一 填空题

1. 密码学发展的四个阶段：手工操作密码、机器密码时代、传统密码、现代公钥密码
2. DES 的明文分组长度是 64bits，密钥长度是 56 或者是 64 比特，密文长度是 64 比特。
3. 数字签名方案是指由 M 明文空间、S 签名空间、K 密钥空间、Sig 签名算法、Ver 验证算法组成的五元组。
4. 信息安全的核心是密码学；密码学研究的主要问题是 信息或信息系统安全（与保密）的问题
5. 加密算法模式有四种分别是： ECB， CBC， CFB， OFB
6. AES 的密钥长度可以是 128、192、256 AES 圈变换的由四个不同的变换组成，它们分别是字节替代、行移位、列混合、圈密钥相加
7. DES 的圈函数中包括扩展变换、异或运算、S 盒代替（8 个 S 盒）、P 盒置换
8. 柯可霍夫原则指出密码系统的安全性不能取决于算法，而应取决于密钥。
9. 根据加密的内容不同，密钥可以分为：主密钥、会话密钥、密钥加密密钥
10. 对称密码体制可以分为流密码和分组密码
11. 哈希函数 MD5 和 SHA-1 的输出长度分别是 128 和 160 比特。
12. 密码学由密码编码学和密码分析学组成。
13. 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 字节代换/非线性代换，AES 加密算法的非线性运算部分是指 s 盒 。
14. DES 与 AES 有许多相同之处，也有一些不同之处，请指出两处不同： AES 密钥长度可变 DES 不可变 ， DES 面向比特运算 AES 面向字节运算 。
15. MD5 的主循环有（4 ）轮。
16. 分组加密算法（如 AES）与散列函数算法（如 SHA）的实现过称最大不同是（可逆）。
17. Hash 函数就是把任意长度的输入，通过散列算法，变换成固定长度的输出，该输出称为消息摘要。
18. Hash 函数的单向性是指 对任意给它的散列值 h 找到满足 H（x）=h 的 x 在计算上是不可行的 。
19. 公钥密码体制的思想是基于 陷门单向 函数，公钥用于该函数的 正向（加密）计算，私钥用于该函数的 反向（解密）计算。
20. 1976 年，W.Diffie 和 M.Hellman 在 密码学新方向 一文中提出了公钥密码的思想，从而开创了线代密码学的新领域。
21. 公钥密码体制的出现，解决了对称密码体制很难解决的一些问题，主要体现一下三个方面： 密钥分发问题 、 密钥管理问题 和 数字签名问题 。
22. RSA 的数论基础是 数论的欧拉定理 ，在现有的计算能力条件下，RSA 被认为是安全的最小密钥长度是 1024 位 。
23. 公钥密码算法一般是建立在对一个特定的数学难题求解上，那么 RSA 算法是基于 大整数因子分解困难性、ElGamal 算法是基于 有限域乘法群上离散对数 的困难性。
24. 为保证安全性，在设计分组密码时，密码变换必须足够复杂，尽量使用 混淆 与 扩散 原则。这样使攻击者除了用 穷举 攻击以外，找不到其他简洁的数学破译方法

二 计算题

请给出 Caesar 密码的加解密规则；
将明文信息中的每个字母，用它在字母表中位置的右边的第 k 个位置上的字母代替，从而获得它相应的密文。
2）设 Caesar 密码中密钥为 KEY=7，假设明文为 ENCRYPTION，则相应的密文是什么？
设在 RSA 方案中，选取 p=5，q=11，公钥 e=7。
1） 计算公钥 e 对应的私钥 d；

