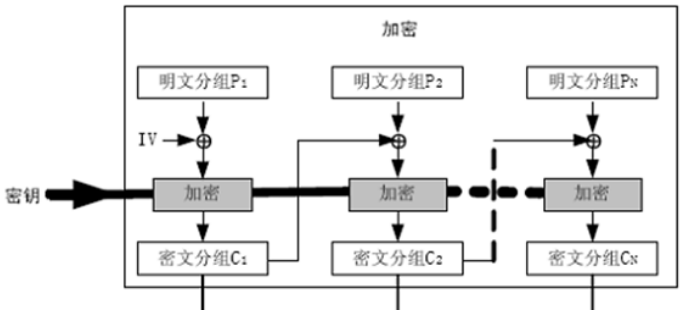
（1）16 进制的“F0”与“E9”的加法，即计算“F0+E9”的值；

（2）16 进制的“03”与“80”的乘法，即计算“03•80”的值。

提示：相应值可以等价于 GF(2)多项式相乘，然后相乘结果再模构造有限域时使用的不可约多项式。

19、下题是对分组密码工作模式的考查，包含了 3 个小题。

分组密码运行模式中的分组密码链接模式（CBC）对消息进行加密的示意图如图所示，其中 IV 表示初始向量，消息被分为 N 组进行加密。



（1）设消息的长度为 2200 字节，选用的密码算法为 AES，则需要把消息分成多少个分组进行加密？

（2）若加密消息 $P_i(1\le i\le N)$，得到密文 $C_i(1\le i\le N)$。若加密者对消息 $P_k(1\le k<N)$进行了修改，则加密得到的密文会有什么变化？

（3）画出 CBC 模式的解密示意图.

20、下题是对线性反馈函数考核，包含了 2 个小题（共 6 分）

已知序列密码算法采用 3 级线性反馈移位寄存器产生的密钥序列进行加解密，攻击者能够截获一明文串为 $M=m_0m_1m_2m_3m_4m_5=101000$，对应的密文串为 $C=c_0c_1c_2c_3c_4c_5=000110$。

（1）求该明文串对应的密钥流 $K=k_0k_1k_2k_3k_4k_5$

（2）给出 3 级 LFSR 的反馈函数

提示：3 级反馈函数可表示为：$f(a_1\ a_2\ a_3)=c_1a_3\oplus c_2a_2\oplus c_3a_1$，而密钥流 K 则是反馈函数输出序列

五、综合计算题，总共 2 道题，请写出具体运算过程。

1、已知 Diffie-Hellman 密钥交换算法的安全性是基于 Z_p 上的离散对数问题。设 p 是一个满足要求的大素数，并且 $0<a<p$ 是循环群 Z_p 的生成元，a 和 p 公开，所有用户都可以得到 a 和 p。在两个用户 A 与 B 通信时，它们可以通过如下步骤协商通信所使用的密钥：

（1）用户 A 选取一个大的随机数 r_A（$1\le r_A\le p-2$） (1)，计算：$s_A=a^{r_A}(\mathrm{mod}\,p)$，并且把 s_A 发送给用户 B。

（2）用户 B 选取一个随机数 r_B $(1\le r_B\le p-2)$，计算 $s_B=a^{r_B}(\mathrm{mod}\,p)$。并且

把S_B发送给用户 A。

（3）用户 A 计算$K = S_B^{r_A} (\mathrm{mod}\ p)$，用户 B 计算$K' = S_A^{r_B} (\mathrm{mod}\ p)$。

若已知 p=47， a=5，r_A=11，r_B=7 ，根据上面协议回答下面问题：

（1）求 S_A，S_B，K， K'的值

（2）在实际应用中，参数 p 和 a 的值都是很大的，比如 p 的取值接近 2^{1024}. 在保证计算安全的情况下为参数 p 和 a 选取合适的值，则参数 a，p，S_A，S_B 为什么可以在不安全信道上传输？

