目录

[1信息安全概述 4](#_Toc503905572)

[1.1信息与信息安全 4](#_Toc503905573)

[信息： 4](#_Toc503905574)

[信息的定义 5](#_Toc503905575)

[信息的功能 5](#_Toc503905576)

[信息的表达 5](#_Toc503905577)

[信息与消息 5](#_Toc503905578)

[信息与数据 5](#_Toc503905579)

[1.2信息安全威胁 5](#_Toc503905580)

[信息安全的目标 5](#_Toc503905581)

[信息安全的任务 6](#_Toc503905582)

[1.3信息安全发展阶段与形式 6](#_Toc503905583)

[信息技术（information technology IT） 6](#_Toc503905584)

[信息技术包括生产和应用两个方面 6](#_Toc503905585)

[微电子，通信，计算机和网络是信息系统的核心技术，其发展进程大致可分为以下四个阶段： 6](#_Toc503905586)

[1.4信息安全保障 8](#_Toc503905587)

[信息安全 8](#_Toc503905588)

[信息安全的目标 8](#_Toc503905589)

[信息安全的任务 8](#_Toc503905590)

[信息安全的属性 8](#_Toc503905591)

[信息安全的特征 9](#_Toc503905592)

[信息系统安全 10](#_Toc503905593)

[1.5信息系统安全保障 11](#_Toc503905594)

[信息系统安全问题产生的根本原因： 11](#_Toc503905595)

[安全问题根源-内因外因示例 11](#_Toc503905596)

[通信安全 COMSEC 12](#_Toc503905597)

[计算机安全COMPUSEC 12](#_Toc503905598)

[信息系统安全 INFOSEC 12](#_Toc503905599)

[信息安全保障 IA 12](#_Toc503905600)

[我国信息安全形势 13](#_Toc503905601)

[2信息安全基础技术 13](#_Toc503905602)

[2.1密码学 13](#_Toc503905603)

[威胁、安全属性与密码学技术 13](#_Toc503905604)

[密码学发展 13](#_Toc503905605)

[近代密码学 14](#_Toc503905606)

[古典密码学 14](#_Toc503905607)

[现代密码学 14](#_Toc503905608)

[加密与解密 14](#_Toc503905609)

[加密与解密 15](#_Toc503905610)

[转轮机 15](#_Toc503905611)

[公钥密码学 15](#_Toc503905612)

[对称密码算法 16](#_Toc503905613)

[对称密码算算法的优缺点 16](#_Toc503905614)

[非对称加密与解密 17](#_Toc503905615)

[非对称密码算法 17](#_Toc503905616)

[非对称密码学特点 17](#_Toc503905617)

[哈希函数 18](#_Toc503905618)

[哈希运算-完整性 18](#_Toc503905619)

[MD5算法 19](#_Toc503905620)

[SHA-1算法 19](#_Toc503905621)

[数字签名 19](#_Toc503905622)

[数字签名 20](#_Toc503905623)

[数字签名的应用 21](#_Toc503905624)

[2.2数字证书与公钥基础设施 23](#_Toc503905625)

[数字证书 23](#_Toc503905626)

[CA :认证权威机构 23](#_Toc503905627)

[RA:证书注册机构 24](#_Toc503905628)

[目录服务(LDAP ) 24](#_Toc503905629)

[CRL 24](#_Toc503905630)

[2.3身份认证 25](#_Toc503905631)

[身份认证基本方法 25](#_Toc503905632)

[动态口令认证 25](#_Toc503905633)

[短信口令认证 25](#_Toc503905634)

[静态口令认证 26](#_Toc503905635)

[静态口令认证缺点 26](#_Toc503905636)

[U 盾(USB Key) 26](#_Toc503905637)

[基于生物特征的身份认证(二) 27](#_Toc503905638)

[2.4访问控制 29](#_Toc503905639)

[访问控制的概念和目标 29](#_Toc503905640)

[访问控制的作用 29](#_Toc503905641)

[授权 30](#_Toc503905642)

[访问控制矩阵 30](#_Toc503905643)

[自主访问控制的特点 30](#_Toc503905644)

[强制访问控制的含义 30](#_Toc503905645)

[自主访问控制与强制访问控制的比较 31](#_Toc503905646)

[基于角色的访问空制(RBAC) 31](#_Toc503905647)

[RBAC模型的特点 31](#_Toc503905648)

[2.5安全审计 32](#_Toc503905649)

[安全审计 32](#_Toc503905650)

[日志 32](#_Toc503905651)

[安全审计方式 32](#_Toc503905652)

[3.网络安全防护技术 33](#_Toc503905653)

[3.1网络基础知识 33](#_Toc503905654)

[TCPAIP协议 33](#_Toc503905655)

[Internet和TCP/IP协议: 33](#_Toc503905656)

[何为协议? 34](#_Toc503905657)

[何为协议? 续 34](#_Toc503905658)

[网络协议模型之OSI与TCP/IP : 34](#_Toc503905659)

[TCP/IP协议分层： 35](#_Toc503905660)

[通信地址: 35](#_Toc503905661)

[网络中的通信地址: 35](#_Toc503905662)

[IP地址分类: 35](#_Toc503905663)

[封装Encapsulation : 36](#_Toc503905664)

[解封装Decapsulation : 36](#_Toc503905665)

[IPv4报头格式： 37](#_Toc503905666)

[IPV4包头格式: 续 37](#_Toc503905667)

[端口port : 37](#_Toc503905668)

[传输控制协议TCP : 37](#_Toc503905669)

[用户数据报协议U DP : 38](#_Toc503905670)

[万维网( World Wide Web,WWW ) 38](#_Toc503905671)

[超文本标记语言HTML 38](#_Toc503905672)

[超文本传输协议HTTP 38](#_Toc503905673)

[统一资源定位符URL 39](#_Toc503905674)

[3.2网络安全威胁 39](#_Toc503905675)

[3.3网络安全防护与实践 39](#_Toc503905676)

[3.4无线局域网安全防护 39](#_Toc503905677)

# 1信息安全概述

## 1.1信息与信息安全

### 信息：

1信息奠基人香农（C.E Shannon）认为，信息是用来消除随机补习确定性的东西。

2信息是事务运动状态或存在方式的不确定性的描述

3信息是具体的，并且可以被人，生物，机器等所感知，提取，识别，可以被传递，存储变换，处理，系那是检索和利用。

4信息来源于物质，又不是物质本身，他从物质的运动中产生出出来，又可以脱离原物质而寄生于媒体物质，相对独立的存在。

### 信息的定义

信息是有意义的数据，他是具有一定价值，是一种需要适当保护的资产。数据是反映客观事物属性的记录，是信息的具体表现形式。数据经过加工处理之后，就变成了信息；而信息需要经过数字化处理转变成数据才能存储和传输。

### 信息的功能

反应事物内部属性，状态，结构，相互联系以及与外部环境的互动关系，减少事物的不确定性。

### 信息的表达

信息本身事务性的，借助于信息媒体以多种形式存在或者传播，它可以存储在计算机，磁带，纸张等介质中，也可以记忆在人的大脑里，还可以通过网络等方式进行传播。

### 信息与消息

信息不同于消息，消息是信息的外壳，信息则是消息的内核，也可以说，消息是消息的笼统概念，信息则是消息的精确概念

### 信息与数据

信息不同于数据，数据是信息的符号解释，或者成载体，信息是数据的内涵，是数据的予以解释，数据是信息存在的一种形式，只有通过解释或者处理才能成为有用的信息，数据可用不同的形式表示，而信息不会岁数据的形式而改变。