2） 设有明文 m=10，求其密文 c，再对密文 c 解密。
请给出 Deffie-Hellman 密钥交换协议的一个实例，设 p=17，g=3

15. 设在有限域F_{23}上的椭圆曲线 E 为$y^2 = x^3 + 2x + 7$。

1）证明 P(5,2)是 E 上的点；
2）计算标量乘 2P，3P。

16. 设 E 是有限域F_{17}上椭圆曲线$y^2 = x^3 - x + 5$。

1）证明 P(7,1)，Q(8,4)是 E 上的点；
2）计算 P+Q 以及 2P、3P

1.请给出密码学的基本模型。

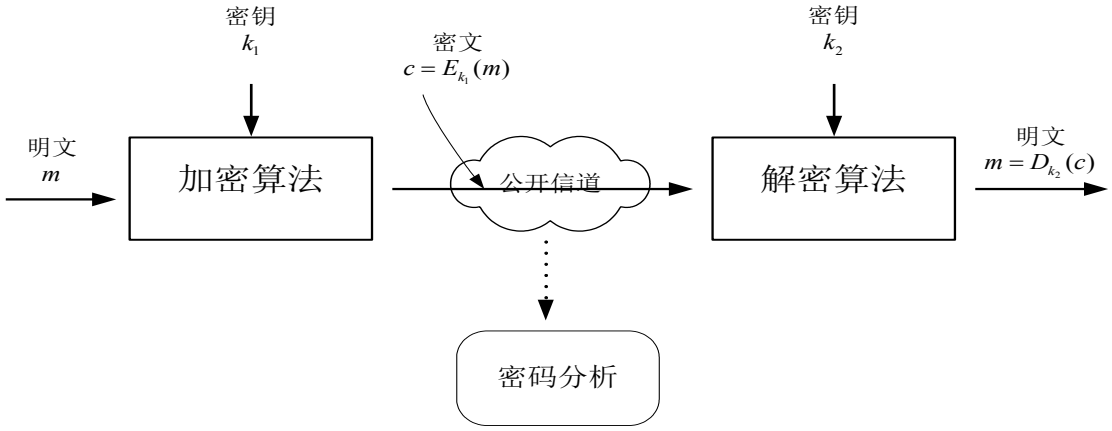


图 1-8 密码学基本模型

对称加密时：$k_1 = k_2$
公钥加密时：k_1不等于k_2

公钥密码体制的安全基础是某些复杂的含有陷门的数学难题。根据公钥密码体系的安全性基础来分类，现在被认为安全、实用、有效的公钥密码体系有三类。请说明这三类问题的具体含义。
(1)基于大数分解（大整数素因子分解）问题的公钥密码体制. 其中包括著名的 RSA 体制和 Rabin 体制.
(2)基于有限乘法群上离散对数问题的公钥密码体制. 其中主要包括 EIGamal 类加密体制和签名方案，Diffie-Hellman 密钥交换方案等.）
(3)基于椭圆曲线加法群上的离散对数问题的公钥密码体制.其中包括椭圆曲线型的 Diffie-Hellman 密钥交换方案，椭圆曲线型的 ECKEP 密钥交换方案; 椭圆曲线型的数字签名算法等

对 DES 和 AES 进行比较，说明两者的特点和优缺点。

DES：分组密码，Feist 结构，明文密文 64 位，有效密钥 56 位。有弱密钥，有互补对称性。适合硬件实现，软件实现麻烦。安全。算法是对合的。

AES：分组密码，SP 结构，明文密文 128 位，密钥长度可变≥128 位。无弱密钥，无互补对称性。适合软件和硬件实现。安全。算法不是对合的。

请简述数字签名的含义及其基本特征。

数字签名（digital signature) 是一种给电子形式存储的消息签名的方法。正因为如此，签名之后的消息能够通过计算机网络传输。数字签名是手写签名的数字化形式，与所签信息"绑定"在一起。具体地讲，数字签名就是一串二进制数。

它应具有下列基本特性：

1) 签名可信性：其他人可利用相关的公开消息验证签名的有效性；

2) 不可抵赖性：签名者事后不能否认自己的签名；

3) 不可复制性：即不可对某一数字内容或消息(message)的签名进行复制；数字签名文件本身可以复制，因此，签名文件本身应该包含诸如日期、时间在内的信息以防止签名被复制.

4) 不可伪造性：任何其他人不能伪造签名者的签名。或者说，任何其他人不能找到一个多项式时间的算法来产生签名者的签名；

请简述对称密码算法和公钥密码算法的区别。

主要体现在密钥形式，密钥管理和应用等三方面

1）对称密码体制中，通信双方共享一个秘密密钥，此密钥既能用于加密也能解密。公钥密码体制中每个用户有两个不同的密钥：一个是必须保密的解密密钥，另一个是可以公开的加密密钥。（3 分）

