**《现代密码学习题》答案**

第一章

**判断题**

**×√√√√×√√**

**选择题**

1、1949年，（ A ）发表题为《保密系统的通信理论》的文章，为密码系统建立了理论基础，从此密码学成了一门科学。

A、Shannon B、Diffie C、Hellman D、Shamir

2、一个密码系统至少由明文、密文、加密算法、解密算法和密钥5部分组成，而其安全性是由（ D）决定的。

A、加密算法B、解密算法C、加解密算法 D、密钥

3、计算和估计出破译密码系统的计算量下限，利用已有的最好方法破译它的所需要的代价超出了破译者的破译能力（如时间、空间、资金等资源），那么该密码系统的安全性是（ B ）。

A无条件安全B计算安全C可证明安全D实际安全

4、根据密码分析者所掌握的分析资料的不通，密码分析一般可分为4类：唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击，其中破译难度最大的是（ D ）。

A、唯密文攻击 B、已知明文攻击 C、选择明文攻击 D、选择密文攻击

**填空题：**

5、1976年，W.Diffie和M.Hellman在 密码学的新方向 一文中提出了公开密钥密码的思想，从而开创了现代密码学的新领域。

6、密码学的发展过程中，两个质的飞跃分别指 1949年香农发表的保密系统的通信理论 和 公钥密码思想 。

7、密码学是研究信息寄信息系统安全的科学，密码学又分为 密码编码 学和 密码分析 学。

8、一个保密系统一般是 明文 、 密文 、 密钥 、 加密算法 、 解密算法 5部分组成的。

9、密码体制是指实现加密和解密功能的密码方案，从使用密钥策略上，可分为 对称 和 非对称 。

10、对称密码体制又称为 秘密密钥 密码体制，它包括 分组 密码和 序列 密码。

第二章

**判断题：**

**×√√√**

**选择题：**

1、字母频率分析法对（B ）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

2、（D）算法抵抗频率分析攻击能力最强，而对已知明文攻击最弱。

A仿射密码B维吉利亚密码C轮转密码D希尔密码

3、重合指数法对（C）算法的破解最有效。

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、维吉利亚密码是古典密码体制比较有代表性的一种密码，其密码体制采用的是（C ）。

A置换密码B单表代换密码C多表代换密码D序列密码

**填空题：**

5、在1949年香农发表《保密系统的通信理论》之前，密码学算法主要通过字符间的 简单置换 和 代换 实现，一般认为密码体制属于传统密码学范畴。

6、传统密码体制主要有两种，分别是指 置换密码 和 代换密码 。

7、置换密码又叫 换位密码 ，最常见的置换密码有 列置换 和 周期转置换密码 。

8、代换是传统密码体制中最基本的处理技巧，按照一个明文字母是否总是被一个固定的字母代替进行划分，代换密码主要分为两类： 单表代换 和 多表代换密码 。

9、一个有6个转轮密码机是一个周期长度为 26 的6次方 的多表代替密码机械装置。

第三章

**判断题：**

**√√√√××**

**选择题：**

2.（1）--（6）DDADAC

**填空题：**

3.（1）.自反性，对称性和传递性

（2）.gcd(a,m)=1

（3）.子域，扩域

（4）.保密系统的通信理论

（5）.冗余度和唯一解距离

（7）.时间复杂度和空间复杂度

第四章

**判断题：**

**（1-5）×√√√×（6-11）××√√√√**

1、在（ C ）年，美国国家标准局把IBM的Tuchman-Meyer方案确定数据加密标准，即DES。

A、1949 B、1972 C、1977 D、2001

2、密码学历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、IDEA D、RC6

3、在DES算法中，如果给定初始密钥K，经子密钥产生的各个子密钥都相同，则称该密钥K为弱密钥，DES算法弱密钥的个数为（B ）。

A、2 B、4 C、8 D、16

4、差分分析是针对下面（A）密码算法的分析方法。

A、DES B、AES C、RC4 D、MD5

5、AES结构由一下4个不通的模块组成，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

6、适合文件加密，而且有少量错误时不会造成同步失败，是软件加密的最好选择，这种分组密码的操作模式是指（ D ）。

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

7、设明文分组序列X1…Xn产生的密文分组序列为Y1…Yn。假设一个密文分组Y1在传输是出现了错误（即某些1变成了0，或者相反）。不能正确解密的明文分组数目在应用（ ）模式时为1.

