# 密码学复习资料

## 一、填空题

1.信息安全的核心是 密码学 ；密码学研究的主要问题是 信息与信息系统安全（与保密）的问题 。

2.密码学发展的四个阶段 古典密码术（手工操作密码）、机器密码时代、传统密码学、现代公钥密码学。

3.一个完整的密码体制或密码系统是指由明文空间（M）、密文空间(C)、密钥空间(K)、加密算法(E)、解密算法(D)组成的五元组。

4.解释密码学上的柯克霍夫原则:密码系统应该就算被所有人知道系统的运作步骤，仍然是安全的。(即使密码系统的任何细节已为人悉知，只要密匙（key，又称金钥或密钥）未泄漏，它也应是安全的。)

5.加密算法模式有四种，分别是： ECB ， CBC ， CFB ， OFB 。

6.DES的分组长度是 64 比特，密钥长度是64（56）比特，密文长度64比特。

7.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 、 圈密钥加 。

8.根据加密内容的不同，密钥可以分为 主密钥、密钥加密密钥、会话密钥。

9.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 。

10.对称密码体制可以分为 流密码 和 分组密码 两类。

密码学由 密码编码学 和 密码分析学 组成。

11.哈希函数MD5和SHA-1的输出长度分别是 128 和 160 比特。

12.密码体制的 4 种基本攻击类型 唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击。

13.密码体制从密钥使用策略上可以分为单钥密码体制与双钥密码体制。

14.数字签名方案具体可以分为三个步骤，即参数建立、签名生成、签名验证。

15.ANSI X9.17 标准将密钥分成三个层次：主密钥（KM）通过手工分配、密钥加密密钥（KK）通过在线分配、数据密钥（KD）。

16.一个密钥的生命周期主要经历了生成与存储、密钥分发、密钥启用与停用、密钥替换与更新、密钥销毁以及密钥撤销。

17.数字证书包含：版本（V3）、序列号、签名算法、发行者、有效期、主体名、主体公钥信息、发行者唯一标识符、主体唯一标识符、扩展项。

18.信息安全的目的：保障网络环境下信息的有效性。

19.RSA 公钥密码体制和 ECC 密码体制的安全性分别基于大整数素因子分解问题的困难性和椭圆曲线离散对数问题。

20.密码的四种链接模式。

21.何为公钥认证？

实际上是使用一对加密字符串，一个称为公钥(public key)，任何人都可以看到其内容，用于加密；另一个称为密钥(private key)，只有拥有者才能看到，用于解密。通过公钥加密过的密文使用密钥可以轻松解密，但根据公钥来猜测密钥却十分困难。

## 二、简答题

1. (1) 请给出Caesar密码的加解密规则；

加密： $c=(m+k)\bmod 26$ ，解密： $m=(c-k)\bmod 26$ 。

m:明文对应的数，c：密文对应的数。

(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？

KUJFWAPVU.

2.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 $d$ ；

$d=23.$

2） 设有明文 $m=10$ ，求其密文 $c$ ，再对密文 $c$ 解密。

3.请给出Deffie-Hellman密钥交换协议的一个实例，设 $p=17$ ， $g=3$

解：(1) Alice秘密选定 $a=5$ ，并计算 $A=g^a=3^5 mod(17)=5$ 。发送 $A=10$ 给Bob；

(2) Bob秘密选定 $b=7$ ，并计算 $B=g^b=3^7 mod(17)=11$ 。发送 $B=11$ 给Alice；

(3) Alice计算 $K=B^a=11^5(mod17)=10$ ；

(4). Bob计算 $K=A^b=5^7(mod17)=10$ . 即Alice与Bob的共享密钥为10。

(a=3,b=4时，A=10,B=13,K=4)

4. 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 $2P$ ， $3P$ 。

5. 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 $2P$ 。

$2P=(11,13)$

6. 密码学的基本模型：

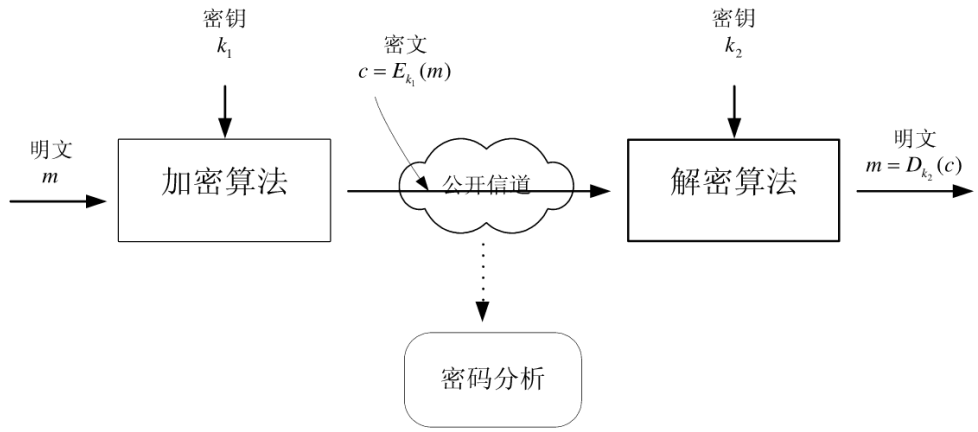



图 1-8　密码学基本模型

对称加密时：$k_1 = k_2$，公钥加密时：$k_1$不等于$k_2$。

7. 简述对称密码算法和公钥密码算法的区别。

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。

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）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。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。

8. 如何理解“适当的安全？”

要点：1）所谓适当的安全，是指安全性的选择应建立在所保护的资源和服务的收益预期大于为之付出的代价的基础之上：破译的代价超出信息本身的价值，破译的时间超出了信息的有效期。

2）采取控制措施所降低的风险损失要大于付出的代价，如果代价大于损失就没有必

要了。

9. 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ElGamal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.

