1、 信息安全的含义

信息安全是指防止信息资源被故意的或偶然的非授权泄露、更改和破坏，或者信息被非法系统辨认、控制和否认。即确保信息的完整性、机密性、可用性、可控性和不可否认性。

2、安全性 4 种攻击形式：截取，伪造，篡改，否认（选择/填空）

3、4 种攻击方式，哪些是主动攻击，哪些是被动攻击（选择/填空）

主动攻击：伪造，篡改；被动攻击：截取，否认

4、信息安全目标：机密性、完整性、可用性、可控性、不可否认性

5、机密性的定义（选择）

机密性是指保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用。

6、保证机密的手段或方法

通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获知信息内容

7、验证信息是否被篡改的方法：消息摘要算法

8、提供抗否认服务的方式：数字签名

9、现代密码学的两次飞跃是什么？

（1）1949 年 Shannon 发表题为《保密系统的通信理论》，为密码系统建立了理论基础，从此密码学成了一门科学。（第一次飞跃）

（2）1976 年，Diffe 和 Hellman 发表了《密码学的新方向》，提出了一种新的密码设计思想，从而开创了公钥密码学的新纪元。（第二次飞跃）

10、1978 年提出的第一实用的公钥密码体制：RSA

11、凯撒密码属于什么密码体制？代替密码

12、Scytale 密码属于什么密码体制？置换密码

13、一个密码系统（体制）的五大组成部分

明文、密文、加密算法、解密算法、密钥

14、分组密码的原理：扩散，混乱（DES 是分组密码）

（1）扩散是指要将算法设计得使每一比特明文的变化尽可能多地影响到输出密文序列的变化，以便隐蔽明文的统计特性

（2）混乱是指在加密变换过程中是明文、密钥以及密文之间的关系尽可能地复杂化，以防密码破译者采用统计分析法进行破译攻击

15、对称密码算法的优缺点

优点：加解密效率高，适合加密大量数据；密钥相对较短；硬件容易实现。

缺点：需要以安全方式进行密钥交换；密钥管理复杂，如每个人需持有许多密钥。

16、哈希（hash）函数也称散列函数，是一种单向密码体制，即它是一个从明文到密文的不可逆映射，即只有加密过程，不能解密。

17、哈希算法概述

对不同长度的输入消息，产生固定长度的输出。这个固定长度的输出称为原输入消息的“散列”或“消息摘要”（Message digest）。

公式表示形式：h=H(M)