2）对称密码体制要求通信双方用的密钥应通过秘密信道私下约定，互联网上若有 n 个用户,则需要$\binom{n}{2} = \frac{n}{2}(n-1)$个密钥，也就需要$C_n^2$条安全信道，保存和管理如此庞大的密钥, 本身便不太安全.；另外，每个用户必须储存$n-1$个密钥，甚至对一个相当小的网络, 也可能变得相当昂贵；而且如果一个秘密密钥泄露了，则攻击者能够用此秘密密钥解密所有用此秘密密钥加密的消息 (至少两个用户被攻破)。公钥密码体制中公钥可以公开，每个用户只需保存自己的私钥。（3 分）

3）对称密码体制只能提供机密性服务，难以实现认证, 无法提供不可否认性服务。

公钥密码体制不仅可以用于加密，还可以协商密钥，数字签名，因此，公钥密码技术的主要价值：密钥分发；大范围应用中数据的保密性和完整性；实体鉴别；不可抵赖性。（3 分）

公钥密码体制的易实现认证，但加密速度虽然不如对称密码体制快, 尤其在加密数据量较大时. 因此，实际工程中常采用的解决办法是 将公钥密码体制和对称密码体制结合，即公钥密码体制用来分配密钥，对称密码体制用于加密消息。（1 分）

在公钥密码的密钥管理中，公开的加密钥和保密的解密钥的秘密性、真实性和完整性都需要确保吗？为什么

①公开的加密钥 Ke：秘密性不需确保，真实性和完整性都需要确保。因为公钥是公开的，所以不需要保密。但是如果其被篡改或出现错误，则不能正确进行加密操作。如果其被坏人置换，则基于公钥的各种安全性将受到破坏，坏人将可冒充别人而获得非法利益。

②保密的解密钥 Kd：秘密性、真实性和完整性都需要确保。因为解密钥是保密的，如果其秘密性不能确保，则数据的秘密性和真实性将不能确保。如果其真实性和完整性受到破坏，则数据的秘密性和真实性将不能确保。

③举例

（A）攻击者 C 用自己的公钥置换 PKDB 中 A 的公钥：

（B）设 B 要向 A 发送保密数据，则要用 A 的公钥加密，但此时已被换为 C 的公钥，因此实际上是用 C 的公钥加密。

（C）C 截获密文，用自己的解密钥解密获得数据。

数字签名的一般结构形式及其安全性要求。

答案提示：安全模型=攻击模型+攻击目的

攻击模型（攻击者的攻击能力，可获得的信息）：

- **惟密钥攻击(key-only attack)**: 攻击者只知道公钥，及验证算法 ver；
- **已知消息攻击（known message attack）**：攻击者拥有一系列以前由 Alice 签名的消息$(m_1, s_1),(m_2, s_2),...$
- **选择消息攻击（chosen message attack）**：攻击者请求 Alice 对一个消息列表（攻击者自己选取的列表）签名，得到这些消息的签名$s_i = sig_{k_{alice}}(m_i)$

攻击者可能的目的（方案的抵抗力）：

- **完全破译（total break）：**攻击者获得 Alice 的私钥，从而它能产生任何消息 Alice 的签名。
- **选择性伪造(selective forgery)：**攻击者能以不可忽略的概率对个人选择的消息产生一个有效地签名。对于给定的一则消息，他能以某种概率决定该消息的签名s。Alice 以前未对该消息签过名。

存在性伪造（existential forgery）：攻击者至少能够为一则消息产生有效签名。

1. 简述密码体制的原则:

(1) 密码体制既易于实现又便于使用，主要是指加密算法解密算法都可高效的实现 (2)密码体制的安全性依赖于密钥的安全性，密码算法是公开的；(3) 密码算法没有安全弱点，也就是说，密码分析者除了穷举搜索攻击外再也找不到更好的攻击方法；(4) 密钥空间要足够大，使得试图通过穷举搜索密钥的攻击方式在计算机上不可行。

2. 简述保密系统的攻击方法。

唯密文攻击，密码分析者除了拥有截获的密文外，没有其他可以利用的信息； 已知明文攻击，密码分析者不仅掌握了相当数量的密文，还有一些已知的明—密文对可供利用；

选择明文攻击，密码分析者不仅可以获得一定数量的明—密文对，还可以选择任何明文并在使用同一未知密钥的情况下能达到相应的密文；

选择密文攻击，密码分析者能选择不同的被加码的密文，并还可以得到对应的明文，密码分析者的主要任务是推出密钥及其他密文对应的明文；选择文本攻击，是选择明文攻击和选择密文攻击的组合