（3）对于 Diffie-Hellman 密钥交换协议，容易遭受中间人攻击，实现一个完整的中间人攻击过程如图 7。若用户 A 和用户 B 采用 Diffie-Hellman 密钥交换协议，经过攻击者 C 的中间人攻击之后，给出用户 A 和用户 B 计算密钥的值。

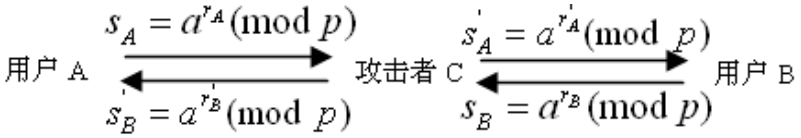


图 7　Diffie-Hellman 密钥交换协议中间人攻击

2、AES 算法的基本运算是在有限域$GF(2^8)$上的加与乘运算。AES 算法构造有限域$GF(2^8)$选择的不可约多项式是 $p(x) = x^8 + x^4 + x^3 + x + 1$。有限域$GF(2^8)$上的域元素，可用十六进制，二进制，以及多项式不同等价表示。例如域元素{57}（十六进制数），对应的二进制为 01010111，对应的多项式为$x^6 + x^4 + x^2 + x + 1$。

（1） 若两域元素分别为{83}和{05}（十六进制），则给出各域元素对应的多项式

（2） 求两域元素的和：{83}+{05}

（3） 求两域元素的积：{83}•{05}

3. 在非对称密码算法 RSA 密钥产生过程中，设 p=13，q=17，取公钥参数 e＝25，完成（1）-（4）题。

（1） 求私钥参数 d；

（2） 如果消息 m=6，求对应的密文。

（3）由上面结果，列出消息发送者和密码分析者各自可以直接获得的参数及对应的值。

（4） 简述 RSA 密码算法能否抵御选择明文攻击？

4. 设输入消息为 ASCII 码字符“a1b2c3d4e5”，按照 SHA-1 算法的填充和扩展规则，完成消息的填充和扩展。（1）输出第 0 组 W[0]，第 1 组 W[1]，第 2 组 W[2]，第 15 组 W[15]，用 16 进制表示。（8 分）（2）输出第 16 组 W[16]，用 16 进制表示。

提示：（1）其中字符’a’对应的 ASCII 序号为十进制的 97，字符’0’对应的 ASCII

序号为十进制的 48；

（2）$W[16]=ROTL^1(W[13]\oplus W[8]\oplus W[2]\oplus W[0])$，$ROTL^t$表示循环左移 t bits。

5、有两用户 A 和 B，已知 A 用户的 RSA 算法的私钥参数 $d_A=7$，$n_A=65$；B 用户的 RSA 公钥参数 $e_B=11$，$n_B=65$。若需要 A 用户发送消息 m=2 给用户 B，A 用户采用 RSA 密码算法对消息 m 进行加密，得到密文 C；并对消息 m 进行签名，得到签名 $sig=m^{d_A}(\mathrm{mod}\, n_A)$，然后把密文消息 C 和签名消息 *sig* 一起发送给 B。

（1）计算 A 用户的公钥中 e_A 的值和 B 用户的私钥中 d_B 的值；

（2）计算 A 用户发送给 B 用户的密文 C 和签名 *sig* 的值；

（3）若在实际应用中，用户 A 和用户 B 都使用题目给出的 RSA 公钥和私钥，是否安全？为什么？

6、Diffie-Hellman 密钥交换算法可以描述为：

① 为算法选择两个全局公开的参数，素数p和p的一个原根g.

② 假设用户 Alice 和 Bob 希望共享一个密钥。用户 Alice 选择一个随机数$x_\mathrm{A}(x_\mathrm{A}<p)$，并计算$y_\mathrm{A}=g^{x_\mathrm{A}}(\mathrm{mod}\, p)$；类似地，用户 Bob 选择一个随机数$x_\mathrm{B}(x_\mathrm{B}<p)$，并计算$y_\mathrm{B}=g^{x_\mathrm{B}}(\mathrm{mod}\, p)$。

③ Alice 通过公共信道把y_A发送给 Bob，Bob 也通过公共信道把y_B发送给 Alice.