10. 请给出ElGamal数字签名方案并说明其合理性。

答：签名方案包括三个过程：参数建立，签名生成，签名验证，合理性。

参数建立：

1) 选取一个大素数$p$，使得$Z_p$上的离散对数问题难解的，取$g$是模$p$ 的一个本原根；

2) 选取正整数$a, 1 < a < p-1$, 计算$b \equiv g^a (\mod p)$;

3) $(p, g)$是公开参数，$b$与a分别作为签名者的公钥与私钥。

签名生成：

对消息$m \in Z_p$，Alice 随机选取一个整数$k, 1 \le k < p-1$ ，满足$\gcd(k, p-1) = 1$, 并计算

$$r = g^k (\mod p),\ s = (m - ar)k^{-1} (\mod p-1)$$

$(r, s)$是 Alice 对消息$m$的签名。将 $(r, s)$发送给 Bob。

签名验证：

Bob 收到$(r, s)$后，先从公开信道上获取 Alice 的公钥$(p, g, b)$，再验证

$$b^r r^s \equiv g^m (\mod p)$$

是否成立？若成立，则接受$(r, s)$ 为 Alice 对$m$的有效签名，否则拒绝此签名。

合理性：

因为$1 \equiv g^{p-1} (\mod p)$, 且$sk = m - ar (\mod p-1)$, 所以

$$b^r r^s = (g^a)^r (g^k)^s = g^{ar+ks} \equiv g^m (\mod p)$$

如果采用 Hash 函数对消息$m$作消息摘要，只要在算法中将消息$m$换成消息摘要$h(m)$即可。

11. 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；

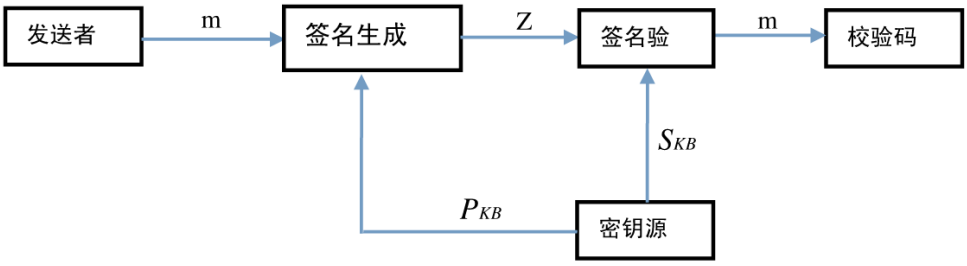
2）不可抵赖性：签名者事后不能否认自己的签名；

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。

5）数据完整性：已签名的内容或消息是不可改变的（既不能被修改、删除等）。如果已签名的消息被改变，则他人可发现消息与签名之间的不一致性。

6）一般模型：




7）功能或作用：可以解决否认、伪造、篡改、冒充等问题。

12. 利用本学期所学知识，设计一文件安全传输方案。

参考答案：以终端 A 为发送方，终端 B 为接收方为例，实现流程大致应如下。

终端 A 操作：

1)与终端 B 预先协商好通信过程中所使用到的对称加密算法、非对称加密算法和哈希函数；

2)采用对称加密算法（密钥称之为会话密钥）对传输信息进行加密得到密文，确保传输信息的保密性；

3)使用终端 B 的公钥对会话密钥进行加密，确保传输信息的保密性以及信息接收方的不可否认性；

4)采用哈希函数（生成文件摘要）确保传输信息的完整性，并使用自己的私钥对文件摘要进行签名（得到数字签名），确保信息发送方的不可否认性；

5)将密文、加密后的会话密钥和数字签名打包封装（放到一起）后，通过网络传输给终端 B。

终端 B 操作：

1)与终端 A 预先已协商好通信过程中所使用到的对称加密算法、非对称加密算法和哈希函数；

2)使用自己的私钥对终端 A 加密的会话密钥进行解密，得到准会话密钥；

3)使用准会话密钥对得到的密文进行解密，得到准明文；

4)使用终端 A 的公钥对得到的数字签名进行解密，得到准明文摘要；

5)使用哈希函数计算得到准明文摘要；

6)将计算得到的摘要与准明文摘要进行比较，若相同则表明文件安全传输成功。

13. 请描述 DES 算法（提示：加密流程图和圈函数结构）。

14. 请给出RSA签名，验证算法及其正确性证明。

15. 请给出Hash函数的定义、性质和应用（2条即可）。

16. (t,n)门限秘密分享方案。

17. 在公钥密码管理中，公钥与私钥的保密性、完整性都需要确保吗？为什么？

18. 简述密码意义上安全的哈希函数应满足什么要求？

单向性，弱抗碰撞的，强抗碰撞的。

19. RSA 公钥加密方案和数字签名方案。

20. 椭圆曲线密码体制。

21. 设$F_2$是二元域，并设$m(x) = x^8 + x^4 + x^3 + x + 1$，则$m(x)$是$F_2$上的不可约多项式，且商$F_2/(m(x))$同构或等同于有限域$GF(2^8)$。

在域$F_2/(m(x))$中求$f_1(x) = x^6 + x^4 + x^3 + x + 1$与$f_2(x) = x^7 + x^4 + x^2 + x + 1$的和与乘积。

$f_1(x) + f_2(x) = x\text{^}7 + x\text{^}6 + x\text{^}3 + x\text{^}2$

$f_1(x) \bullet f_2(x) = x\text{^}5 + x\text{^}4 + x\text{^}3 + x\text{^}2 + x + 1$