**第一章**

1．关于电子商务安全，下列说法中错误的是 （ D ）

A．电子商务安全包括计算机网络安全和电子交易安全

B. 电子商务安全是制约电子商务发展的重要因素

C. 电子商务安全与网络安全的区别在于其有不可否认性的要求

D. 决定电子商务安全级别的最重要因素是技术

2. 网上交易中，如果定单在传输过程中订货数量发生了变化，则破坏了安全需求中的 ( C )。

A. 可用性 B.机密性 C.完整性 D. 不可抵赖性

3． 原则保证只有发送方和接收方才能访问消息内容。 （ A ）

A. 机密性 B. 完整性 C. 身份认证 D. 访问控制

4. 电子商务安全涉及的三种因素中，没有 。 （ C ）

A. 人 B. 过程 C. 设备 D. 技术

5. 在 PDRR 模型中， 是静态防护转化为动态的关键，是动态响应的依据。（B）

A. 保护 B. 检测 C. 响应 D. 恢复

6. 在电子商务交易中，消费者面临的威胁不包括 （A ）

A. 虚假订单 B. 付款后不能收到商品

C. 客户资料机密性丧失 D. 非授权访问

7. 截获 攻击与保密性相关；伪造 攻击与认证相关； 篡改 攻击与完整性相关； 中断 攻击与可用性相关。（供选择的答案：篡改、截获、伪造、中断）

8. 如果电子商务系统无法访问了，则破坏了电子商务安全的 可用性 需求。

9. 电子商务安全的目标是：保证交易的真实性、机密性、完整性、 不可抵赖性 和 可用性 。

**第二章**

1. 棋盘密码是将26个英文字母放在5×5的表格中，每个字母对应的密文由行号和列号对应的数字组成，如图2.23所示。如h对应的密文是23，e对应15等。

1 2 3 4 5

1 a b c d e

2 f g h ij k

3 l m n o p

4 q r s t u

5 v w x y z

图2.23 棋盘密码

请问它是属于 （ A ）

A. 单表替代密码 B. 多表替代密码 C. 置换密码 D. 以上都不是

2. 攻击不修改消息的内容。 （ A ）

A. 被动 B. 主动 C. 都是 D. 都不是

3. 在RSA中，若取两个质数p=7、q=13，则其欧拉函数φ(n)的值是（ B ）

A. 84 B. 72 C. 91 D. 112

4. RSA算法建立的理论基础是 ( B )

A. 替代和置换 B. 大数分解 C. 离散对数 D. 散列函数

5. 数字信封技术是结合了对称密码技术和公钥密码技术优点的一种加密技术，它克服了（ D ）

A、对称密码技术密钥管理困难 B、公钥密码技术分发密钥困难

C、对称密码技术无法进行数字签名 D、公钥密码技术加密速度慢

6. 生成数字信封时，我们用 。 ( D )

A、一次性会话密钥，发送方的私钥 B、一次性会话密钥，接收方的私钥

C、发送方的公钥，一次性会话密钥 D、接收方的公钥，一次性会话密钥

7. 如果发送方用自己的私钥加密消息，则可以实现 。 ( D )

A. 保密性 B. 保密与鉴别 C. 保密而非鉴别 D. 鉴别

8. 如果A要和B安全通信，则B不需要知道 。 ( A )

A. A的私钥 B. A的公钥 C. B的公钥 D. B的私钥

9. 通常使用 验证消息的完整性。 ( A )

A. 消息摘要 B. 数字信封 C. 对称解密算法 D. 公钥解密算法

10. 两个不同的消息摘要具有相同散列值时，称为 （ B ）

A. 攻击 B. 冲突 C. 散列 D. 签名

11. 可以保证信息的完整性和用户身份的确定性。 （ C ）

A. 消息摘要 B. 对称密钥 C. 数字签名 D. 时间戳

12. 与对称密钥加密技术相比，公钥加密技术的特点是 （D ）

A. 密钥分配复杂 B. 密钥的保存数量多

C. 加密和解密速度快 D. 可以实现数字签名

13. 正整数n的 欧拉函数 是指小于n并与n互素的非负整数的个数。

14. 时间戳是一个经加密后形成的凭证文档，它包括需加 时间戳的文件的摘要（Digest）、DTS收到文件的日期和时间和 时间戳权威的签名 三个部分。

15. 请将下列常见密码算法按照其类型填入相应单元格中。

① RSA ② MD5 ③ AES ④ IDEA ⑤ DES ⑥ Diffie-Hellman ⑦ DSA ⑧ SHA-1

⑨ ECC ⑩ SEAL

对称（分组）密码算法：3 4 5

流密码：10

公钥密码算法 ：1 6 9 7

Hash算法：2 8

1. 对于自同步流密码，如果密钥流不是与密文相关，而是与明文相关（例如先用种子密钥作为密钥流的前几个密钥字符，再用明文序列作为密钥流接下来的密钥字符），会产生什么问题？