## 1.2信息安全威胁

### 信息安全的目标

保证信息尚需安全属性得到保持，不被破坏，从而对组织业务能力进行支撑。

### 信息安全的任务

保护信息资产（信息及信息系统）免收未经授权的访问使用，披露，破坏，修改，查看，记录及销毁，

## 1.3信息安全发展阶段与形式

### 信息技术（information technology IT）

1.是用于管理和处理信息所采用的的各种技术的总称。

2.主要是利用计算机科学和通信技术来设计开发安装和实施信息系统及应用软件信息处理是获取信息并对他进行变换，使之成为有用信息并发布出去的过程，主要包括信息的获取，存储，加工，发布和表示等环节。

目前，信息收集和处理已经成为人们社会工作的一个重要组成部分。

### 信息技术包括生产和应用两个方面

1.计算技术生产主要体现在信息技术产业本身，包括计算机软件，计算机硬件，设备制造，微电子电路等。

2.信息技术应用体现在信息技术的扩散上，包括信息服务，信息管理系统等。

### 微电子，通信，计算机和网络是信息系统的核心技术，其发展进程大致可分为以下四个阶段：

#### 第一阶段：电讯技术的发明

信息技术的起源可追溯到19世纪30年代，其标志性事件是电话电报的出现。

电讯技术新时代：

1835年，美国人莫尔斯发明了电报。

1837年，莫尔斯电磁式有线电报问世。

1886年，马可尼发明无线电报机。

1876年贝尔发明了电话机。

1906年，美国物理学家费森登成功研究出无线电广播。

1912年，美国Emerson公司制造出世界第一台收音机。

1935年，约翰贝德发明了世界上第一台电视机。

#### 第二阶段：计算机技术得发展

进入20世纪30年代，计算机理论与技术迅速发展，信息技术进入计算机阶段

20世纪50年末，第一代电子管计算机出现，用于军事科研信息处理

60年代中期，第二代晶体管计算机主键在民用企业中使用

60年代末，集成电路（Integrated Circuit IC）和大规模集成电路计算机接踵而至，并开始在社会普及应用。

#### 第三阶段：互联网的使用

20世纪60年代末，美国出现了第一个用于军事目的的计算机网络APPANET。APPANET的重要意义在于它使连接到网络上的计算机能够相互交流信息。

20世纪90年代，计算机网络的发展成为全球网络-因特网，网络技术和网络应用迅速发展。此外，这一阶段电话，计算机的等设备，也是实现了互联互通，信息和数据的传输更加容易。信息激素在这一阶段飞速发展，深刻的影响着人们的工作和生活方式。

#### 第四阶段：网络社会

20世纪末，以因特网为核心的信息技术进一步发展，人们的工作生活和学习越来越离不开网络，国家的经济，社会治理也与网络密不可分

告诉发展的信息网络，一方面通过显示社会投影，构成了虚拟网络社会，另一方面通过网络信息渗透，融合了各种已存在的社会实体网络，是网络社会成为了整个现实社会的结构形态，致辞，信息技术步入了一个崭新的阶段-网络社会阶段

在这一阶段，云计算，物联网和大数据技术进入人们的生活，信息和数据的保存，传输更加容易。

## 1.4信息安全保障

### 信息安全

1.信息安全一般指信息系统（包括硬件软件，数据，人。物理环境及基础设施）收到保护。不受偶然的或者恶意的原因的影响而遭到破坏，更改，泄露。系统连续可靠正常的运行，信息服务不中终端，最终实现业务的连续性。信息安全的根本目的是使信息不受内部，外部，孜然等因素的威胁。所谓信息安全就是关注信息本身的安全，而不管是否应用了计算机作为信息处理的手段。

2.在我国信息安全标准化委员会发布的GB/T 25069-2010《信息安全技术术语》中，信息安全是指保持，维持信息的保密性，完整性和可用性，也可包括真实性，可核查性，抵抗赖性和可靠性等性质。