A、电子密码本模式和输出反馈模式

B、电子密码本模式和密码分组链接模式

C、密码反馈模式和密码分组链接模式

D、密码分组链接模式和输出反馈模式

8、IDEA使用的密钥长度为（ C ）位。

A、56 B、64 C、128 D、156

9、Skipjack是一个密钥长度为（C）位分组加密算法。

A、56 B、64 C、80 D、128

10、分组密码主要采用 混乱 原则和 扩散 原则来抵抗攻击者对该密码体制的统计分析。

11、在今天看来，DES算法已经不再安全，其主要愿意是 源于密钥空间的限制，容易被穷举攻破 。

12、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 安全性、速度 和 灵活性 。

13、DES的轮函数F是由三个部分： 扩展置换 、 非线性代换 和 线性置换 组成的。

14、DES密码中所有的弱密钥、半弱密钥、四分之一弱密钥和八分之一弱密钥全部加起来，一共有 256 个安全性较差的密钥。

15、关于DES算法，密钥的长度（即有效位数）是 56 位，又其 互补 性使DES在选择明文攻击下所需的工作量减半。

16、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加密算法的非线性预算部分是指 字节代换，AES加密算法的非线性运算部分是指**S**盒。

17、在 2001 年，美国国家标准与技术研究所正式公布高级加密标准AES。

18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。

19、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 。

第五章

**判断题：**

**（1-5）√×√√×**

**选择题：**

1、m序列本身是适宜的伪随机序列产生器，但只有在（ A ）下，破译者才不能破解这个伪随机序列。

A、唯密文攻击 B、已知明文攻击 C、选择明文攻击 D、选择密文攻击

2、Geffe发生器使用了（ C ）个LFSR。

A、1 B、2 C、3 D、4

3、J-K触发器使用了（ B ）个LFSR。

A、1 B、2 C、3 D、4

4、PKZIP算法广泛应用于（ D ）程序。

A、文档数据加密 B、数据传输加密 C、数字签名 D、文档数据压缩

5、A5算法的主要组成部分是3个长度不通的线性移位寄存器，即A、B、C。其中A有（A ）位，B有（ D）位，C有（ E ）位。

A、19 B、20 C、21 D、22 E、23

6、SEAL使用了4个（ B ）位寄存器。

A、24 B、32 C、48 D、56

7、按目前的计算能力，RC4算法的密钥长度至少应为（ C ）才能保证安全强度。

A、任意位 B、64位 C、128位 D、256位

8、目前，使用最广发的序列密码是（ A ）。

A、RC4 B、A5 C、SEAL D、PKZIP

**填空题：**

9、序列密码的起源可以追溯到 Vernam密码算法 。

10、序列密码结构可分为 驱动部分 和 组合部分 两个主要组成部分。

11、序列密码的安全核心问题是 如何将一小段的比特串（密钥）扩展成足够“长”的密钥 。

12、序列密码的工作方式一般分为是 同步和自同步。

13、一般地，一个反馈移位寄存器由两部分组成： 移位寄存器 和 反馈函数 。

14、反馈移位寄存器输出序列生成过程中， 对输出序列周期长度起着决定性的作用，而 对输出的序列起着决定性的作用。

15、选择合适的n级线性反馈函数可使序列的周期达到最大值 2的n次方－1 ，并具有m序列特性，但敌手知道一段长为 n 的明密文对时即能破译这n级线性反馈函数。

16、门限发生器要求：LFSR的数目是 奇数 ，确信所有的LFSR的长度 互素 ，且所有的反馈多项式都是 本原的 ，这样可达到最大周期。

第六章

**判断题：**

**（1-5）√√√√×（6-10）√××√√**

**选择题：**

1、下面（A ）不是Hash函数的等价提法。

A、压缩信息函数 B、哈希函数 C、单向散列函数 D、杂凑函数

2、下面（ B ）不是Hsha函数具有的特性。

A、单向性 B、可逆性 C、压缩性 D、抗碰撞性

3、线代密码学中很多应用包含散列运算，而应用中不包含散列运算的是（ A ）。

A、消息机密性 B、消息完整性 C、消息认证码 D、数字签名

4、西面（ C ）不是Hash函数的主要应用。

A、文件校验B、数字签名C、数据加密D、认证协议

5、MD5算法以（ D ）位分组来处理输入文本。

A、64 B、128 C、256 D、512

6、MD5的主循环有（B ）轮。

A、3 B、4 C、5 D、8

7、SHA1接收任何长度的输入消息，并产生长度为（B ）bit的Hash值。