M：任意长度的消息。

H：哈希（Hash）函数或杂凑函数或散列函数。

h：固定长度的哈希值。

18、哈希算法的性质（特点）　（重点记忆 理解）强抗碰撞

压缩：消息 M 是任意有限长度，哈希值 h 是固定长度

容易计算：对于任意给定的消息，容易计算其哈希值

单向性：对于给定的哈希值 h，要找到 M 使得 H(M)＝h 在计算上是不可行的

强抗碰撞：找任意一对不同的消息 M_1, M_2 ，使 $H(M_1)=H(M_2)$ 在计算上是不可行的

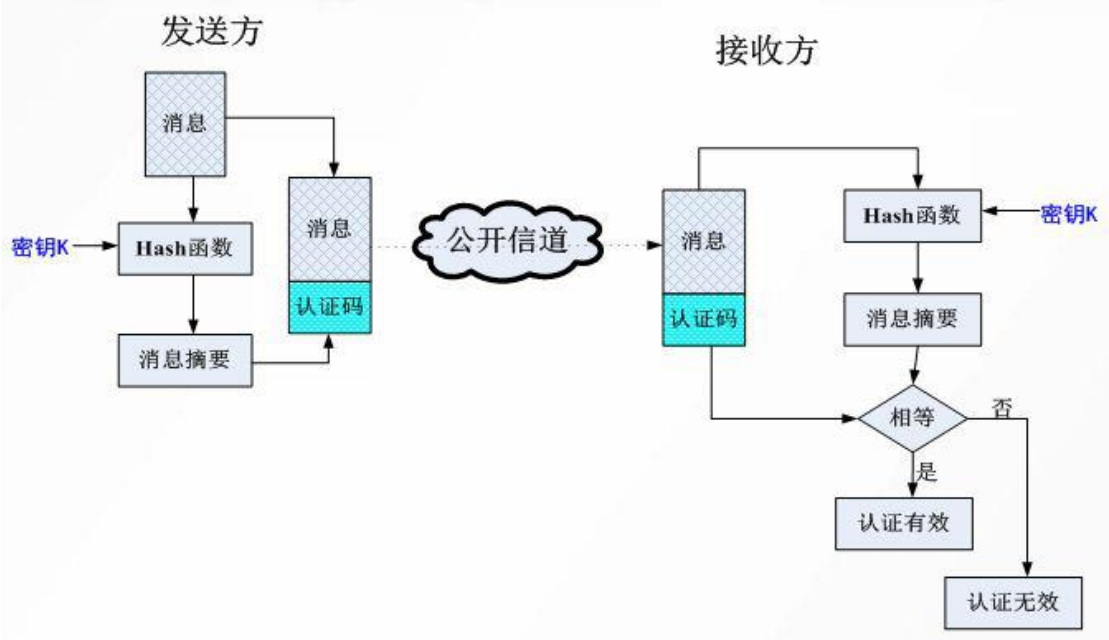
MD5(128 位)和 SHA(160 位)是最著名的两个算法

19、hash 的应用：

数字签名，信息的完整性验证，用于口令的传输和存储

20、消息认证实现过程（理解，简答设计题，画图）

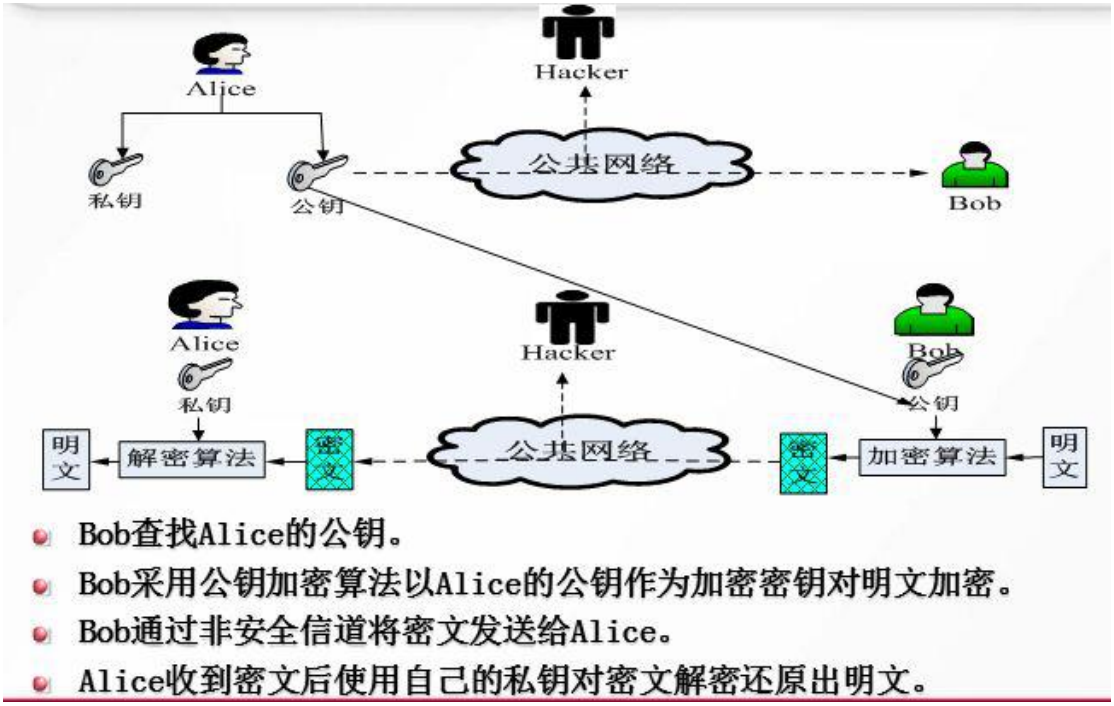
认证可分为实体认证和消息认证



通信双方：发送方，接收方，共享密钥 K

发送方输入消息 M，用密钥 K 和 hash 函数产出固定长度的输出消息摘要，即消息认证码 MAC。消息和 MAC 一起通过公开信道发送给接收方，接收方用相同的密钥 K 对接收到的消息进行相同的 hash 计算，得出消息摘要并与接收到的 MAC 进行比较。如果相等，则证明接收方可以相信消息未被修改，来自真正发送方，认证有效；否则，消息被篡改，认证无效。