### 信息安全的目标

保证信息上述安全属性得到保持，不被破坏，从而对组织业务运行能力提供支撑。

### 信息安全的任务

保护信息资产（信息及信息系统）免收未经授权的访问使用，披露，破坏，修改，查看，记录及销毁。

### 信息安全的属性

信息安全:1.基本属性：完整性，机密性，可用性

2.其他属性：真实性，可控性，不可否认性。

#### 从消息的层次来看，信息安全的属性有：

1.机密性：加密性也称保密性，控制信息资源的开放范围，确保信息在存储，使用，传输过程中不会泄露给非授权用户，实体和进程，或被其利用。

2.完整性：确保信息在存储，使用，传输过程中保持未经授权不能改变的特性，即对抗主动攻击，保持数据一致，防止数据被非法用户修改和破坏。

3.不可否认性：又称抵抗赖性，即建立有效的责任机制，防止用户否认其发送信息的行为和信息的内容。

#### 从网络层次来看，信息安全的属性有：

1.可用性：确保授权用户，实体和进程对信息及资源的正常使用不会被不合理拒绝，允许其可靠而及时的访问信息及资源。

2.可控性非法利用信息和信息系统

### 信息安全的特征

**相对性**

安全是性对的，动态的，没有绝对安全的系统，所以需要及时对系统安全问题进行跟踪处理，定期进行整体安全评估，及时发现问题把那个加以解决。

**时效性**

安全不能一劳永逸，需要根据安全风险，及时制定应对策略。

**相关性**

在更改配置等操作时，需要对系统重新进行评估和同步更新安全措施。

**不确定性**

攻击发起的事件，地点，攻击者和攻击目标都具有不确定性，在制定安全应对措施时，要尽量可能考量所有潜在安全威胁。

**复杂性：**

信息安全是意向系统工程，设计到安全管理，教育，培训，立法，国际合作等领域。

#### 与传统信息安全相比，信息安全具有4个鲜明特征：

**系统性：**

系统的从技术上，管理，工程和标准法规等各层面综合保护信息安全

**动态性：**

对信息安全不能抱着一劳永逸的思想，应该根据风险的变化，在信息系统的整个生命周期中采用相应的安全措施来控制风险**。**

**无边界性：**

信息系统安全威胁超越了显示低于和现实行业的限制

**非传统性：**

与军事安全，政治安全等传统安全相比，信息安全设计的领域和硬性范围十分广泛。

### 信息系统安全

#### 数据安全

数据的秘密性

数据的真实性

数据的完整性

IBM公司的定义：采取措施保护数据免收未经授权的泄露，篡改和毁坏。

#### 设备安全

1.信息设别的安全是信息系统安全的首要问题：

2.设备的稳定性，设备的可靠性，设别的可用性。

设备：硬设备，软设备。

#### 内容安全

内容安全是信息安全在法律，政治，道德层次上的要求：政治上健康，符合国家法律法规，符合中华民族盗的规范。

#### 行为安全

行为安全是信息安全的终极目的：

行为的秘密性

行为的完整性

行为的可控性

符合哲学上，事件是检验真理的唯一标准

#### 从受威胁的队形，可以将我国面临的信息安全威胁分为3类：

国际威胁：

一是恐怖组织通过网络大肆发布恐怖信息，渲染暴力活动费。

二是邪教组织通过网络极力宣传种族歧视等

三是西岗实例通过网络宣传他们的意思，价值观生活方式，进行文化渗透，侵略。

四是其他国家国家情报机构手机我国政治，军事，经济等情报信息

组织威胁：

主要针对企业或者组织受保护的财产。专有技术。

具体表现为：网络恐怖分子破坏公共秩序，制造社会混乱等，通过工业间谍掠夺竞争优势，打击竞争剁手，是企业或者组织蒙受或者声誉损失

个人威胁：

一是对知识产权的威胁

二是侵犯，破坏个人计算机系统中的信息，通过互联网对财产进行侵犯，对E-mail系统进行破坏，硬性人们的工作，学习和生活。

## 1.5信息系统安全保障

### 信息系统安全问题产生的根本原因：

内因：系统自身的脆弱性

外因：人为威胁，环境威胁：

### 安全问题根源-内因外因示例

内因：

复杂性导致脆弱性

凡是人做的东西总会存在问题

外因：

国家威胁（信息战士，情报机构）

组织威胁（恐怖分子，商业间谍，犯罪团伙）

局部威胁（社会性黑客，娱乐性黑客）

来自大自然的威胁：雷电，地震，火灾洪水等自然灾害，电力，空调等呗电磁脉冲破坏，信息系统机房和设备遭到破坏。

### 通信安全 COMSEC

20世纪40-70年代

核心思想：通过密码技术解决通信保密，保证数据的保密性和完整性，主要关注传输过程中的数据保护。

安全威胁：搭线窃听，密码学分析

安全措施：加密

### 计算机安全COMPUSEC

20世纪70-90年代

核心思想：确保信息系统的保密性，完整性和可用性

安全威胁：非法访问，恶意代码，脆弱口令

安全措施：安全操作系统设计技术

### 信息系统安全 INFOSEC

20世纪90年代后

核心思想：确保信息在存储，处理和传输过程中免收偶然或者恶意的泄密，非法访问或者破坏。

安全威胁：网络侵入，病毒破坏，信息对抗等

安全措施：防火请，防病毒，漏洞扫描，入侵检测，PKI,VPN等

### 信息安全保障 IA

今天

核心思想：动态安全保障信息系统的业务正常，稳定的运行。综合技术，管理，过程，人员。

安全威胁：黑客，恐怖分子，信息战，自然灾害，电力中断等。

安全措施，技术安全保障体系，安全管理体系，人员意识、培训、教育。

### 我国信息安全形势

我国信息安全环境日趋复杂，网络安全问题对互联网的健康发展带来日益严峻的挑战，网络安全事件的应行李和破坏程度不断扩大。

针对网络信息的破坏活动日益严重，利用网络进行违法犯罪案件逐年提升。

安全漏洞和安全隐患增多，对信息安全构成严重威胁。

黑客攻击，恶意代码对重要信息系统安全造成严重影响。

# 2信息安全基础技术

## 2.1密码学

### **威胁、安全属性与密码学技术**

#### 面临的攻击威胁：

截获(泄露信息)，篡改(修改信息)，伪造(伪造信息来源)否认(事后否认发送信性息和行为)   
所破坏的信息安全属性：

完整性， 真实性，不可否认性  
解决问题所采用的密码学技术：

对称密码和非对称密码，哈希函数、数字签名、对称密码和非对称密码，数字签名，数字签名

### 密码学发展

第一个阶段是从古代到19世纪末一一古典密码

第二个阶段从20世纪初到1949年一一近代密码

第三个阶段从C.E.Shannon( 香农) 于1949年发表的划时代论文“The Communication Theory Quaatem of Secret Systems" 开始一一现代密码

第四个阶段从1976年W.Diffie和M.Hellman发表论文“New Directions in Cryptography" 开始一一公钥密码

### 近代密码学

20世纪初到1949年

主要标志是机械密码/机电密码，用机电代替手工。

近代密码体制是用机械或电动机械实现的，最著名的就是转轮机(Rotor Machine )。

古典密码学  
古典密码体制的安全性在于保持算法本身的保密性，受到算法限制。  
不适合大规模生产不适合较大的或者人员变动较大的组织用户无法了解算法的安全性

### 现代密码学

1949~ 1975年:1949年，Shannon的论文“The Communication Theory of Secret Systems".

1967年，David Kahn 的专著《The Code breakers》

Shannon 1971年~ 1973年，IBM Watson实验室的Horst Feistel

等人发表的几篇技术报告。

1974年，IBM提交了算法LUCIFER，后来成为了DES。

\*新特点: 数据的安全基于密钥而不是算法的保密。

加密与解密  
明文(Plaintext): 原始消息，被隐蔽消息，未经加密的消息。  
密文(Ciphertext)或密报(Cryptogram): 明文经密码变换而成的一种隐蔽形式。  
.加密员或密码员(Cryptographer): 对明文进行加密操作的人员。

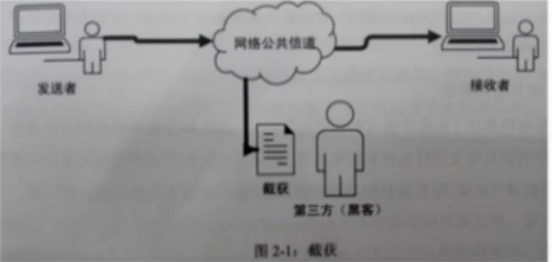
截获是指一个非授权方介入系统，窃听传输的信息，导致信息泄露。它破

坏了信息的保密性。

非授权方可以是一个人，也可以是一个程序。

截获攻击主要包括:通过嗅探和监听等手段截获信息，从而推测出有用信息，

如用户口令、账号，文件或程序的不正当复制等。

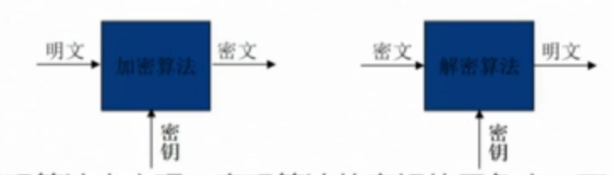


### 加密与解密

加密( Encryption) :将明文变换为密文的过程。把可懂的语言变换成(人类/机器) 不可懂的语言。

解密( Decryption) :由密文恢复出原明文的过程。加密的逆过程即把不可懂的语言变换成可懂的语言。

加密可以采用密码算法来实现，密码算法从密钥使用角度，可分为对称密码算法和非对称密码算法。



### 转轮机

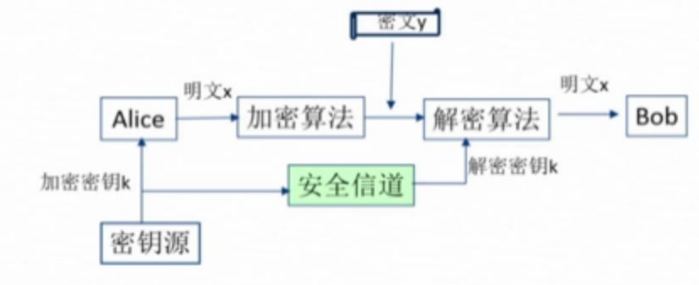
转轮密码机ENIGMA,由ArthurScherbius于1919年发明。在二次世界大战期间，Enigma曾作为德国陆、海、空三军最高级密码机。

英国的TYPEX打字密码机

德3轮ENIGMA的改进型

在英国通信中使用广泛，且在破译密钥后帮助破解德国信号

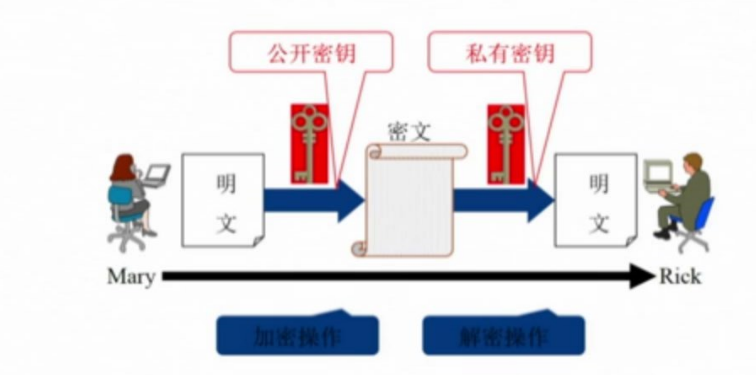
公钥密码学  
\*1976年以后:  
1976年，Diffie & Hellman的“New Directions in Cryptography”提出了非对称密钥密码。  
1977年，Rivest,Shamir & Adleman提出了RSA公钥算法。  
90年代，逐步出现椭圆曲线等其他公钥算法。  
公钥密码使得发送端和接收端无密钥传输的保密通信成为可能!