④ Alice 获得共享秘密密钥的计算方式是$K_\mathrm{A}\equiv {y_\mathrm{B}}^{x_\mathrm{A}}(\mathrm{mod}\, p)$. Bob 获得共享秘密密钥的计算方式是$K_\mathrm{B}\equiv {y_\mathrm{A}}^{x_\mathrm{B}}(\mathrm{mod}\, p)$.

⑤ 密钥交换完成.

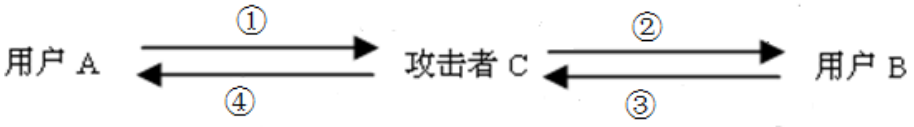
若已知$p=97,\ g=5,\ x_\mathrm{A}$ =13, x_B =6 根据上面协议回答问题：

（1）证明$K_\mathrm{A}\equiv K_\mathrm{B}$.

（2）求y_A，y_B，K_A.

（3）在实际应用中，参数p, g的值都是很大的，比如p的取值接近 2^{1024}. 在保证计算安全的情况下为参数p, g选取合适的值，则在p, g, x_A, x_B, y_A, y_B, K_A, K_B等参数对应的数值中，分析者可以直接获得的有哪些？

（4）上面所述的 Diffie-Hellman 密钥交换协议有可能被中间人攻击。实现攻击的过程如下所示。已知①为：$y_\mathrm{A}=g^{x_\mathrm{A}}(\mathrm{mod}\, p)$，③为$y_\mathrm{B}=g^{x_\mathrm{B}}(\mathrm{mod}\, p)$。补充第②和④步，实现一个完整的中间人攻击过程。


用户 A
①
④
攻击者 C
②
③
用户 B

部分习题集答案

第四题　综合问答题

1、维吉尼亚密码体制的考查

（1）解密函数 D_k 和加密函数 E_k 一样，假设密文 $c=(c_1, c_2, \ldots, c_n)$，则解密函数为：

$D_k(c_1, c_2, \ldots, c_n)=((c_1-k_1) \bmod 26，(c_2-k_2) \bmod 26，\ldots，(c_n-k_n) \bmod 26$