21、公钥体制加解密模型（简答设计题）



22、公钥密码算法的两个问题

（1）RSA 算法的安全性基于大整数素因子分解问题

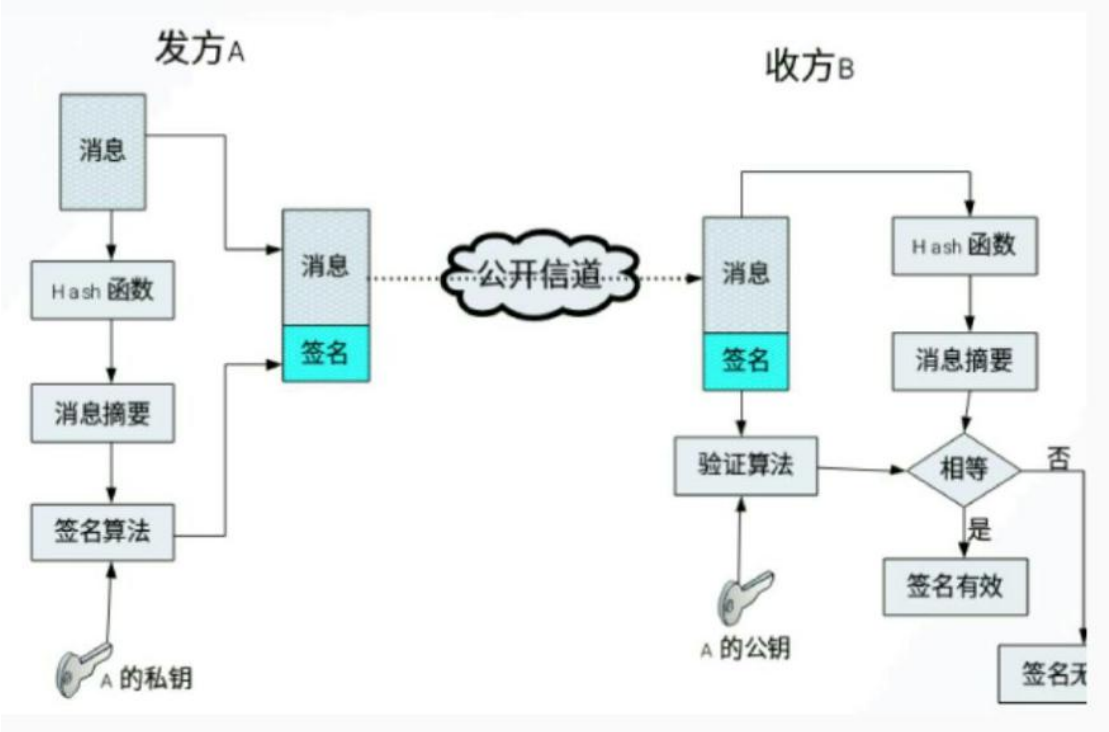
（2）Elgamal 算法的安全性则基于有限域乘法群上的离散对数问题

23、数字签名的应用：身份认证、数据完整性、不可否认性**等**

24、数字签名基于两条基本的假设：一是私钥是安全的，只有其拥有者才能获得；二是产生数字签名的惟一途径是使用私钥。

25、数字签名方案的组成：P:明文空间；S:签名空间；K:密钥空间；Sig:签名算法；Ver:验证算法；

26、数字签名原理图（简答设计题，能用言语表达出来）



发送方 A 输入消息，用 hash 函数算出其消息摘要，再利用 A 的私钥和签名算法生成数字签名并和消息一同经过公开信道发送给接收方 B。B 利用 A 的公钥对签名消息进行验证，计算得出消息摘要，与接收到的消息摘要进行比较，如果相等，则消息真实，签名有效；否则，消息无效。

27、数字签名五大特征

可信（认证）：签名使文件的接收者相信签名者是慎重地在文件上签字的。

不可伪造：签名证明是签名者而不是其他人慎重地在文件上签字。

不可重用：签名是文件的一部分，不法之徒不可能将签名移到不同的

文件上。

不可改变：在文件签名后，文件不能改变的。

不可抵赖：在签名者否认自己的签名时，签名的接收者可向可信的第三方申请仲裁。

28、密钥协商（密钥交换算法）

设 p 是一个大素数，$g \in Z_p$ 是模 p 本原元，p 和 g 公开，所有用户均可获取，并可为所有用户所共有。

⑴用户 A 随机选取一个大数 a，$0 \leqslant a \leqslant p-2$。

⑵用户 A 计算 $K_a=g^a \pmod p$，并将结果传送给用户 B。

⑶用户 B 随机选取一个大数 b，$0 \leqslant b \leqslant p-2$。

⑷用户 B 计算 $K_b=g^b \pmod p$，并将结果传送给用户 A。

⑸用户 A 计算 $K=(K_b)^a \pmod p$。

⑹用户 B 计算 $K=(K_a)^b \pmod p$。

用户 A 和用户 B 各自计算生成共同的会话密钥 K。

这是因为： $K=(K_b)^a=(g^b)^a=g^{ab}=(g^a)^b=(K_a)^b$。

29、PKI（public key infrastructure 公钥基础设施）的含义：PKI 是生成、管理、存储、分发和吊销基于公钥密码学的公钥证书所需要的硬件、软件、人员、策略和规程的总和。