对称密码算法  
对称密码算法(也称单钥或私钥密码算法) :加密密钥和解密密钥相同，  
或实质上等同，即从一个易于推出另一个。  
DES、3DES、IDEA、AES  
密钥相对较短，一般采用128，192或256 比特  


对称密码算算法的优缺点  
优点:  
效率高，算法简单，系统开销小  
适合加密大量数据  
明文长度与密文长度相等  
缺点:  
需要以安全方式进行密钥交换

密钥管理复杂  
无法解决消息的篡改、否认等问题

### 非对称加密与解密



非对称密码算法  
  
非对称密码算法: 加密密钥和解密密钥不同，从一个很难推出另一个。其中，  
对外公开的密钥，称为公开密钥( public key),简称公钥; 必须保密的密钥，称为私有密钥( private key),简称私钥。又叫公钥密码算法( Public-keycipher)。  
一RSA、ECC、EIGamal  
\*公钥加密私钥解密  
.私钥加密公钥解密  
\*密钥长度512- 2048位

### 非对称密码学特点

1.优势

密钥分发数目与参与者数目相同

在有大量参与者的情况下易于密钥管理

安全

支持数字签名和不可否认性

无需事先与对方建立关系，交换密钥

2.缺点

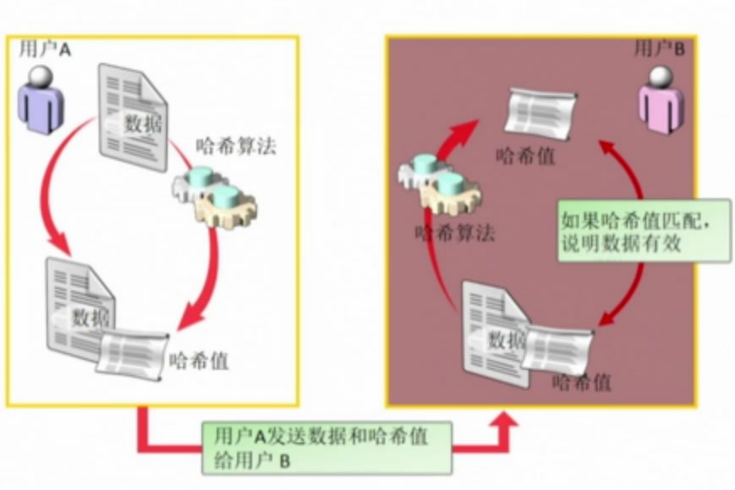
速度相对较慢

可能比同等强度的对称密码算法慢10倍到100倍

加密后，密文变长

哈希函数  
对称密码和非对称密码算法主要解决信息的机密性问题，而实际系统和网络还可能受到消息篡改等攻击。  
篡改攻击主要包括:修改信息内容，改变程序使其不能正确运行等。哈希函数可以用来保证信息的完整性。  
哈希(Hash) 函数(也称为杂凑函数或单向散列函数)接受一个消息作为输入，产生一个称为哈希值的输出。输出的哈希值也可称为散列值、消息摘要(Message Digest,MD)

### 哈希运算-完整性



### MD5算法

MD5 (RFC 1321) developed by Ron Rivest (“R”of the RSA )at MIT in 90's.

MD: 消息摘要Message Digest,

输入: 任意长度的消息

输出: 128位消息摘要

处理: 以512位输入数据块为单位

SHA-1算法  
SHA( Secure Hash Algorithm,安全哈希算法) 由美国国家标准技术研究所开发，1993 年作为联邦信息处理标准发布，2008 年又有更新。  
\*输入: 最大长度为264位的消息;  
\*输出: 160位消息摘要;  
处理: 输入以512位数据块为单位处理.  
比较SHA1/ MD5

散列值长度

SHA1160bits MD5 128bits

安全性

SHA1算法被视为MD5的替代候选算法

速度

SHA1慢些(openssl speed md5/sha1)

- type| 16 bytes 256 bytes 1024 bytes 8192 bytes 64 bytes

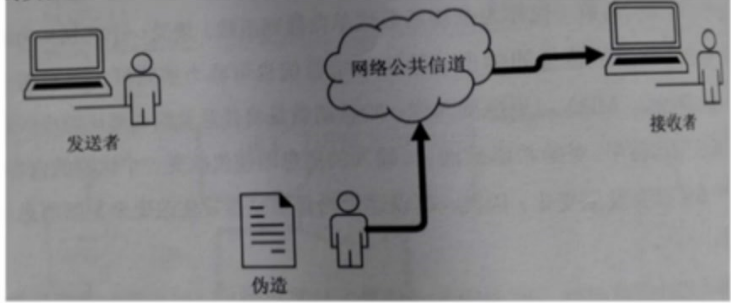
-md5|5425.31k 19457.48k 55891.45k 104857.60k 143211.40k

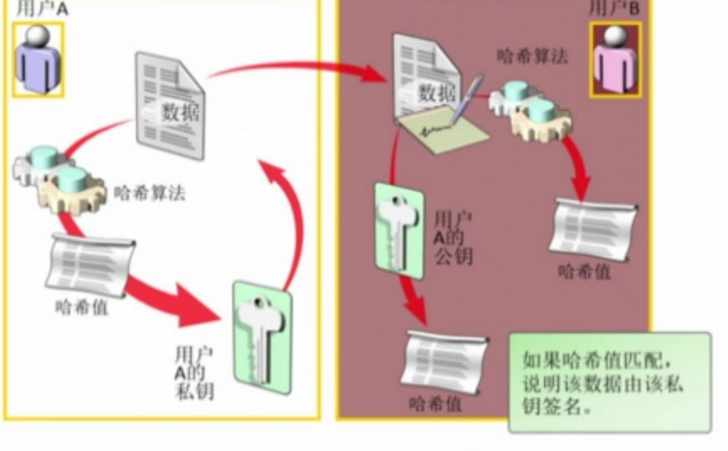
sha1| 5104.58k16008.41k 37925.33k57421.81k 68241.68k