$= m_1, m_2, \ldots, m_n$

（2）明文字符 b 对应 1，y 对应 24，e 对应 4

加密过程为：$c_1=1+5 \bmod 26 =6$　$c_2=24+2 \bmod 26=0$　$c_3=4+1 \bmod 26=5$。

2、此题是对 DES 算法的考核，共 2 题。（共 6 分）

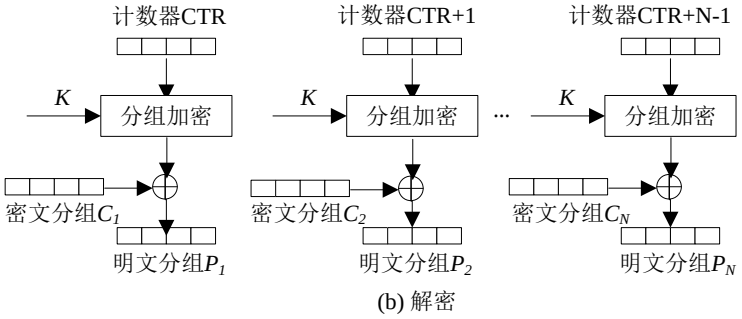
（1）完成题目中的填空；

①　E 盒扩展　；　②　S 盒压缩　；③　P 盒替代　。

（2）下图 3 是 S 盒中的 S_1，如果输入为（111011），则输出应为___0 ___

3、此题是对分组密码的工作模式考查，共 2 题。

（1）CTR 解密运行过程如下：



(b) 解密

CTR 运行模式解密过程示意图

（2）会影响 3 组的密文分组无法正常解密

4、此题是对 RSA 算法考查，共 2 题。

（1）完成题目中的填空；

①_____{e=7，n=143}____；　②_____{d=103，n=143}_____；

（2）假设发送的消息 m=4，求 Alice 接收得密文 c。（给出详细求解过程）

解：密文： $c=m^e \bmod n$ （1 分） $c=4^7 \bmod 143$

$c=(2^8)*(2^6) \bmod 143$

$c=82$

5、下题是对 SHA-1 算法考查，包含了 2 个小题。

（1）给出第二部分填充消息的比特位长度？第三部分数据长度的比特位长度？

解：填充公式： $l+1+k \equiv 448 (\bmod 512)$

l=8*8=64， 448-64=384，因此第二部分填充消息的比特位长度为 384 。

第三部分数据长度的比特位长度为 64

（2）消息填充之后，输出第 0 组 W[0]，第 1 组 W[1]，第 2 组 W[2]。（十六进制表示）

解：其中 a 的十六进制为 61，b 为 62 c 为 63 d 为 64 0 为 30 1 为 31 2 为 32 3 为 33

因此 W[0]=61626364 w[1]= 30313233 w[2]=80000000

6. 仿射密码算法

解密公式为：$x= k^{-1}(y-b) \bmod 26$

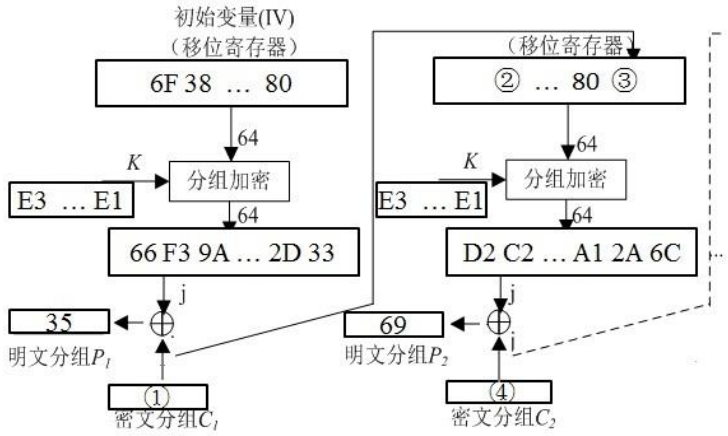
明文字符 c 对应 2，加密过程为：$y=17\times2+11 \bmod 26=19$。

7. 按箭头顺序依次为：轮密钥加、字节替代、行移位、列混合、轮密钥加、字节替代、行移位、轮密钥加。

字节替代、行移位各执行 10 次，轮密钥加 11 次，列混合 9 次。

8. CFB

①35H⊕66H=53H ②38H ③53H ④BBH



9. E 扩展，E 盒的输入为 16 进制的{EA09782C}

0	1	1	1	0	**1**
0	1	0	1	0	**0**
0	0	0	0	0	**1**
0	1	0	0	1	**0**
1	0	1	1	1	**1**
1	1	0	0	0	**0**
0	0	0	1	0	**1**
0	1	1	0	0	1

10. Diffie-Hellman 密钥交换算法 参考答案：

$K=6^{11\times27} \bmod 41=6^{297} \bmod 41$

由欧拉定理，$6^{40} \bmod 41\equiv1$

故 $6^{297} \bmod 41\equiv6^{17} \bmod 41$

$6^2 \bmod 41\equiv36\equiv-5$　$6^4 \bmod 41\equiv25$　$6^8 \bmod 41\equiv10$　$6^{16} \bmod 41\equiv18$