A、64 B、160 C、128 D、512

8、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（ D ）。

A、分组 B、迭代 C、非线性 D、可逆

9、生日攻击是针对（ D ）密码算法的分析方法。

A、DES B、AES C、RC4 D、MD5

10、设Hash函数的输出长度为n bit，则安全的Hash函数寻找碰撞的复杂度应该为（ C ）。

A、O（P（n））B、O(2n) C、O（2n-1）D、O（2n/2）

11、MD5的压缩函数中，512bit的消息被分为16块输入到步函数，每一块输入（ B ）次。

A、3 B、4 C、5 D、8

**填空题：**

12、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 散列值 。

13、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 。

14、Hash函数的抗碰撞性是指 。

15、MD5算法的输入是最大长度小于 2的64次方 bit的消息，输出为 128 bit的消息摘要。

16、MD5的分组处理是由4轮构成的，每一轮处理过程类似，只是使用的 寄存器 不同，而每轮又由16个步函数组成，每个步函数相投，但为了消除输入数据的规律性而选用的 逻辑函数 （非线性函数） 不同。

17、SHA1的分组处理是有80步构成的，每20步之间的处理差异在于使用的 寄存器 和 非线性函数 是不同的，而每步的32bit消息字生成也有所差异，其中前 16 步直接来自消息分组的消息字，而余下的 14 步的消息字是由前面的4个值相互异或后再循环移位得到的。

18、与以往攻击者的目标不通，散列函数的攻击不是恢复原始的明文，而是寻找 散列函数 的过程，最常用的攻击方法是 生日攻击，中途相遇攻击 。

19、消息认证码的作用是 验证信息来源的正确性 和 验证消息的完整性 。

20、MD5、SHA1、SHA256使用的寄存器长度为 32 bit，SHA512使用的寄存器长度为 64 bit.

21、设消息为“Hi”，则用MD5算法压缩前，填充后的消息二进制表示为 。

第七章

**判断题：**

**（1-7）×√××√√√**

**选择题：**

1、下列（ D）算法不具有雪崩效应。

A、DES加密B、序列密码的生成C、哈希函数D、RSA加密

2、若Alice想向Bob分发一个会话密钥，采用ElGamal公钥加密算法，那么Alice应该选用的密钥是（ C ）。

A、Alice的公钥 B、Alice的私钥 C、Bob的公钥 D、Bob的私钥

3、设在RSA的公钥密码体制中，公钥为（e,n）=(13,35)，则私钥d=（ B）。

A、11 B、13 C、15 D、17

4、在现有的计算能力条件下，对于非对称密码算法Elgamal，被认为是安全的最小密钥长度是（ D ）。

A、128位 B、160位 C、512位 D、1024位

5、在现有的计算能力条件下，对于椭圆曲线密码算法，被认为是安全的最小密钥长度是（ B ）。

A、128位 B、160位 C、512位 D、1024位

6、指数积分法针对下面（ C ）密码算法的分析方法。

A、背包密码体制 B、RSA C、ElGamal D、ECC

**填空题：**

7、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。

8、 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。

9、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 。

10、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 。

11、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。

12、基于身份的密码体制，李永用户公开的信息作为公钥来解决用户公钥的真实性问题，但在实际应用中，这种体制存在以下两方面不足： 用户私钥的安全性 ， 这种体制的应用范围 。

13、Rabin公钥密码体制是1979你M.O.Rabin在论文《Digital Signature Public-Key as Factorization》中提出的一种新的公钥密码体制，它是基于 合数模下求解平方根的困难性 （等价于分解大整数）构造的一种公钥密码体制。

14、1984年，Shamir提出了一种 基于身份的加密方案IBE 的思想，方案中不使用任何证书，直接将用户的身份作为公钥，以此来简化公钥基础设施PKI中基于公钥证书维护的过程。