### 数字签名

除了保护信息的机密性和完整性，密码学技术也可以

解决信息的可鉴别性(真实性或认证性)和不可否认性。

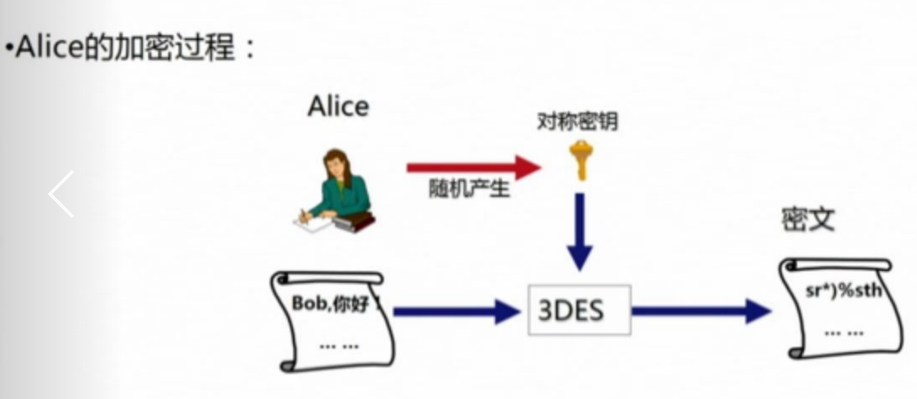


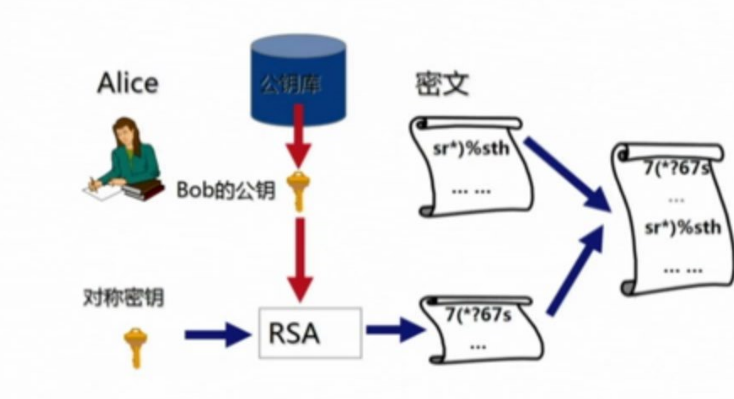


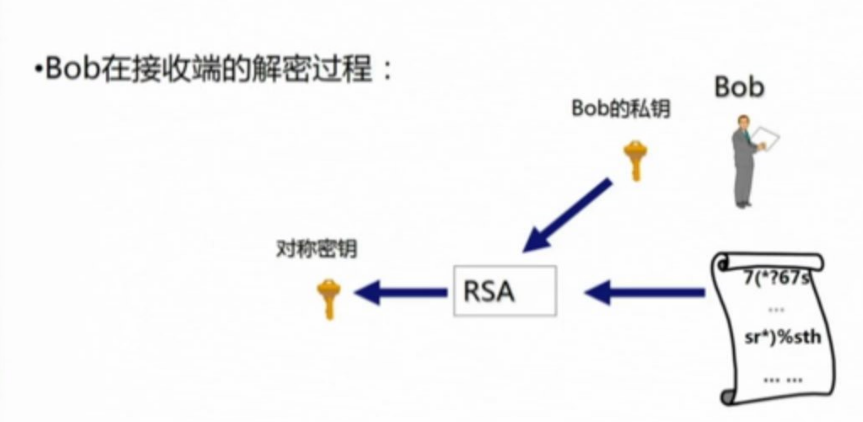
数字签名  
传统签名的基本特点:  
能与被签的文件在物理上不可分割  
签名者不能否认自己的签名  
签名不能被伪造  
容易被验证  
数字签名是传统签名的数字化，基本要求:  
能与所签文件“绑定”  
签名者不能否认自己的签名  
签名不能被伪造  
容易被验证

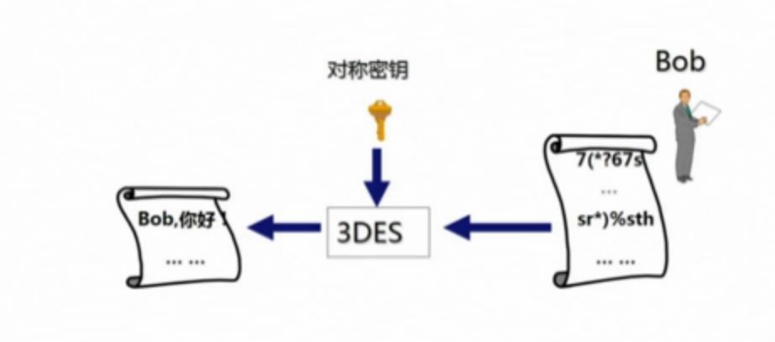
数字签名的应用  
(1) 可信性:签名让文件的接收者相信签名者是慎重地在文件上签名的。  
(2) 不可重用性:签名不可重用，即使同一消息在不同时刻的签名也是  
有区别的。如果将签名部分提取出来，附加在别的消息后面，验证  
签名会失败。这是因为签名和所签名消息之间是一一对应的，消息  
不同签名内容也不同，因此签名无法重复使用。  
(3) 数据完整性:在文件签名后，文件不能改变。  
(4) 不可伪造性:签名能够证明是签名者而不是其他人在文件上签名，  
任何人都不能伪造签名。  
(5) 不可否认性:在签名者否认自己的签名时，签名接收者可以请求可  
信第二方进行仲裁。

混合加密









## 2.2数字证书与公钥基础设施

数字证书  
绑定用户身份和公钥  
网络世界的电子身份证，与现实世界的身份证类似，能够证明个人、团体或设备的身份。  
包含相关信息:  
包含姓名、地址、公司、电话号码、Email地址、...与身份证上的姓名、地址等类似包含所有者的公钥  
拥有者拥有证书公钥对应的私钥  
由可信的颁发机构颁发：比如身份证由公安局颁发一样  
颁发机构对证书进行签名，与身份证上公安局的盖章类似，可以由颁发机构证明证书是否有效，可防止擅改证书上的任何资料  
公钥基础设施

PKI: Public Key Infrastructure 公钥基础设施

利用公开密钥技术建立的提供信息安全服务的在线基础设施。它利用加密、数字签名、数字证书来保护应用、通信或事务处理的安全。

是一个包括硬件、软件、人员、策略和规程的集合，用来实现基于公钥密码体制的密钥和数字证书的产生、管理、存储、分发和撤销等功能。

如同电力基础设施为家用电器提供电力一样，PKI为各种应用提供安全保障，提供网络信任基础。

CA :认证权威机构  
CA 专门负责数字证书的产生、发放和管理，以保证数字证书  
真实可靠。它是公钥基础设施PKI 的核心，CA 负责管理P阳  
结构下的所有用户(包括各种应用程序)证书，把用户的公钥和  
用户的其他信息捆绑在一起，在网上验证用户的身份。  
  
CA数字证书的发放机构，其主要功能包括:  
-签发数字证书  
签发证书  
更新证书  
一管理数字证书  
撤销、查询  
审计、统计  
-验证数字证书：黑名单认证( CRL )  
-RA 的设立、审查及管理

### RA:证书注册机构

-证书注册权威

Registration Authority

-受理用户的数字证书申请

对证书申请者身份进行审核并提交CA制证

类似于申请身份证的派出所

-提供证书生命期的维护工作

受理用户证书申请

协助颁发用户证书

审核用户真实身份

受理证书更新请求

受理证书吊销

### 目录服务(LDAP )

证书的存储库，提供了证书的保存、修改、删除和获取的能力CA采用LDAP标准的目录服务存放证书，其作用与数据库相同，优点是在修改操作少的情况下，对于访问的效率比传统数据库要高

CRL  
.CRL (Certificate Revocation List):证书撤销列表，也称“证书黑名单”  
--在证书的有效期期间，因为某种原因(如人员调动、私钥泄漏等等),导致相应的数字证书内容不再是真实可信，此时，进行证书撤销，说明该证书已是无效  
.CRL中列出了被撤销的证书序列号



## 2.3身份认证

身份认证基本方法  
身份认证是用户登录系统或网站面对的第一道安全防线，如输入账号口令来登录。身份认证是在网络中确认操作者身份的过程。  
身份认证一般依据以下三种基本情况或这三种情况的组合来鉴别用户身份。  
(1)用户所知道的东西，例如口令、密钥等;