答：会使密钥流变得不随机，降低了密码的安全性。

17. 利用扩展的欧几里德算法求28 mod 75的乘法逆元。

表2 求gcd(28, 75)时扩展欧几里得算法运行表

循环次数 Q X1 X2 X3 Y1 Y2 Y3

赋初值 - 1 0 75 0 1 28

1 2 0 1 28 1 -2 19

2 1 1 -2 19 -1 3 9

3 2 -2 5 9 3 -8 1

答：28在模75下的乘法逆元为19。

18. 求253 mod 11=？ ② 求模43的所有本原根。

在一个使用RSA的公钥密码系统中，如果截获了发给一个其公开密钥是e=5，n=35的用户的密文是c=10。则明文m是什么？

答：253 mod 11 = 0。 本原根是3、5、12、13、14、15、17、19、20、21、22、24、26、27、28、30、31、32、34、36、37、38、39、40、41。

19. 公钥密码体制的加密变换和解密变换应满足哪些条件？

答：加密变换应该是单向的，解密变换必须与加密变换互为反函数，同时具有易于计算和难以逆推的特点。这种方案存在一个明显的缺陷：中间人攻击。如果有人截获了密文和小明的公钥，在发送给接收方之前使用自己的公钥将密文进行解密并篡改，然后再用小明的公钥加密，接收方在使用小明的私钥解密时就会得到错误的明文。

21. 小明想出了一种公钥加密的新方案，他用自己的公钥加密信息，然后将自己的私钥传给接收方，供接收方解密用，请问这种方案存在什么缺陷吗？

答：公钥密码体制的加密变换和解密变换应满足的条件：

（1）对任意明文进行加密变换是很容易的，并且若知道解密密钥，那么对密文的解密也是很容易的；

（2）信息的发送方对任意明文进行加密变换后，接收方进行解密变换就可以得到明文；

（3）若不知道解密密钥，那么即使知道加密密钥，具体的加密与解密算法以及密文，确定明文在计算上也是不可行的。

私钥在传输途中可能被攻击者窃取。 小明用自己的私钥加密信息，他的公钥是公开的，接收方接收到信息后，直接用他的公钥去解密信息。

22. 小强想出了一种数字签名的新方案，他用一个随机的对称密钥加密要签名的明文得到密文，再用自己的私钥加密该对称密钥（签名），然后把密文和加密后的对称密钥一起发送给接收方，接收方如果能解密得到明文，就表明验证签名成功。请问用该方案能够对明文签名吗，为什么？

答：该方案不能对明文签名。因为对称密钥是随机生成的，同一个明文可能会有多个不同的密文，而且接收方无法判断哪一个是正确的，因此数字签名需要使用私钥加密的消息摘要来保证唯一性和真实性。

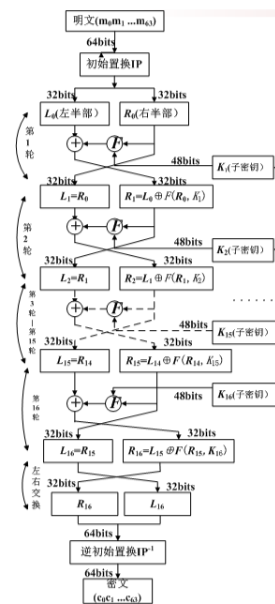
23. MAC与消息摘要有什么区别？

答：消息摘要只能保证消息的完整性，MAC不仅能够保证完整性，还能够保证真实性

1. 对称密钥密码体制和公钥密码体制的密钥分配各有哪些方法？

答：对称密钥密码体制的密钥分配方法包括预先共享密钥、Diffie-Hellman密钥交换和基于密码学哈希函数的密钥派生；公钥密码体制的密钥分配方法包括直接传输公钥、使用数字证书和使用密钥协商协议。

**Des加密过程**



DES算法是密码学中的最基本的加密算法，其基本加密过程如下：

①64位密钥经子密钥产生算法产生出16个子密钥，供16轮加密迭代使用。

②64位明文经过初始置换IP，将数据打乱重新排列并分成左右两半。

③由加密函数f实现子密钥K1对R0的加密，结果为32位的数据组f（R0，K1），f(R0,K1)再与L0模2相加，又得到一个32位的数据组L0模2f（R，K1），以L0模2f（R，K1）作为第二次加密迭代的R1，以R0作为第二次加密迭代的L1.

④第二次至第十六次加密迭代，分别使用使用子密钥K2-K16进行，过程与第一次加密迭代相同；

⑤第十六次加密迭代结束后，产生一个64位的数据组，以其左边32位作为R16，右边32位作为L16，两者合并，再经过逆初始置换IP，将数据重新排列，得到64位密文。