3. 安全散列函数需要哪些特性？

安全散列函数需要满足如下性质

H 可用于任意长度大小的数据块

H 可产生定长的输出

对任意给定的 x,计算 H(x)容易

对任意给定的 h，找到 x，满足 H(x)＝h 很难 （单向性）

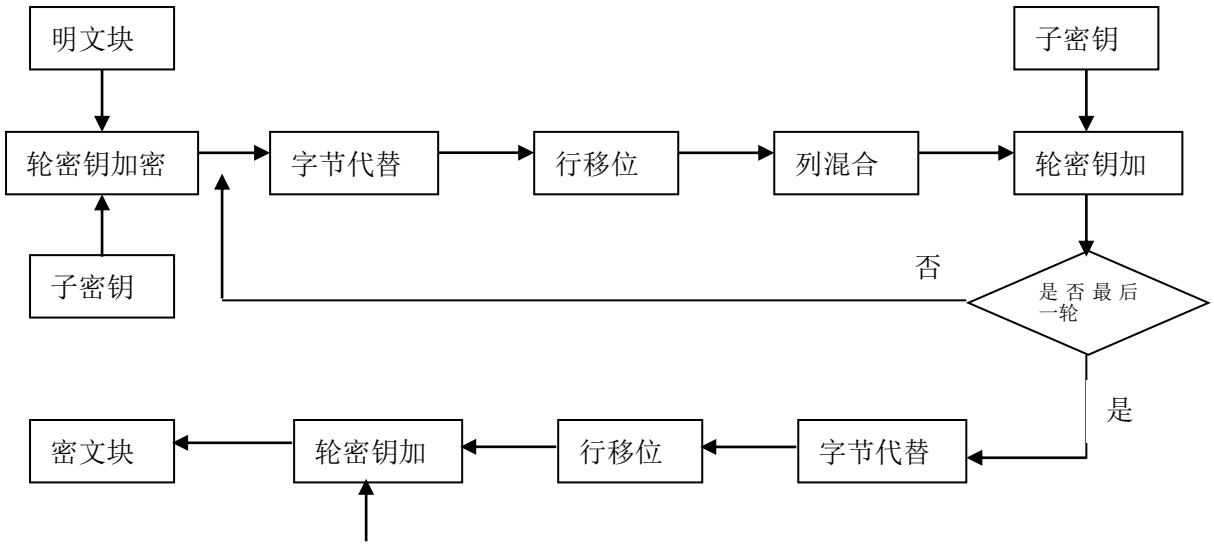
对任意给定的 x，找到 y，满足 H(x)＝H(y)很难（弱碰撞性）

找到任何满足 H(x)＝H(y)的分组对（x，y）很难（强碰撞性）

4. 简述 AES 算法加密过程，也可画图说明。

答：AES 算法的加密过程是在一个 4×4 的字节矩阵上动作，这个矩阵又称为“体”或者“状态”，其初值就是一个明文区块（矩阵中一个元素单位大小就是明文区块中的一个字节（8 比特））。加密时，明文块与子密钥首先进行一次轮密钥加，然后各轮 AES 加密循环（除最后一轮外）均包含 4 个步骤：

- 字节代替：通过一个非线性的替换函数，用查找表的方式把每个字节替换成对应的字节。
- 行移位：将矩阵中的每个横列进行循环式移位。
- 列混合：为了充分混合矩阵中各个起先的操作，这个步骤使用线性转换来混合每行内的四个字节。
- 轮密钥加密：矩阵中的每一个字节都与该次循环的子密钥做 XOR 逻辑运算；每个子密钥由密钥生成方案产生。



5. 密钥管理的原则：①区分密钥管理的策略和机制。②全程安全原则。③最小权利原则。④责任分离原则。⑤密钥分级原则。⑥密钥更新原则。⑦密钥应有足够的长度。⑧密码体制不同，密钥管理也不相同。

6. 密钥的产生方式：

①初级密钥可以在密钥加密密钥的控制下通过安全算法动态地产生。

②密钥加密密钥可以采用伪随机数生成器、安全算法或电子学噪声源产生。

③对于主密钥，虽然一般它的密钥量很小，但作为整个密码系统的核心，需要严格保证它的随机性，避免可预测性。因此，主密钥通常采用掷硬币、骰子或使用物理噪声发生器的方法来产生。