故 $6^{17} \bmod 41\equiv18\times6\equiv26$

11、DES 的考核

解：（1）S 盒压缩和 P 盒置换的输出是 32bits，E 盒扩展和 E 盒与轮密钥异或的输出是 48bits

（2）6（或者 0110））

12、 AES 算法考核

解： （1）

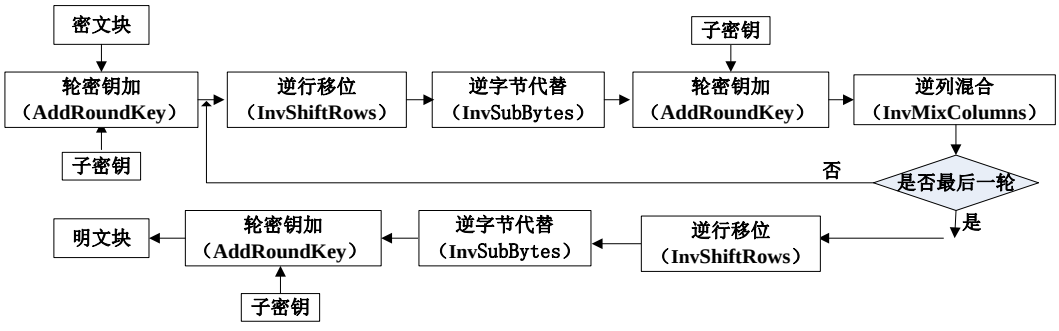


图 1　AES 解密过程

（2）128bits 需要扩展密钥长度是 11*128-128=1280bits

192bits 需要扩展密钥长度是 13*128-192=1472bits

256bits 需要扩展密钥长度是 15*128-256=1664bits

13、OFB 工作模式考核（共 8 分）

解：（1）

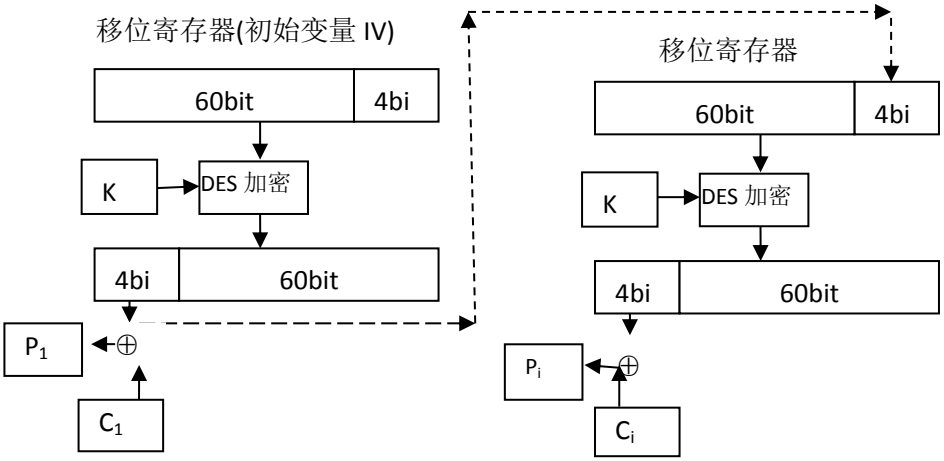


图 2 OFB 工作模式解密图

（2）OFB 工作模式下，DES 密钥流生成器是属于同步流密码，密（明）文符号是独立的，明文和密文一个错误传输只会影响一个符号，不影响后面的符号。

14、序列密码考核（共 6 分）

解： （1） 4 级线性移位寄存器的反馈函数为 $f(a_1,a_2,a_3,a_4)=a_1\oplus a_2\oplus a_4$，

因此对应特征多项式为 $f(x)=x^4+x^3+x+1$

特征多项式不是本原多项式，不是 m 序列

因为 $x^6-1=(x^2-x-1)(x^4+x^3+x+1)$，即 $x^4+x^3+x+1 \mid x^6-1$

最小整数为 6，即周期为 6

（2）画出 LFSR 反馈状态图

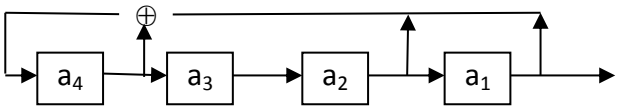


图 3 4 级线性反馈移位寄存器状态图

15、消息认证知识点考核 （共 6 分）

解：（1） 解密算法 D、Message、Message、Mac 算法（C）

（2）这消息认证模式能达到信息安全目标中完整性、保密性

16、DES 的考核

解：“itis2015”转换为 ASCII 值分别为

i 105 01101001 t 116 01110100 i 105 01101001 s 115 01110011

2 50 00110010 0 48 00110000 1 49 00110001 5 53 00110101

经过 IP 初始置换之后的值

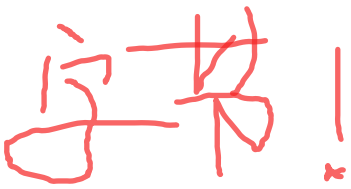