第八章

**判断题：**

**（1-7）××××√√×**

**选择题：**

1、通信中仅仅使用数字签名技术，不能保证的服务是（ C）。

A、认证服务B、完整性服务C、保密性服务D、防否认服务

2、Alice收到Bob发给他的一个文件的签名，并要验证这个签名的有效性，那么签名验证算法需要Alice选用的密钥是（C ）。

A、Alice的公钥B、Alice的私钥 C、Bob的公钥 D、Bob的私钥

3、在普通数字签名中，签名者使用（ B ）进行信息签名。

A、签名者的公钥 B、签名者的私钥 C、签名者的公钥和私钥 D、签名者的私钥

4、签名者无法知道所签消息的具体内容，即使后来签名者见到这个签名时，也不能确定当时签名的行为，这种签名称为（D ）。

A、代理签名B、群签名 C、多重签名 D、盲签名

5、签名者把他的签名权授给某个人，这个人代表原始签名者进行签名，这种签名称为（ A ）。

A、代理签名 B、群签名C、多重签名D、盲签名

6、下列（ A ）签名中，签名这的公钥对应多个私钥。

A、失败——停止签名 B、前向安全签名 C、变色龙签名 D、同时生效签名

7、下列（ B ）签名中，除了签名者以外还有人能够生成有效签名。

A、失败——停止签名 B、前向安全签名 C、变色龙签名 D、同时生效签名

**填空题：**

8、在数字签名方案中，不仅可以实现消息的不可否认型，而且还能实现消息的 完整性 、 机密性。

9、普通数字签名一般包括3个过程，分别是 系统初始化 、 签名产生过程 和 签名验证过程。

10、1994年12月美国NIST正式办不了数字签名标准DSS，它是在 ElGamal 和 Schnorr数字签名的方案 的基础上设计的。

11、根据不通的签名过程，多重数字签名方案可分两类：即 有序多重数字签名 和 广播多重数字签名 。

12、群签名除具有一般数字签名的特点外，还有两个特征：即 匿名性 和 抗联合攻击 。

13、盲签名除具有一般数字签名的特点外，还有两个特征：即 匿名性 和 不可追踪性 。

14、代理签名按照原始签名者给代理签名者的授权形式可分为3种： 完全委托的代理签名 、 部分授权的代理签名 和 带授权书的代理签名 。

15、门限数字签名是一种涉及一个组，需要由多个用户来共同进行数字签名的，其具有两个重要的特征： 门限特性 和 健壮性 。

16、一次性数字签名是指签名者只能签署一条消息的签名方案，如果签名者签署消息不多于一个，那么 私钥就有可能泄露 。

第九章

**判断题：**

（1-7）√√×√××√

**选择题：**

2.（1）-（6）.BCCDBB

**填空题：**

3.（1）.每一步必须明确定义，并且不会引起歧义

.对每种可能的情况必须规定具体的动作

（2）.完全，计算，统计

（3）.隐蔽性，绑定性

（4）.Schnorr利用离散对数的知识证明

（5）.在求解中方便求根

（6）.取数协议，支付协议，存整协议

（7）.注册，投票，计票

（8）.匿名性，课追踪性

第十章

**1判断题**

（1-5）√√√√√（6-8）√××

**2选择题**

（1-5）ADCBC （6-8）CCD

3简答题.

（1）.会话密钥，密钥加密，主密钥

（2）.集中式交换方案和分布式交换方案。

（3）.使用前状态，使用状态，使用后状态和延期状态

（4）.密钥生成

（5）.网外分发，网内分发

（6）.公开密钥分发和秘密密钥的分发

（7）.无中心控制分发和有中心控制分发

（8）.中间人攻击

（9）.用户安全分量，密钥托管分量和数据恢复分量

（10）.密钥托管代理，数据恢复密钥，数据恢复业务和托管密钥防护

（11）.拉格朗日插值

（12）.中国剩余

**部分简答题答案：**

1.公钥密码体制与对称密码体制相比有什么有点和不足？

优点：

1. 密钥的分发相对容易；
2. 密钥管理简单；
3. 可以有效地实现数字签名。

缺点：

1. 与对称密码体制相比，费对称密码体制加解密速度比较慢；
2. 同等安全强度下，费对称密码体制要求的密钥位数要多一些；
3. 密文的长度往往大于明文长度。

2. 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。

3.简述保密系统的攻击方法。

1. 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；
2. 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；
3. 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；
4. 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；
5. 选择文本攻击，是选择明文攻击和选择密文攻击的组合

4.简述DES算法中S盒的特点。

1. 具有良好的非线性，既输出的每一个比特与全部输入比特有关；
2. 每一行包括所有的16种4位二进制；
3. 两个输入相差1bit时，输出相差2bit；
4. 如果两个输入刚在中间2个比特上不同，则输出至少有两个比特不同；
5. 如果两个输入前两位比特不同而最后两位相同，则输出一定不同；
6. 相差6bit的输入共有32对，在这32对中有不超过8对的输出相同；
7. S盒是DES中唯一非线性部分