30、PKI（公钥基础设施）：以公钥技术为基础，以数字证书为媒介

31、（填空）PKI 核心机构：CA

管理的核心对象：公钥证书

核心解决网络中的信任问题

32、PKI 核心机构：CA（数字认证中心），CA 管理 X.509 证书

33、X.509 证书内容（填空）

版本号，序列号，认证机构标识，主体标识，主体公钥信息

证书有效期，密钥/证书用法，扩展，认证机构签名

34、PKI 主要组件的简介

公钥证书：由可信实体签名的电子记录，记录将公钥和密钥（公私钥对）所有者的身份捆绑在一起。公钥证书是 PKI 的基本部件。

根 CA：一个单独的、可信任的根 CA 是 PKI 的基础，生成一个自签名证书，亦称 CA 证书或根证书。

注册机构和本地注册机构：接受个人申请，检查其中信息并发送给 CA。RA 可设计成 CA 的代理处，分担 CA 的一定功能以增强可扩展性。

目录服务（证书库）：PKI 的一个重要组成部分，主要用于发布用户的证书和证书作废列表（黑名单）。

PKI 应用接口系统：为各种各样的应用提供安全、一致、可信任的方式与 PKI 交互，确保所建立起来的网络环境安全可靠，并降低管理成本。

35、网络数据加密常见方式：链路加密，节点加密，端到端加密

36、认证最高境界：零知识（填空）

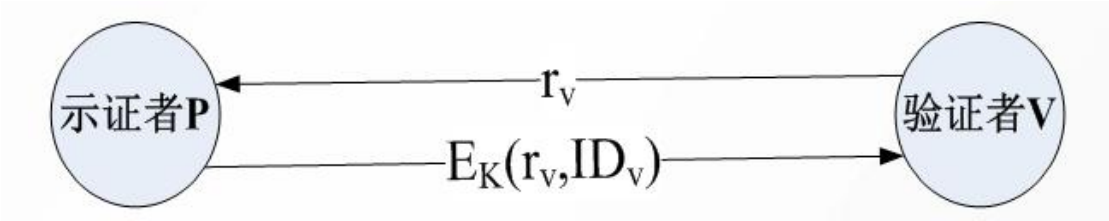
37、利用随机数实现单/双向身份识别（利用对称密钥或非对称密钥实现）

单向身份识别：

⑴验证者 V 选取随机数 r_v 发送给示证者 P。

⑵示证者 P 计算 $E_K(r_v, ID_v)$并发送给验证者 V。

⑶验证者 V 解密 r_v求出 ID_v，验证 ID_v是自己的身份信息，r_v是前一次自己选取的。



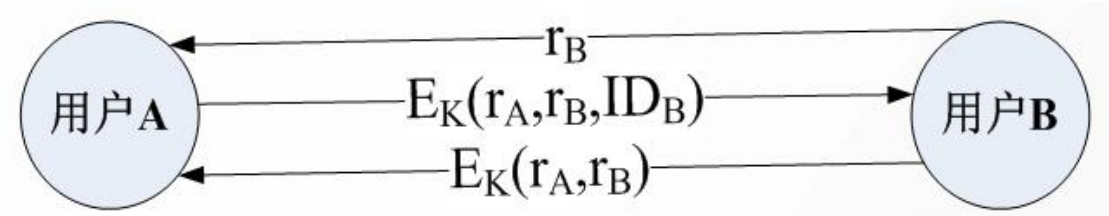
双向身份识别：

⑴用户 B 选取随机数 r_B发送给用户 A。

⑵A 选取随机数 r_A作为询问，计算 $E_K(r_A, r_B, ID_B)$ 发给 B。

⑶B 解密,求出(r_A, r_B)，经核实正确，知道对方为掌握密钥 K 的实体。B 再计算 $E_K(r_A, r_B)$ 发送给 A。

⑷A 解密，求出(r_A, r_B)，经核实正确，知道对方为掌握密钥 K 的实体。



38、Kerberos 认证协议（身份认证协议）

（1）MIT 开发的一种身份鉴别服务。

（2）Kerberos 提供了一个集中式的认证服务器结构，认证服务器的功能是实现用户与其访问的服务器间的相互鉴别。

（3）实现采用的是对称密钥加密技术

39、Kerberos 认证模型：

认证服务器 AS(Authentication Server)：它同时应该连接并维护

一个中央数据库存放用户口令、标识等

票据许可服务器 TGS(Ticket Granting Server)。

整个系统将由四部分组成：AS，TGS，Client，Server。

40、Kerberos 两种票据：服务许可票据，票据许可票据

41、利用掌握的网络知识分析网络协议的不安全性，针对不安全方面问题如何增强安全性？

答：ARP 不安全，原因：ARP 欺骗，易受到“中间人”攻击

IP 不安全，原因：缺乏对通信双方真实身份的认证能力，缺乏对网络上传输的数据包进行机密性和完整性保护

TCP 不安全，原因：它没有三方握手，身份认证，抗重放攻击，加密以及完整性认证。

安全性增强：ARP 避免攻击->电脑绑定 ARP

IP->IPsec 安全协议，IP 与 MAC 绑定

TCP->SSL/TSL 强化 TCP 协议

42、IPsec 协议属于网络层

43、IPsec 协议的组成：ESP、AH、IKE 协议

44、Lifetime（票据的生存期）和 TS（时间戳）都是为了防重放攻击

45、重放攻击

46、IPsec 安全体系结构

（1）IPSec（IP Security）是一种由 IETF(互联网工程任务组，全球互联网最具权威的技术标准化组织)设计的端到端的确保 IP 层通

信安全的机制。

（2）IPSec 不是一个单独的协议，而是一组协议，IPSec 协议的定义文件包括了 12 个 RFC(Request For Comments)文件和几十个 Internet 草案，已成为工业标准的网络安全协议。

