### 加密解密技术

对称加密技术(包括DES 3DES RC-5 IDEA)

DES 该算法采用替换和移位方式 对64位数据加密，秘钥长度56位。速度快，秘钥易产生。

3DES 三重DES 两个秘钥。加密：K1加密 K2解密 K1加密

解密：K1解密 K2加密 K1解密 秘钥长度加倍112位

RC-5 RSA数据安全公司多数产品使用。

IDEA 64位数据块，128位秘钥。比DES加密性好。

非对称加密技术（RSA RSC ECC）

RSA 属于公钥密码系统，1024位秘钥 反向使用公钥密码系统便提供了数字签名的功能，RSA 的安全性较高，但是随之而来的计算量也较大（例如指数运算），且会随着规模的增加而增大。RSA和DSA的安全性及其它各方面性能都差不多，而ECC较之则有着很多的性能优越，包括处理速度，带宽要求，存储空间等等。ECC 160位秘钥

对称加密称为私钥加密，对称密码编码技术。加密高效，但加密强度不大，秘钥分发困难。

非对称加密成为公钥加密，一个公钥对应一个私钥，加强加密强度，安全性提升，但加密速度慢，为对称加密的数千倍。经常加密信息摘要，（数据量小的）。

---------------------------------------------------------------------------------------------------------------------------------

信息摘要（MD5 SHA）

信息摘要简要描述较长的信息或文件。可以用于数字签名。

SHA 散列值160位（加密密钥长度） 安全性较高。

MD5 散列值128位（加密密钥长度）

数字签名（核心）

数字签名技术是对非对称加密技术和信息摘要的综合应用。

先对正文产生信息摘要，然后使用发送者私钥进行加密，完成签名（绝对性证明为A发送的，因为私钥只有本人有），当接收方接收到信息摘要，会使用非对称技术用发送发的公钥解密，若解密，则确定为发送者发送。

数字证书（核心）

CA 数字证书授权中心。用户获取网站的数字证书后通过验证CA签名和确认数字证书的有效性。从而验证第三方网站的安全性。

数字证书包括版本 序列号 签名算法标识符 签发人姓名 有效期 主题名 主题公钥信息

用户与网站安全通信时，用户使用网站的公钥，网站使用私钥，用户发送数据使用网站的公钥加密，网站使用私钥解密，用户接收信息时，网站使用私钥加密，用户使用公钥解密。

数字信封

数字信封分为两步 使用对称秘钥加密技术将数据进行加密，然后采用非对称加密，将此对称秘钥用对方的公钥加密。（加密完成为数字信封打包）

### 网络安全

网络安全协议

PGP 基于RSA公钥加密体系的邮件加密协议。

SSL 是Netscape公司开发安全协议。工作于传输层以上（包括传输层）

SSL协议包括SSL记录协议，SSL握手协议，SSL警报协议。

SSL主要提供三方面的服务：

（1）用户和服务器的合法性认证 要在握手交换数据时数字认证。以确保用户合法性。

（2）加密数据以隐藏被传送的数据 对握手信息加密，并用数字证书鉴别。

（3）保护数据的完整性 HASH函数和机密共享提供信息完整性服务。

SET 基于信用卡进行电子化交易的应用提供安全措施的规则。

TLS 应用于两个通信应用程序之间提供保密性和数据完整性。

网络攻击

主动攻击：中断 篡改 伪造 被动攻击： 监听

中断：通过阻隔源站向目的站之间的通信，以达到攻击目的 例如（剪网线 DDoS攻击）

篡改：先获得源站点信息，将信息进行修改，再以源站身份发送目的站例如（中间人攻击）

伪造：源站点并未发送信息，攻击方以源站点身份向目的站点发送信息。

监听：获取通信双方的通信信息，不做破坏，不易察觉。

DDoS攻击（核心）

DDoS :分布式拒绝服务攻击（肉鸡攻击）凡是能导致合法用户不能够访问正常网络服务的行为都算是拒绝服务攻击。

例如通过分散在各地的僵尸计算机进行攻击，让你的系统所提供的服务被阻断而无法顺利地为其他用户提供服务。

这种攻击方式不入侵你的系统，而是让你的系统无法正常提供服务。

这种攻击方式也是最难处理的，因为要么需要系统核心支持自动阻挡DDoS攻击的机制，要么需要自行撰写侦测软件来进行判断。

ARP欺骗

由于局域网的网络流通不是根据IP地址进行，而是根据[MAC地址](https://baike.sogou.com/lemma/ShowInnerLink.htm?lemmaId=71171&ss_c=ssc.citiao.link" \t "https://baike.sogou.com/_blank)进行传输。所以，MAC地址在A上被伪造成一个不存在的MAC地址，这样就会导致网络不通，A不能Ping通C！这就是一个简单的ARP欺骗。