01101001
01110100
01101001
01110011
00110010
00110000
00110001
00110101

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP 置换的输出的后 4 行分别为输入的 第 1 列，第 3 列，第 5 列， 第 7 列，每列次序颠倒，因此后 4 行分别为：

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
0	0	0	0	0	1	0	1
0	0	0	1	1	0	0	0

十六进制为：0x00FF0518



17、SHA-1 函数考核 （共 6 分）

解：（1）一个分组 512 比特，则 512/8=64 字节，199/64≈3，因此总共分组 4 个分组

最后一分组的消息长度 199 mod 64= 7，另外有 64bits，即 8 字节作为数据长度，因此填充消息长度为 64-7-8=49 字节

（2）若消息的长度为 252 字节，按照 SHA-1 算法的规定，需要对消息进行分组和填充. 252/64≈3, 252 mod 64=60，因此总共 5 个 512bits 块，一个 512bits 分组总共 80 个轮次，5 个 512bits 则需要运行 400 次 SHA-1 压缩函数

18、 AES 算法考核

解： （1）有限域加法运算为异或运算

因此 *F0+E9=0x19*

（2）*16* 进制的*“03”*与*“80”*的乘法，即计算*“03•80”*的值。

“03” 等价于多项式是“x+1”，*“80”*等价于“x^7”

（x+1）x^7=x^8+x^7（mod x^8+x^4+x^3+x+1）

≡（x^8+x^4+x^3+x+1）+ x^7+x^4+x^3+x+1

≡x^7+x^4+ x^3+x+1

“03•80”=10011011=0x9b

备注：此题也采用其它计算方法

19、OFB 工作模式考核

解：（1）AES 明文长度 128bits,即 16 字节，因此分组长度为：

2200/16=137.5

即 2200 分组有 138 个明文分组

（2）若加密消息$P_i(1 \le i \le N)$，得到密文$C_i(1 \le i \le N)$。若加密者对消息P_k $(1 \le k < N)$进行了修改，则加密得到的密文 C_k 会发生变化，由于密文 C_k 反馈，所以 C_k 之后所有密文都会发生变化