（3）IPSec 在 IPv6 中是必须支持的，而在 IPv4 中是可选的。

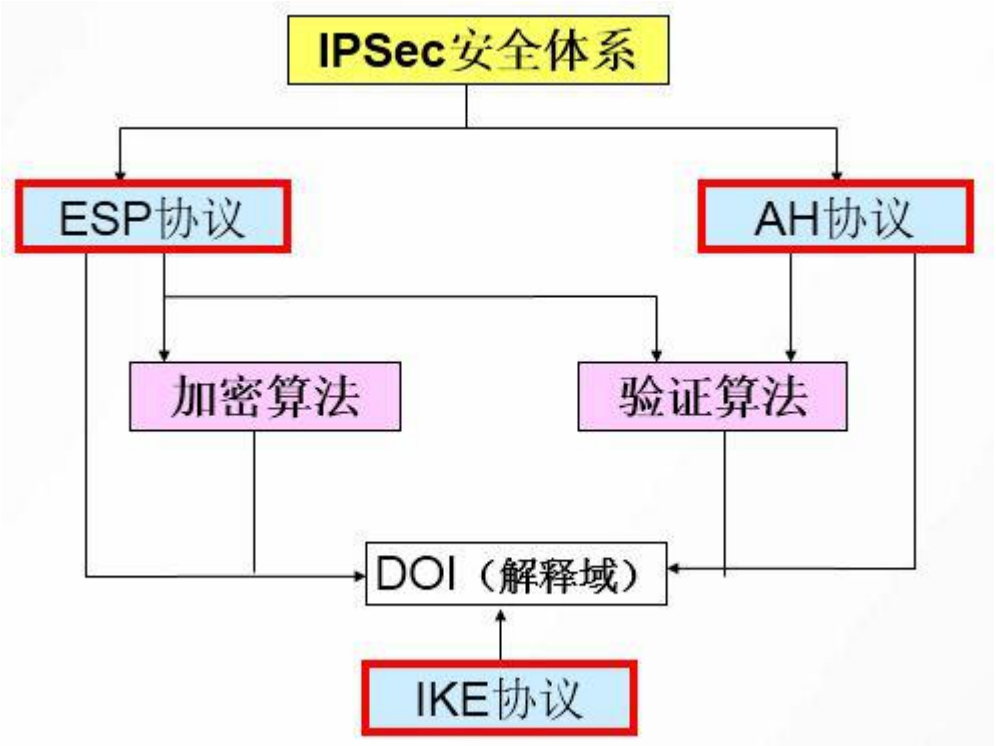
47、IPsec 是在网络层确保安全性

SSL/TSL 是在传输层确保安全性

SSL/TLS 是在应用层确保安全性

48、IPSec 传输模式（在网络层工作是网络层协议）

49、IPSec 体系结构图



50、IPSec 协议中的 AH 协议为数据包提供哪些安全服务，每种安全服务如何实现？

数据完整性验证

通过哈希函数（如 MD5）产生的校验来保证

数据源身份认证

通过在计算验证码时加入一个共享密钥来实现

防重放攻击

AH 报头中的序列号可以防止重放攻击。

51、传输模式要保护的是 IP 包的载荷，隧道模式保护的是整个 IP 包

52、哪个协议与 NAT 不冲突？

传输模式下 ESP 与 NAT 无冲突，隧道模式下 ESP 有冲突（不验证 IP 头）

53、AH 与 ESP 相比：AH 认证功能更强

54、AH 与 NAT 有冲突

55、ESP（封装安全载荷）功能

提供无连接的完整性、数据来源验证、抗重放攻击、数据包加密、数据流加密，加密是 ESP 的基本功能

56、SSL 协议安全性分析

鉴别机制：公开密钥技术和数字证书可以实现客户端和服务器端的身份鉴别。ClientHello 和 ServerHello 发过去自己的证书(里面包含了身份和自己的公钥)。

加密机制：混合密码体制的使用提供了会话和数据传输的加密性保护。双方使用非对称密码体制协商出本次将要使用的会话密钥，并选择一种对称加密算法

完整性机制：定义了共享的、可以用来形成报文鉴别码 MAC 的密钥。

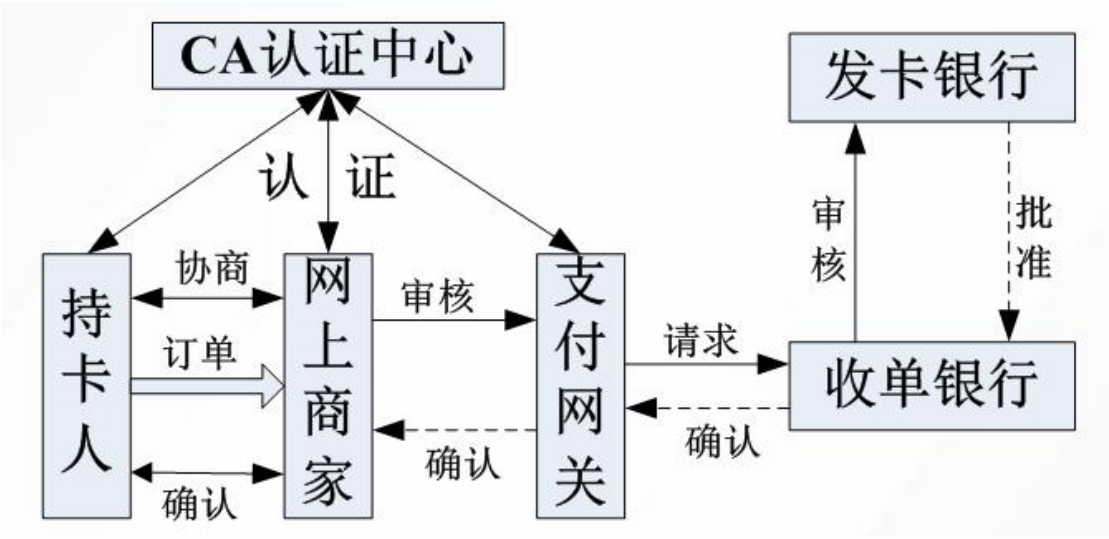
抗重放攻击：SSL 使用序列号来保护通信方免受报文重放攻击。这个序列号被加密后作为数据包的负载。