（2) 用户拥有的东西，例如印章、U 盾(USB Key) 等;  
(3) 用户所具有的生物特征:例如指纹、声音、虹膜、人脸等。

### 动态口令认证

\*动态口令

又称一次性口令(One Time Password,OTP )

一口令动态性-- 每次变化，无须人工干预

- 口令随机性-- 随机性强，难以猜测

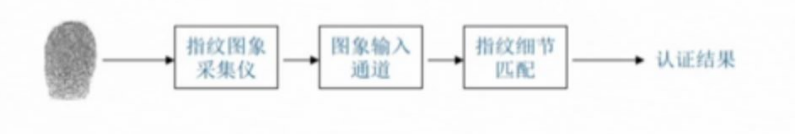
短信口令认证  
是利用移动网络动态口令的认证方式。短信口令验证以手机短信形式请求包含6 位随机数的动态口令，身份认证系统以短信形式发送随机的6 位动态口令到用户的手机上，用户在认证时输入此动态口令即可.由于手机与用户绑定比较紧密，短信口令生成与使用场景是物理隔绝的，因此口令在通路上被截取几率较低。

静态口令认证  
（1)根据”用户所知”进行认证的方法有:静态口令认证、  
短信口令认证和动态口令认证等。

静态口令  
口令固定不变，并且长期有效  
弱鉴别(weak authentication)

静态口令认证缺点  
通信窃取一窃听获得明文的用户名和口令。重放攻击一截获登录数据(明/密)，重放攻击  
字典攻击一选择有意义的单词或数字作字典  
暴力攻击一穷举全部可能组合猜测口令  
外部泄漏一搜索存有口令的纸片或文件  
窥探一安装监视器或从背后窥探  
社交工程一冒充合法用户、假冒管理员，骗取口令。

U 盾(USB Key)  
(2) 根据"用户所有"进行认证的方法有:U 盾(USB Key)、电子印章等。  
USB Key 认证:基于USB Key 的认证方法是近几年发展起来的一种方便、安全的身份认证技术。它采用软硬件相结合的挑战/应答认证模式。USB Key 是一种USB 接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用USB Key 内置的密码算法实现对用户身份的认证。挑战/应答认证模式，即认证系统发送一个随机数(挑战)，用户使用USB Key 中的密钥和算法计算出一个数值(应答)，认证系统对该数值进行检验，若正确则认为是合法用户。  
基于生物特征的身份认证(一)  
每个人所具有的唯一生理特征  
 --指纹，视网膜，声音，虹膜、语音、面部、签名等  
指纹  
-一些曲线和分又以及一些非常微小的特征  
 提取指纹中的一些特征并且存储这些特征信息: 节省资源，快速查询  
手掌、手型  
--手掌有折痕，起皱，还有凹槽  
--还包括每个手指的指纹  
一人手的形状(手的长度，宽度和手指)表示了手的几何特征

基于生物特征的身份认证(二)  
\*视网膜扫描  
扫描眼球后方的视网膜上面的血管的图案;  
。虹膜扫描  
虹膜是眼睛中位于瞳孔周围的一圈彩色的部分  
虹膜有其独有的图案，分叉，颜色，环状，光环以及皱褶  
\*语音识别  
记录时说几个不同的单词，然后识别系统将这些单词混杂在一  
起，让他再次读出给出的一系列单词  
\*面部扫描  
- 人都有不同的骨骼结构，鼻梁，眼眶，额头和下颚形状  
指纹识别的实现原理  
\*通过特殊的光电扫描和计算机图像处理技术，对指纹进行  
采集、分析和比对，自动、迅速、准确地认证出个人身份。  
。指纹识别的过程  
按照用户和姓名等信息将其存在指纹数据库中的模板  
指纹调出来，然后再用用户输入的指纹与该模板的指  
纹相匹配，以确定这两幅指纹是否出于同一幅指纹。  


虹膜识别的实现原理  
\*虹膜是环绕在瞳孔四周有色彩的部分  
 --每一个虹膜都包含一个独一无二的基于像冠、水晶体，细丝、斑点、结构。凹点、射线、皱纹和条纹体、等特征的结构  
--每一个人的虹膜各不相同，一个人的左眼和右眼就可能不一样，即使是双胞胎的虹膜也可能不一样  
--人的虹膜在出生后6-18个月成型后终生不再发生变化  
其他身份认证技术  
.单点登录( SSO,Single Sign-on )  
用户只需在登录时进行一次注册，就可以访问多个系统，不必重复输入用户名和密码来确定身份  
\*Kerberos提供了一个网络环境下的身份认证框架结构  
--实现采用对称密钥加密技术  
--公开发布的Kerberos版本包括版本4和版本5  
- 安全性、可靠性、可伸缩性、透明性

远程用户拨号认证系统( Remote Authentication Dial In User Service )RADIUS是一种C/S结构的协议，它的客户端最初就是NAS( Net Access Server) 服务器，现在任何运行RADIUS客户端软件的计算机都可以成为RADIUS的客户端

--基本设计组件有认证、授权和记账(AAA)

--简单明确，可扩充

使用UDP端口1812,1813

## 2.4访问控制

访问控制的概念和目标  
访问控制:针对越权使用资源的防御措施  
目标：防止对任何资源(如计算资源，通信资源或信息资源)进行未授权的访问，从而使资源在授权范围内使用，决定用户能做什么,也决定代表一定用户利益的程序能做什么。

访问控制的作用  
未授权访问: 包括未经授权的使用、泄露、修改、  
销毁信息以及颁发指令等。  
 --非法用户对系统资源的使用  
 --合法用户对系统资源的非法使用  
作用:机密性、完整性和可用性  
主体与客体

主体

发起者，是一个主动的实体，可以操作被动实体的相关信息或数据

--用户、程序、进程等

客体

一种被动实体，被操作的对象，规定需要保护的资源

--文件、存储介质、程序、进程等

主体: 接收客体相关信息和数据，也可能改变客体相关信息一个主体为了完成任务，可以创建另外的主体，这些子主体可以在网络上不同的计算机上运行，并由父主体控制它们  
客体: 始终是提供、驻留信息或数据的实体主体和客体的关系是相对的，角色可以互换  
控制策略  
是主体对客体的相关访问规则集合，即属性集合。访问策略体现了  
一种授权行为，也是客体对主体某些操作行为的默认。  
访问控制是主体依据某些控制策略或访问权限，对客体本身或其资源赋予不同访问权限的能力，从而保障数据资源在合法范围内得以有效使用和管理。  
访问控制安全策略实施遵循最小特权原则。在主体执行操作时，按照主体所需权利的最小化原则分配给主体权力。最大限度地限制主体实施授权行为，避免突发事件、操作错误和未授权主体等意外情况可能给系统造成的危险。

授权  
规定主体可以对客体执行的操作:  
读，写，执行，拒绝访问  
自主访问控制  
自主访问控制(Discretionary Access Control.DAC) 是一种广泛应用的访问控制方法。采用这种方法，资源的所有者(往往也是创建者)可以规定谁有权访问他们的资源，用户(或用户进程)可以选择与其他用户共享资源。

访问控制矩阵  
矩阵元素: 规定了相应用户对应于相应的文件被准予的访问许可、访问权限



自主访问控制的特点  
优点:  
--根据主体的身份和访问权限进行决策  
--具有某种访问能力的主体能够自主地将访问权的某个子集授予其它主体  
--灵活性高，被大量采用  
缺点:  
---信息在传递过程中其访问权限关系会被改变

强制访问控制的含义  
强制访问控制(Mandatory Access Con往01,MAC) 是指主体和客体都有一个固定的安全属性，系统用该安全属性来决定一个主体是否可以访问某个客体。如果系统认为具有某一个安全属性的主体不适合访问某个客体，那么任何其他主体都无法使该主体具有访问该客体的权利。