入侵检测技术

入侵检测系统所采用的技术分为特征检测和异常检测。已从安全审计系统独立出来的系统。

特征检测：也成为误用检测，系统可识别已出现的入侵模型，但新的入侵模型将毫无办法。

异常检测：入侵者活动异于正常主题活动。要正确区分不正常操作与真正的入侵。

防火墙技术（核心）

防火墙可以实现内部网（信任网络）和外部（不信任网络）之间或内部网不同网络安全区域之间的隔离与控制，保证网络系统以及网络服务的可用性。

根据防火墙结构分为：屏蔽路由器，双穴主机，屏蔽主机防火墙，屏蔽子网防火墙。

1. 包过滤型防火墙：工作于网络层，对内部网络分析，并按一定的安全策略进行限制。

只能阻止少部分IP欺骗。

（2）双宿网关防火墙：使用至少两块网卡的堡垒主机为防火墙，位于外部网络，使内部网络与外部网络分离，阻挡不可信网络的非法入侵。

（3）屏蔽主机防火墙：由包过滤型防火墙和双宿网关防火墙合成，实现网络层安全（包过滤）应用层安全（代理）

（4）屏蔽子网防火墙，两个屏蔽路由器和一个堡垒主机，单DMZ防火墙结构，支持网络层和应用层，就算被攻破也无法影响到内部网络，目前最安全的防火墙系统。

VPN技术

[虚拟专用网络](https://baike.sogou.com/lemma/ShowInnerLink.htm?lemmaId=44751&ss_c=ssc.citiao.link" \t "https://baike.sogou.com/_blank)功能是：在[公用网络](https://baike.sogou.com/lemma/ShowInnerLink.htm?lemmaId=69016699&ss_c=ssc.citiao.link" \t "https://baike.sogou.com/_blank)上建立专用网络，进行加密通讯。在企业网络中有广泛应用。[VPN网关](https://baike.sogou.com/lemma/ShowInnerLink.htm?lemmaId=75926849&ss_c=ssc.citiao.link" \t "https://baike.sogou.com/_blank)通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN有多种分类方式，主要是按协议进行分类。VPN可通过服务器、硬件、软件等多种方式实现。VPN具有成本低，易于使用的特点。

### 计算机病毒与木马

计算机病毒与木马的基本概念

病毒重在于破坏，破坏电脑的软件硬件 电脑系统 文件等等 而且病毒种类繁多，不易查找。

木马重在于控制电脑，不确定控制后是否有破坏，木马容易潜伏于后台或内嵌于程序，绑定与文件夹等等，不易查找。

计算机病毒的分类

计算机病毒1引导型病毒 2文件型病毒 3混合型病毒（集两种与一体）

引导型病毒：改写磁盘上引导扇区内容，软盘硬盘皆可能感染。

文件型病毒：感染文件以文件名为COM EXE OVL等为主 它的安装必须借助于病毒载体程序

混合型病毒综合系统引导型病毒和文件型病毒特性。最难灭杀。

病毒种类的命名（核心）

（1）系统病毒：前缀为Win32 Win95 W32 W95 PE 感染Windows操作系统的.exe .dll文件

（2）蠕虫病毒：前缀为Worm 通过网络和系统漏洞传播，大部分蠕虫病毒向外发送带毒邮件，如冲击波（阻塞网络） 小邮差（带毒邮件）

（3）木马病毒：前缀Trojan 例如 Trojan.QQ3344 Trojan.Lmir.PSW.60

（4）黑客病毒：前缀Hake

（5）脚本病毒：前缀Script 通过网页传播，还有VBS JS脚本病毒如VBS.Happytime 等等

（6）宏病毒： 第一前缀Macro 第二前缀Word(DOC) Excel等等它是一种特殊的脚本病毒。

（7）后门病毒：前缀Backdoor 该病毒通过网络传播，系统开后门，安全隐患大

（8）病毒种植程序病毒：体内释放新病毒，新病毒进行破坏，如冰河播种者（Dropper.Binghe2.2c）。MSN射手（Dropper.Worm.Smibag）

（9）破坏性程序病毒：前缀Harm 使用图标诱惑用户。如格式化C盘（Harm.formatC.f）

杀手命令（Harm.Command.Killer）

1. 玩笑病毒：前缀Joke 恶作剧病毒 如女鬼（Joke.Girl.ghost）
2. 捆绑机病毒：前缀Binder 将病毒与软件（QQ IE）等捆绑起来。如捆绑QQ（Binder.QQPass.QQBin） 系统杀手（Binder.killsys）等