57、SET 的中文：安全电子交易协议（填空）

58、了解一下电子商务安全与 SET 协议

利用 SET 可以实现电子商务交易中的机密性、认证性、数据完整性和不可否认性等安全功能。

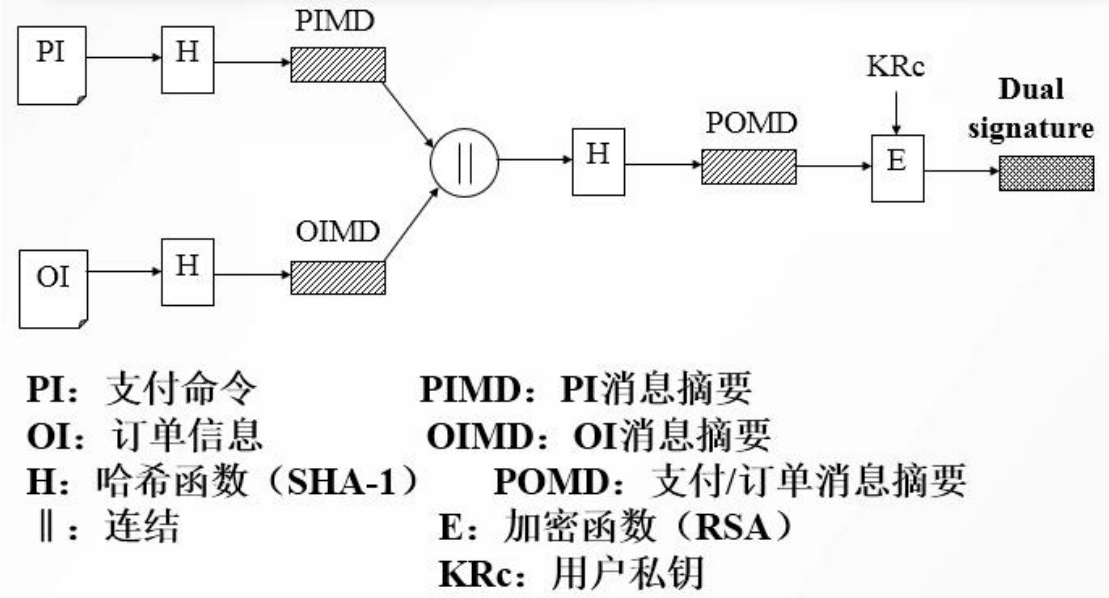
SET 协议涉及的实体：持卡人，发卡银行，收单银行，商家，支付网关，认证中心



59、双重数字签名

双重数字签名就是在有的场合，发送者需要寄出两个相关信息给接收者，对这两组相关信息，接收者只能解读其中一组，另一组只能转送给第三方接收者，不能打开看其内容。这时发送者就需分别加密两组密文，做两组数字签名，故称双重数字签名。