--主体和客体分配有一个安全属性  
--应用于军事等安全要求较高的系统  
--可与自主访问控制结合使用

自主访问控制与强制访问控制的比较  
--自主访问控制  
 细粒度  
 灵活性高  
 配置效率低  
--强制访问控制  
 控制粒度大  
 灵活性不高  
 安全性强

### 基于角色的访问空制(RBAC)

--RBAC的基本思想是根据用户所担任的角色来决定用户在系统中的访问权限。

--一个用户必须扮演某种角色，而且还必须激活这一角色，才能对一个对象进行访问或执行某种操作。



RBAC模型的特点

--便于授权管理(角色的变动远远低于个体的变动)

--便于处理工作分级，如文件等资源分级管理

--利用安全约束，容易实现各种安全策略，如最小特权、职责分离等

--便于任务分担，不同角色完成不同的任务

## 2.5安全审计

安全审计  
\*即便是采取了很多方法来保障计算机或网络安全，但仍然不可避免系  
统感染病毒或数据安全受到威胁。受到威胁后，如何从安全事故中恢复  
过来，使系统尽快运作起来，需要预先采取一些措施。安全审计是提高  
安全性的重要工具，它能够再现问题，以帮助事后的责任追查和数据恢  
复等。  
\*审计技术的出现早于计算机技术，它按照时间顺序产生、记录系统事  
件，并对其进行检查。安全审计可以跟踪和监测系统中的异常事件，也  
可以监视系统中其他安全机制的运行情况。

\*计算机安全审计(Audit) 是指按照一定的安全策略，记录历史操作事件，

并利用记录进行分析，发现系统漏洞、入侵行为等，并改善系统性能和

安全性的一系列过程。安全审计是对访问控制的必要补充，它会对用户

使用何种信息资源、使用的时间，以及如何使用(执行何种操作)进行记

录与监控。通过对系统和用户进行充分和适当的审计，能够分析发现安

全事件的原因，并提供相应的证据。

### 日志

是安全审计系统的主要组成部分。为了维护自身系统资源的运行状

况，计算机系统一般都会有相应的日志系统，记录有关日常事件或者误

操作警报的日期及时间。

\*受到可疑攻击或安全威胁后，可以通过查看事件安全日志来确认可疑或

恶意的行为。例如，通过查看事件日志，发现非工作时间某个用户成功

登录账户，则可能有人窃取了账号和口令:日志中有多次登录失败的记录，

则可能有攻击者尝试进入系统。

### 安全审计方式

安全审计可以分成被动式审计、主动式审计两种。

被动式审计就是简单地记录一些活动，并不做处理。

主动式审计一般包括:结束一个登录会话、拒绝一些主机的访问

(包括WEB 站点，FTP (File Transfer Protocol,文件传输协

议)服务器和电子邮件服务器)、跟踪非法活动的源位置等行为。  
安全审计的作用主要包括以下四个方面。  
(1)威慑和警告潜在的攻击者和滥用授权的合法用户。如果系统使用者知道他们的行为活动被记录在审计日志中，相应人员需要为自己的行为负责，他们就会审慎自己的行为，不太会违反安全策略和绕过安全控制措施。  
(2)提供有价值的系统使用日志，帮助系统管理员及时发现系统入侵行为或潜在的系统漏洞。对审计的每一次记录进行分析，可实时发现或预防、检测入侵活动。实时入侵检测审计能及时发现非法授权者对系统的访问，也可以探测到病毒活动和网络攻击。

(3)在发生故障后，可以帮助评估故障损失、重建事件和数据恢复。通过审查系统活动，可以比较容易地评估故障损失，确定故障发生的时间、原因和过程。通过对审计日志进行分析可以帮助重建系统或事件，也能协助恢复数据文件。同时，还有助于避免再次发生此类故障。

(4) 对系统控制、安全策略与规程中特定的改变做出评价和反馈，便于修订决策和部署。

# 3.网络安全防护技术

## 3.1网络基础知识

### TCPAIP协议

### Internet和TCP/IP协议:

因特网(Intemet )通过TCP/P协议将遍布在全世界各地的计算机互联，从而形成超级计算机网络。

### 何为协议?

1.协议其实是一种约定。

2.大家预先约定好规则，之后都按照这同一个规则执行。

3.就像多家公司合作，一开始要签协议似的。

### 何为协议? 续

1.网络中的协议( Protocol),是指实现约定或定义的一组通信规则。

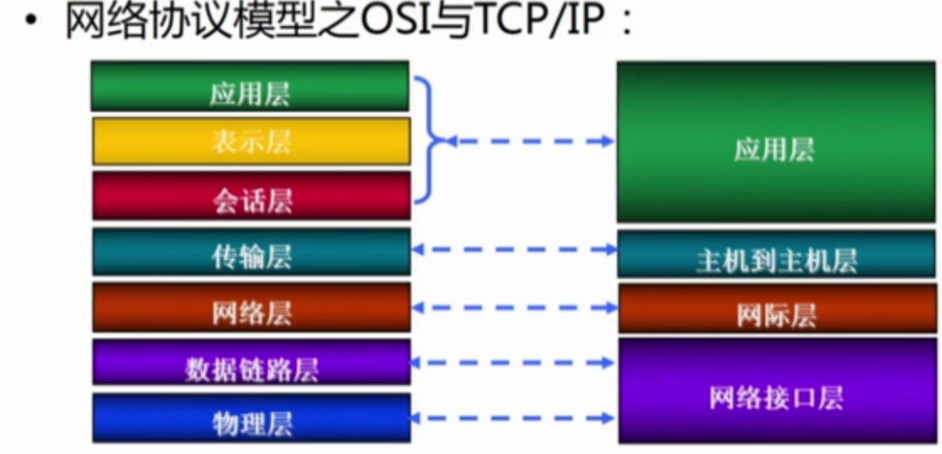
2.它精确地规定了所交换数据的格式和传输方法。

3.不同网络必须遵守统一的协议才能相互通信。

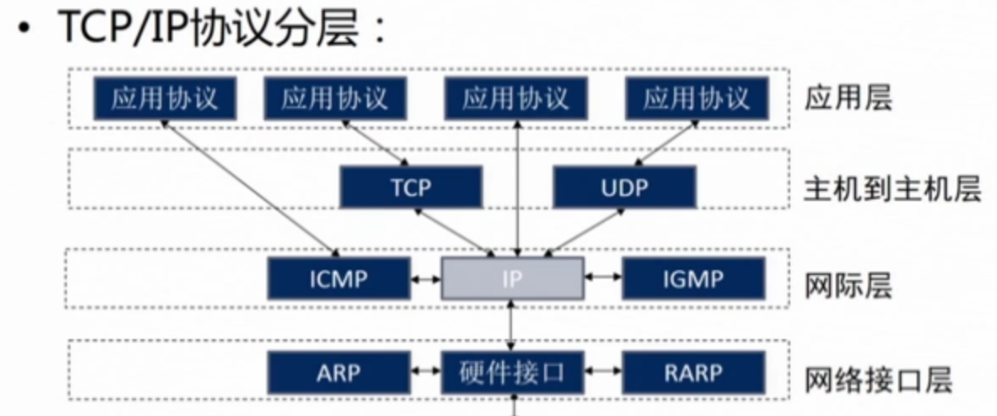
4.TCP/IP是一组不同层次上的多个协议组合。

5.其定义了电子设备如何接入互联网，以及数据如何在他们之间传输。

### 网络协议模型之OSI与TCP/IP :



### TCP/IP协议分层：



### 通信地址:

1.通信其实就是将数据从一端传送到另一端的过程。这有点像发快递。

2.发快递需要知道寄出地址和寄到地址。

3.在网络中，寄出地址为源地址，寄到地址为目的地址。



### 网络中的通信地址:

1.通信中，每台计算机还必须有一个全球唯一的物理地址。

2.这个地址工作在网络接口层被称为MAC(48bit).