（3）评分标准: 错一个扣 1 分,扣完为止（共 4 分）

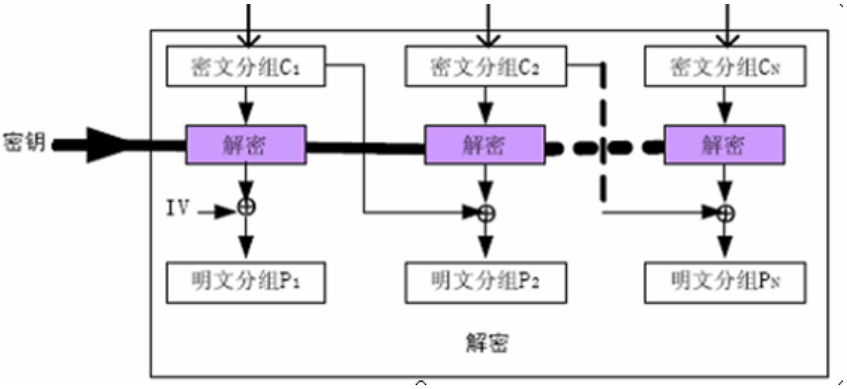


图 1 CBC 解密过程

20、序列密码考核

解： （1）

明文串对应的密钥流 $K = M \oplus C = 101000 \oplus 000110 = 101110$

（2）LFSR 反馈函数

3 级反馈函数表示为：$f(a_1\ a_2\ a_3) = c_1a_3 \oplus c_2a_2 \oplus c_3a_1$，根据已知密钥流可以得到下面三个方程

$$1 = c_1 \oplus c_3 \quad 1 = c_1 \oplus c_2 \quad 1 = c_1 \oplus c_2 \oplus c$$

因此得到 $c_1 = 0, c_2 = 1, c_3 = 1$，因此 $f(a_1\ a_2\ a_3) = a_2 \oplus a_1$

五、综合题

1、 Diffie-Hellman 密钥交换协议的考查 （18 分）

（1）求s_A，s_B，K 和K'的值

解：分别计算：$s_A = a^{r_A} = 5^{11} mod\ 47 = 13$;

$s_B = 5^7 mod\ 47 = 11$;

在交换s_A，s_B后，

分别计算：$K = s_B{}^{r_A} mod\ 47 = 11^{11} mod\ 47 = 39$

$K' = s_A{}^{r_B} mod\ 47 = 13^{7} mod\ 47 = 39$

（2）解：基于离散对数困难问题，给定参数p，a，求s_A容易，反之，给定p和s_A，求a是困难的。参数s_B同理。

（3）通过中间人攻击，用户 A 计算共享密钥值为： $K = s'_B{}^{r_A} mod\ p$ 。用户 B 计算的共享密钥为：$K' = s'_A{}^{r_B} mod\ p$

2、AES 基本运算考查（12 分）

（4） 若用十六进制表示两域元素分别为{83}和{05}，则给出各域元素对应的多项式

解：83 对应的二进制为 10000011，对应的多项式为 x^7+x+1。

05 对应的二进制为 00000101， 对应的多项式为 x^2+1。

（5） 求两域元素的和：{83}+{05}

解：{83}+{05}=10000011⊕00000101=10000110={86}

（6） 求两域元素的积：{83}•{05}

解：

{83}•{05}={83}•{{04}⊕{01}} （1分）

{83}•{02}={10000011}•{02}={00000110}+{00011011}

={00011101}={1D} （2分）

{83}•{04}={1D}•{02}={00011101}•{02}={00111010}={3A} （2分）

{3A}+{83}={00111010}⊕{10000011}={10111001}={B9} （1分）

备注：也可以采用多项式直接求解

3. 在非对称密码算法 RSA 密钥产生过程中，设 p=13，q=17，取公钥参数 e＝25，完成（1）-（4）题。

（1） 求私钥参数 d；

φ(n)=12×16=192

192=25×7+17　　25=17+8　　17=8×2+1

1=17-8×2=17-(25-17)×2=17×3-25×2

=(192-25×7) ×3-25×2=192×3-25×23

等式两端模 192 得　　d≡-23≡169(mod 192)

（2） 如果消息 m=6，求对应的密文。

6^2≡36(mod221)　　6^4≡-30　　6^8≡16

6^{16}≡256≡35

6^{25}≡6×6^8×6^{16}≡35×16×6≡45.