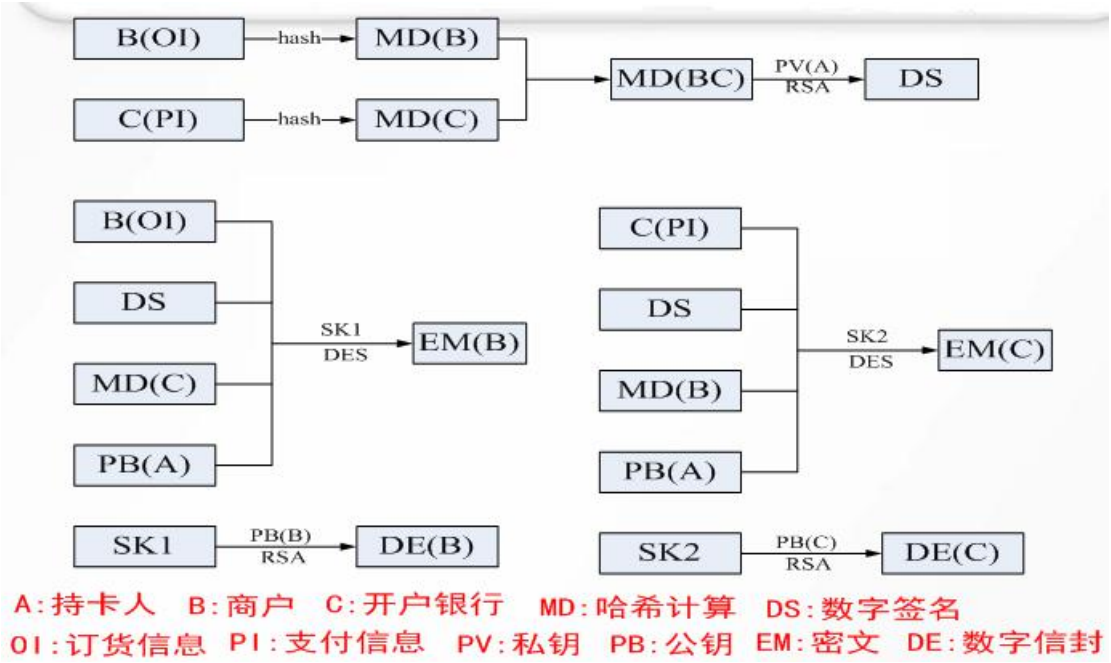
60、双重数字签名的应用



将 OI（订单信息）和 PI（支付信息）用 hash 函数分别生成消息摘要 PIMD（PI 消息摘要）和 OIMD（OI 消息摘要），连结两个消息摘要，

再用 hash 函数生成 POMD（PI/OI 消息摘要），再用用户私钥 KRc 和 E 加密函数（RSA）生成双重签名 Dual signature。

61、持卡者实现过程



商户和开户银行分别将 OI（订单信息）和 PI（支付信息）用 hash 函数计算 MD(B)和 MD(C)生成消息摘要，连结 BC 计算 MD(BC)，再用持卡人的私钥 PV(A)和加密算法（RSA）生成双重签名。

商户订单信息 B(OI)，双重签名 DS，开户银行消息摘要 MD(C)，持卡人 A 的公钥 PB(A)一起利用

62、计算机病毒是一段附着在其他程序上的、可以自我繁殖的程序代码。

63、病毒最根本特征：破坏性

64、常见病毒：

引导型病毒：**大麻病毒、小球病毒、火炬病毒等**

文件型病毒

宏病毒：宏就是能够组织在一起的，可以作为一个独立命令来执行的一系列 Word 命令。**美丽莎 、七月杀手、13 号病毒等**

脚本病毒通过**网页、Email** 等传播。运行网页中 **ActiveX 控件**。欺骗性，如**邮件附件采用双后缀**。

蠕虫病毒：蠕虫(Worm)是一个程序或程序序列，通过分布式网络来扩散传播特定的信息或错误，进而造成网络服务遭到拒绝并发生死锁或系统崩溃。**冲击波病毒**

木马病毒一般分为**客户端**（控制端）和**服务端**（被控端）。

65、无法开机，硬件没坏，可能是中了引入型病毒；**若无法打开网页是脚本病毒；PPT 感染是宏病毒**

66、引导型病毒是通过感染硬盘主引导区或 DOS 引导扇区使电脑中病毒

67、简单包过滤防火墙的原理

1、根据流经防火墙的数据包头信息，决定是否允许该数据包通过。

2、创建包过滤规则

68、简单包过滤防火墙工作在哪层网络？网络层

69、代理防火墙在应用层

70、NAT（网络地址转换）的好处（填空）

1、缓解 IP 地址匮乏问题；

2、对外隐藏了内部主机的 IP 地址，提高了安全性

71、防火墙五大基本功能？

1、防火墙是网络安全的屏障

2、防火墙可以强化网络安全策略

3、对网络存取和访问进行监控审计

4、防止内部信息外泄

5、防火墙的抗攻击能力

72、防火墙的不足：

1、防火墙给人虚假的安全感

2、可能带来传输延迟、瓶颈及单点失效

3、不能替代防火墙内的安全措施

4、不能防范来自内部的攻击和不通过它的连接

5、不能防范利用标准协议缺陷进行的攻击;

6、不能阻止被病毒感染的程序或文件的传递

7、不能防范策略配置不当引起的安全威胁

8、不能防范本身安全漏洞的威胁

73、网络正常，访问不了新浪网：拒绝服务攻击（DOS）

74、DOS（Denial of Service）指拒绝服务攻击是阻止或拒绝合法使用者存取网络服务的一种破坏性攻击方式。

75、负载均衡算法：基于轮询；基于加权轮询；最少链接；加权最少链接

76、透明接入：透明模式下防火墙相当于网桥，原网络结构没有改变

77、安全因素最重要的因素是人（填空）

78、栈和堆的区别

分配和管理方式不同

堆是动态分配的，其空间的分配和释放都由程序员控制。

栈由编译器自动管理。栈有两种分配方式：静态分配和动态分配。静态分配由编译器完成，比如局部变量的分配。动态分配由 malloca() 函数进行分配，但是栈的动态分配和堆是不同的，它的动态分配是由编译器进行释放，无须手工控制。