5.为什么二重DES并不像人们想象的那样可以提高密钥长度到112bit，而相当于57bit？简要说明原因。

明文攻击可以成功攻击密钥长度为112位的二重DES，其计算量级位2的56次方，与攻击DES所需的计算复杂度2的55次方相当，两者基本在同一个数量级

6．简述DES与AES的相同之处：

1. 二者的圈函数都是由3层构成，非线性层，线性混合层，子密钥异或，只是顺序不同；
2. AES的子密钥异或对应于DES中S盒之前的子密钥异或；
3. AES的列混合运算的目的是让不同的字节相互影响，而DES中的F函数的输出与左边的一半数据相加也有类似的效果；
4. AES的非线性运算是字节代换，对应于DES中唯一的非线性运算S盒；
5. 行移位运算保证了每一行的字节不仅仅影响其他行对应的字节，而且影响其他行所有的字节，这与DES中置换P相似

7.简述序列密码算法和分组密码算法的不同。

分组密码是把明文分成相对比较大的快，对于每一块使用相同的加密函数进行处理，因此，分组密码是无记忆的，相反，序列密码处理的明文长度可以小到1bit，而且序列密码是有记忆的，另外分组密码算法的实际关键在于加解密算法，使之尽可能复杂，而序列密码算法的实际关键在于密钥序列产生器，使之尽可能的不可预测性。

9.密钥序列生成器是序列密码算法的核心，请说出至少5点关于密钥生成器的基本要求。

1. 种子密钥K的长度足够大，一般在128位以上；
2. KG生成的密钥序列{ki}具极大周期；
3. 混合性，既{ki}的每一个比特均与K的大多数比特有关；
4. 扩散性，既K任意比特的改变要引起{ki}在全貌上的改变；
5. 密钥序列{ki}的不可预测，密文及相应的明文的部分信息，不能确定整个{ki}

10.简述A5算法的实现过程。

该算法可以描述成由一个22bit长的参数和64bit长的参数生成两个114bit长的序列的黑盒子。。。。。。。。

1简要说明散列函数的特点。

1. H可以应用于任意长度的消息；
2. H产生定长的输出；
3. 对任意给定的消息x，计算H（x）比较容易，用硬件和软件均可实现
4. 单向性：又称为抗原像性，对任意给定的消息x，找到满足y不等于x，且H（x）=H（y）的消息x在计算上是不可行的
5. 抗弱碰撞性：又称为抗第二原像性，对任意给定的消息x，找到满足y不等于x，且H（x）=H（y）的消息y在计算上是不可行的；
6. 抗强碰撞性：找到任何满足H（x）=H（y）的偶对（x，y）在计算上是不可行的

11.简述MD5的算法。

1. 附加填充位；
2. 初始化链接变量；
3. 分组处理；
4. 步函数；

12.简述SHA1的算法

1. 附加填充位；
2. 初始化链接变量；
3. 以512位的分组为单位处理信息，其核心是一个包含4个循环的模块，每个循环由20个步骤组成；
4. 每一循环均以当前正在处理512bitYq和160bit的缓存值A,B,C,D和E为输入，然后更新缓存内容；
5. 得到最终散列值；

13.与RSA密码体制和ELGamal密码体制相比，简述ECC密码体制的特点。

1. 椭圆曲线密码体制的安全性不同于RSA的大整数因子分解问题及ELGamal素域乘法群离散对数问题。

（2）椭圆曲线资源丰富，同一个有限域上存在着大量不同的椭圆曲线，这为安全性增加了额外保证。

（3）效率方面，在同等安全水平上，椭圆曲线密码体制的密钥长度与RSA，ELGamal的密钥小得多，所以计算量小，处理速度快，存储空间小，传输宽带要求低。

（4）安全性，椭圆曲线密码体制具有更高的安全性

14.简述数字签名的特点。

1. 可信性：签名使文件的接收者相信签名者是慎重的在文件上签名的；
2. 不可重用性：签名不可重用，既统一消息在不同时刻的签名是不同的；
3. 不可改变性：在文件签名后，文件不能改变
4. 不可伪造性：签名能够证明是签名者而不是其他人在文件上签名，任何人都不能伪造签名；
5. 不可否认性：在签名者否认自己的签名时，签名接收者可以请求第三方进行仲裁

15.为什么对称密码体制不能实现消息的不可否认性？

因为通信双方拥有同样的密钥，所以接收方可以否认接收到的消息，发送方也可以否认发 送过某消息，既对称密码体制很难解决签别认证和不可否认性的问题