（3）由上面结果，列出消息发送者和密码分析者各自可以直接获得的参数及对应的值。

消息发送者可以直接获得的参数及对应的值为：m=6, e=25, n=221, c=45

密码分析者可以直接获得的参数及对应的值为：e=25, n=221, c=45

（4） 简述 RSA 密码算法能否抵御选择明文攻击？

能

4. SHA

（1）W[0]=61316232H　　W[1]= 63336434H

W[2]=65358000H　W[15]= 00000050H

（2）$W[16] = ROTL^1(W[13] \oplus W[8] \oplus W[2] \oplus W[0])$

$=ROTL^1(61316232 \oplus 65358000)$

$=ROTL^1(404E232)= 809C464$

5 解: （1）请分别计算出 A 用户和 B 用户的私钥值 d 的值；

已知 公钥 n_A=65,首先分解 n_A=5*13 得到 p=5，q=13

计算欧拉函数 $\Phi(n_A)$=（p-1）（q-1）=48

A 用户私钥计算：已知 A 用户私钥 d_A=7， gcd（$\Phi(n_A)$，e_A）=1，根据 RSA 密钥生成过程 $e_Ad_A \equiv 1 \bmod \Phi(n_A)$ 即 $7d_A \equiv 1 \bmod 48$

欧几里得扩展算法：48=6*7+6　7=6*1+1

1=7-6=7-(48-6*7)=7*7-48

可得 $7*7 \equiv 1 \bmod 48$ 即 d=7

同理 B 用户私钥：e_B=11，　$11d_B \equiv 1 \bmod 48$

48=4*11+4　11=2*4+3　4=1*3+1

1=4-(11-2*4)=3*4-11=3*(48-4*11)-11=3*48-13*11

d_B=48-13=35

（2）A 用户发送密文 C 和签名 Sig 给 B 用户

根据 RSA 加密算法规则，A 需要发送消息给 B，则需要用 B 的公钥加密

B 的公钥 e_B=11，因此密文 $C \equiv 2^{11} \bmod 65$

$C \equiv (2^{10})*2 \bmod 65 \equiv 49*2 \bmod 65 \equiv 33$

A 需要发送签名 Sig 给 B，则需要 A 的私钥签名，

A 的私钥 d_A=7， $Sig \equiv 2^7 \bmod 65 \equiv 63$

（3）

不安全

p 和 q 值太小，要求大素数 p 和 q,一般 1024bits 和 2048bits；

6、DH 算法（共 20 分）

解：（1）证明$K_A \equiv K_B$.

证明：

Q $y_A = g^{x_A} (\mathrm{mod}\ p), y_B = g^{x_B} (\mathrm{mod}\ p)$

$\therefore K_A \equiv y_B{}^{x_A} \equiv (g^{x_B})^{x_A} \equiv g^{x_B x_A} (\mathrm{mod}\ p)$

$\therefore K_B \equiv y_A{}^{x_B} \equiv (g^{x_A})^{x_B} \equiv g^{x_A x_B} (\mathrm{mod}\ p)$

$\therefore K_A \equiv K_B (\mathrm{mod}\ p)$

（2）求y_A，y_B，K_A.

Q $y_A \equiv g^{x_A} (\mathrm{mod}\ p) \equiv 5^{13} (\mathrm{mod}\, 97)$

$\equiv (5^3)^4 \cdot 5 (\mathrm{mod}\, 97) \equiv 28^4 \cdot 5 (\mathrm{mod}\, 97)$

$\equiv 8^2 \cdot 5 (\mathrm{mod}\, 97) \equiv 29 (\mathrm{mod}\, 97)$

$y_B = g^{x_B} (\mathrm{mod}\ p) \equiv 5^6 (\mathrm{mod}\, 97) \equiv 8$

$K_A \equiv y_A{}^{x_B} \equiv 29^6 (\mathrm{mod}\, 97) \equiv 65^3 (\mathrm{mod}\, 97)$

$\equiv 54 * 65 (\mathrm{mod}\, 97) \equiv 18 (\mathrm{mod}\, 97)$

（3） 在实际应用中，分析者可用直接获取p，g，y_A，y_B

（4）上面所述的 Diffie-Hellman 密钥交换协议有可能被中间人攻击。

第②步是 $y_C \equiv g^z (\mathrm{mod}\ p)$，第④步是 $y_C \equiv g^z (\mathrm{mod}\ p)$