产生碎片不同

对堆来说，频繁的 new/delete 或者 malloc/free 势必会造成内存空间的不连续，造成大量的碎片，使程序效率降低。

对栈而言，则无碎片问题，因为栈是先进后出的队列，不可能有一个内存块从栈中间弹出。

生长方向不同

堆是向着内存地址增加的方向增长的，从内存的低地址向高地址方向增长。

栈的生长方向与之相反，是向着内存地址减小的方向增长，由内存的高址向低址方向增长。

79、公钥密码算法分类

基于大整数素因子分解问题 ：RSA，Rabin 等

基于有限域乘法群上的离散对数问题：Elgamal（DSA）

椭园曲线上的离散对数问题：ECC

背包问题：Merkle-Hellman，Chor-Rivest

基于余代数编码中的线性解码问题：McEliece

80、RSA 的密钥对生成算法/数字签名方案（了解，可能会考）

1、选取两个大素数 p 和 q，两个数长度接近，1024 位

2、计算 n=p*q， ψ(n)=(p-1)(q-1)

3、随机选取整数 e(1<e< ψ(n))，满足 gcd(e, ψ(n))=1

4、计算 d，满足 d*e=1（mod ψ(n)）。

注：n 公开， p 和 q 保密。

e 为公钥，d 为私钥。

例子：

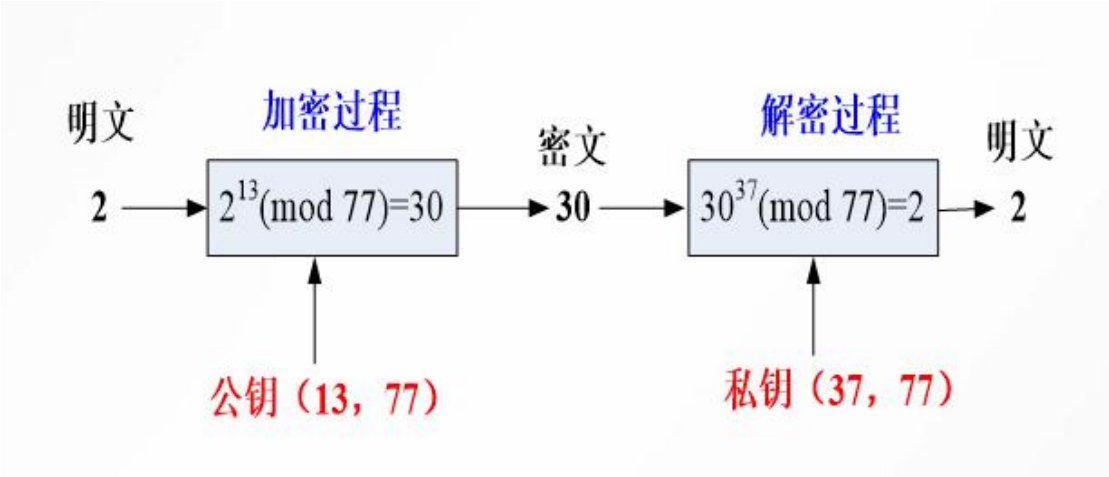
设 p=7, q=11, 取 e=13，求 n， ψ(n)及 d

解：n=7*11=77

ψ(n)=（7-1）*（11-1）=60

因 e=13，满足(1<e< ψ(n))且满足 gcd(e, ψ(n))=1，所以，可以取加密密钥 e=13

通过公式 e*d=1 mod 60 求出 d=37。



81、 RSA 密钥长度：1024 位

82、密钥的生命周期（重点掌握分配和协商）

生成，存储，分配，使用，备份/恢复/存档，更新/撤销/销毁

分配：无中心、中心化、公钥密码体制的密钥分配模式（重点发送发A3步，B3步）

协商：Diffie-Hellman密码交换算法

83、堆溢出的实例，栈溢出的实例

84、A要传输一个大文件给B,要求A不能否认——混合加密（必考）（A 4步，B 3步）

1、A选择一个对称密钥，用RSA算法加密消息

2、A用B的公钥加密对称密钥形成数字信封

3、A算出消息摘要，再用自己的私钥对消息摘要进行签名

4、A把密文、数字信封和签名一起发给B

5、B用自己的私钥解密数字信封，得到对称密钥

6、B用对称密钥把密文解密成明文

7、B计算消息摘要后，用A的公钥来验证签名是否有效

85、公钥加密和对称加密的区别？

公钥：用于加密或验证签名

公钥加密：加/解密时，分别使用不同的密钥，一个对外界公开，称为“公钥”；一个只有所有者知道，称为“私钥”。

对称加密：加解密使用相同密钥。

86、（选择）数字证书的内容

证书有效期：证书有效时间包括两个日期：证书开始有效期和证书失效期。

密钥/证书用法：描述该主体的公/私密钥对的合法用途。

扩展：说明该证书的附加信息。

认证机构签名：用认证机构的私钥生成的数字签名。

87、SA 包括：SPI：用于标识具有相同 ip 地址和相同安全协议的不同 SA，IP 目的地址，IPSec 协议

习题：

1、可以被数据机密性机制防止的攻击方式是（ C ）。

A. 假冒源地址或用户的地址欺骗攻击

B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取

D. 数据在途中被攻击者篡改或破坏