问答题

1. DES特点：分组比较短、密钥太短，密码生命周期短、运算速度较慢。

安全特性：DES算法具有极高的安全性，到目前为止，除了用穷举搜索法对DES算法进行攻击外，还没有发现更有效的办法。

适用场合：

AES特点：安全；代码紧凑，速度够快，适合软硬件实现；结构简单；密钥大小可变

安全特性：

适用场合：

3DES特点： 实现方便，节省投资，DES模块本身不需要改变，只改变上层应用程序。

安全特性：是高强度的加密算法

适用场合：PGP、S/MIME、Mozilla

RC4特点：密钥长度可变

安全特性：

适用场合：

1. RSA原理与计算，给p、q、e、c求d和m

找素数

选取两个512bit的随机素数p,q

计算模n和Euler函数*φ*(n)

n＝pq

*φ*(n)=(p-1)(q-1)

找ed≡1 mod *φ*(n)

选取数e，用扩展Euclid算法求数d

发布

发布(e,n)，这是公钥ke

d保密，(d, n)是私钥 kd

加密

明文分组m作为整数须小于n

c=me mod n

解密

m=cd mod n

例：

* 选p＝7，q＝17

则n＝pq＝119

且φ(n)＝(p-1)(q-1)＝6×16＝96

* 取e＝5

则d＝77 (5×77＝385＝4×96＋1≡1 mod 96)

* 公钥（5，119），私钥（77，119）
* 加密m＝19

则c＝me mod n= 195 mod 119 = 66 mod 119

* 解密c＝66

m＝cd mod n = 6677mod 119＝19 mod 119

1. 公钥算法的用途，从加密（传递会话密钥）到签名
2. Hash函数的特性与用途

特性：单向性质、弱抗碰撞特性、强抗碰撞特性

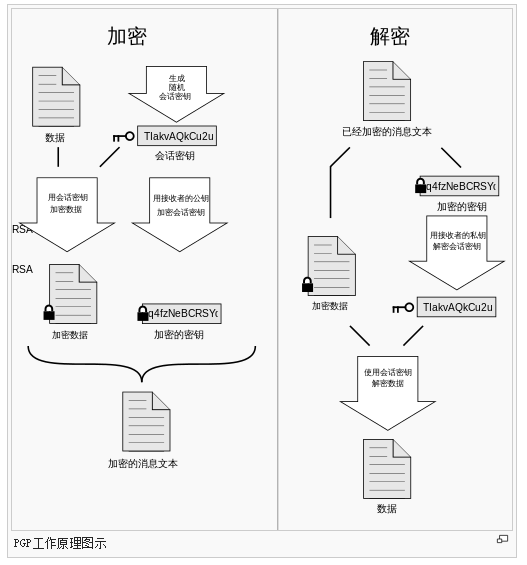
用途：主要用于信息安全领域中加密算法，它把一些不同长度的信息转换成杂乱无章的固定长度的编码里，叫做HASH值。

1. 随机数的特性与用途

特性：不可预测性和不可重复性

用途：

1. 以PKCS#5为代表的，从口令衍生密钥加密文件的方法
2. 以PGP为代表的邮件/文件的加密交换/存储方案；



1. 破解，7475方法等，对抗破解的方法的讨论
2. 逆向，比如针对apk的，以及对抗逆向的方法的讨论；
3. 缓冲区溢出；

缓冲区溢出指的是一种系统攻击的手段，通过向程序的缓冲区写超过其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。简单地说就是程序对接受的输入数据没有进行有效的检测导致错误，后果可能造成程序崩溃或者执行攻击者的命令。在C语言中，常见的缓冲区溢出的函数是：sprintf(), vsprintf(),gets(),scanf()等。

1. 计算器病毒的机制与防范讨论；不光关心windows，也要考虑linux，更要关心手机，包括安卓和苹果。

计算机病毒的机制：

病毒程序是一种特殊程序，其最大的特点是具有感染能力。病毒的感染动作受到触发机制的控制，病毒触发机制还控制了病毒的破坏动作。病毒程序一般由感染模块、触发模块、破坏模块、主控模块组成，相应为传染机制、触发机制和破坏机制。

传染机制：1）寻找一个可执行文件

2）检查该文件是否有感染标记

3)如果没有感染标记，进行感染，将病毒代码放入宿主程序

触发机制：根据预定条件是否满足，控制病毒的感染或破坏动作。依据触发条件的情况，可以控制病毒感染和破坏动作的频率

破坏机制：实现病毒编写者预定破坏动作的代码，可能是破坏文件、数据，破坏计算机的空间效率和时间效率或使机器运行崩溃。

对病毒的防范：

A．反病毒方法：

预防；

检测：一旦系统被感染，就立即断定病毒色存在并对其进行定位；

鉴别：对病毒进行检测后，辨别该病毒的类型；

清除： 在确定病毒的类型后，从受染文件中删除所有的病毒并恢复程序的正常状态

B. 高级反病毒技术：

通用解密技术

数字免疫系统

C. 行为—阻塞软件

1. 讨论比特币中的密码技术是如何起关键作用的；

比特币是一个由密码学和分布式系统构成的数字货币系统。所以对于比特币，他的密码技术特别重要。比特币中的密码技术主要是公钥、私钥和SHA256函数。

公钥和私钥是相互对应的。公钥就是你的钱包地址，私钥相当于你的密码。当你用公匙加密一组数据的时候只有用私匙才可以解密这组数据。 反之当你用私匙加密一组数据的时候，只有用公钥才可以查看这组数据。 比特币的发送就是利用了这个机制

SHA256函数

第一个用sha256来散列付款信。第二个就是散列这些付款信息的散列来生成比特币的block。

1. 文件加密存储，360密盘、truecrypt、ntfs的文件夹绿色加密、bitlock等机制与原理；

360密盘：360密盘根本没有使用AES高强度[加密算法](http://www.haosou.com/s?q=%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95&ie=utf-8&src=wenda_link" \t "_blank)，而只是在[开源](http://www.haosou.com/s?q=%E5%BC%80%E6%BA%90&ie=utf-8&src=wenda_link" \t "_blank)软件filedisk[源代码](http://www.haosou.com/s?q=%E6%BA%90%E4%BB%A3%E7%A0%81&ie=utf-8&src=wenda_link" \t "_blank)的基础上稍做修改，360密盘的加密算法是XOR，根本不是什么AES高强度加密

Truectypt：<http://www.docin.com/p-567554233.html>

ntfs的文件夹绿色加密

bitlock

1. 考虑这3个应用：电商及网银、无纸化办公、QQ。有哪些安全问题和需求、目前是怎么做得，该怎么注意安全，该怎么改进或解决。另，网银u盾和动态口令牌，原理或机制上有啥区别？
2. 那些泄漏案例引发的思考。素材：用户名、口令、邮箱、qq库、开房记录、云中照片、12306、CSDN、tianya、Ashley-Madison，以及传说但是后来未经证实的163的5亿邮箱，等。对于这些泄漏案例，你可以猜测、分析其泄漏的途径和机制，给出你的看法、建议，尤其是针对当前使用的登录、存储、备份、管理、立法等方面的某些缺陷，从技术、管理、立法方面，你有什么建议、改进方案等，深入思考、讨论一下。