1.通信中，每台计算机还必须有一个逻辑地址。

2.这个地址工作在IP层被称为IP地址(32bit )。

### IP地址分类:

1.咱们刚刚看到的IP地址叫做IPv4,还有另外一种叫做IPV6。

2.目前IPV4地址已经不够用了。而且，IPv6地址比IPV4地址多。

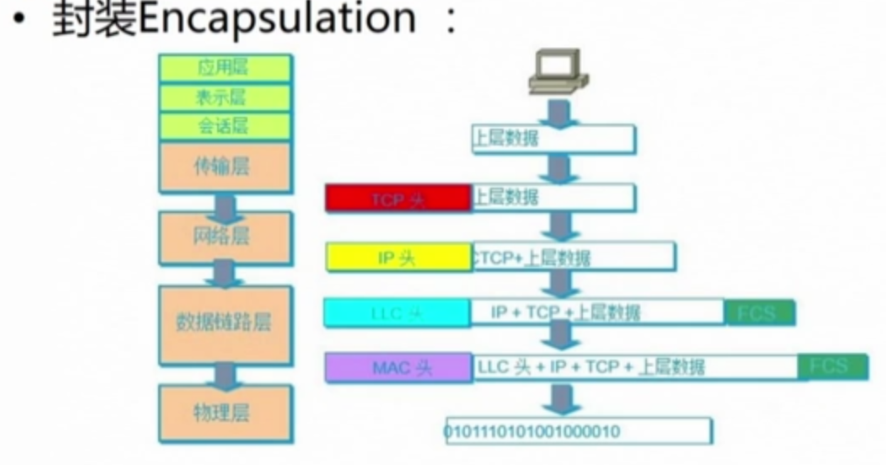
3.以后有可能会启用IPV6.

4.虽然有4和6之分，但是它们都属于TCP/IP地址族。  
IP地址分类: 续  
1.目前被大量使用的地址是IPV4地址。  
2.IPV6地址是由IET F设计的下一代IP协议。  
3.IPV6不仅可以解决IPV4地址被耗尽的问题。  
4.还可以提高IP协议本身的性能和安全性。  
注:  
ETF (Internet Engineering Task Force )互联网工程任务组

### 封装Encapsulation :

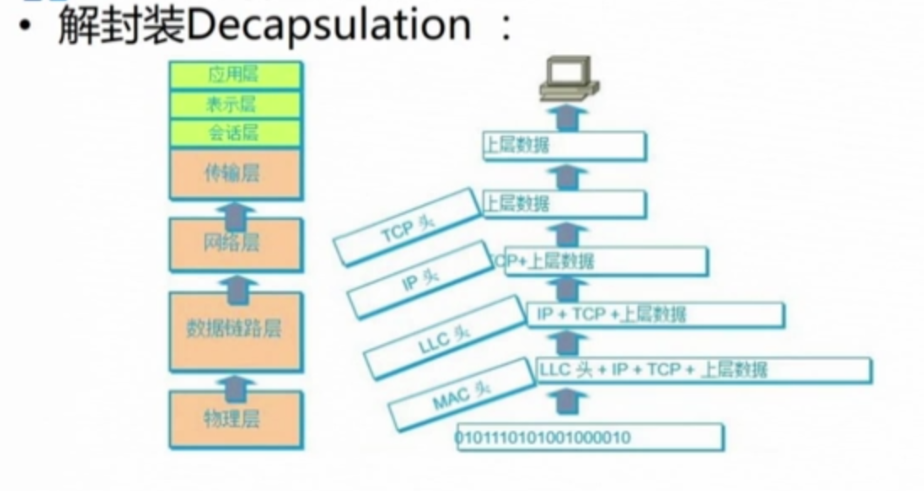
1.当高层进程要进行数据传输时，会先将数据从高层向低层传送。

2.经过低层时，会分别加上该低层的头部信息置于数据首部。

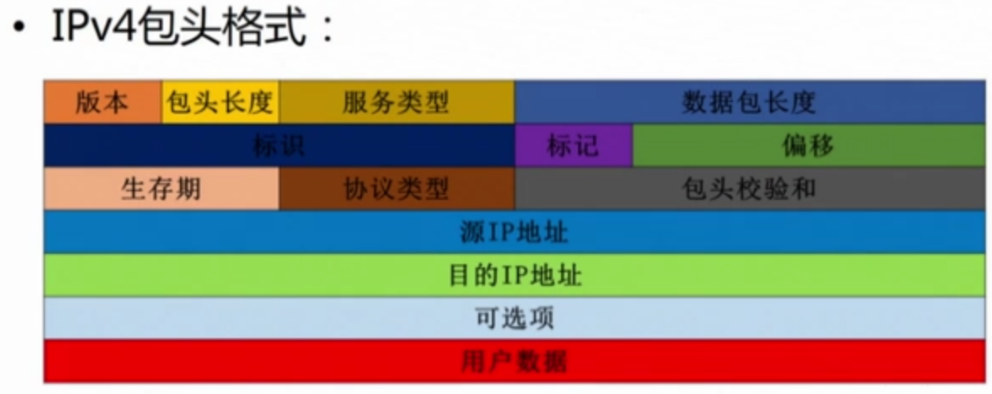


### 解封装Decapsulation :

1. 执行封装的逆过程。



### IPv4报头格式：



### IPV4包头格式: 续

1.版本：IPv4版本

2.包头长度: IPV4包头长度

3.服务类型: 针对该IPV4数据包定义转发优先级

4.数据包长度: IPV4数据包总长度= IPv4包头长度+IPv4用户数据长度

5.标识: 分片重组时保持统一

6.标记: 第二bit置1,表示不能分片; 第三bit置1,表示最后一片。

7.偏移: 分片重组时还原原始数据位置

8.生存期: 每经过一跳此数值减1,避免数据平面环路导致的无限转发

9.协议类型: 表示上层协议类型

10.包头校验和: 用于校验IPV4包头的正确性

11.原IP地址: 发送方的IPV4地址

12.目的IP地址: 接收方的IPV4地址

13.可选项: 用于表示对IPV4数据包进行一些特殊处理的信息

14.用户数据: IPV4头部上层负载的全部数据

### 端口port :

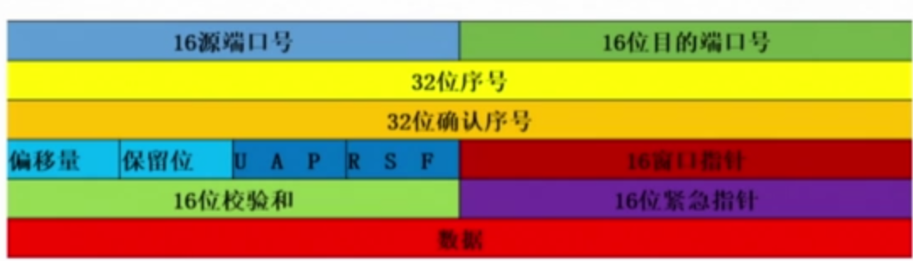
1.计算机中有一些协议常用端口,这些端口绑定了一些服务且明确表示使用某种服务协议。如80端口表示HTTP协议。

2.黑客攻击常将各种协议端口作为入侵通道。端口通过端口号标记，范围是0~6553

### 传输控制协议TCP :

1.提供面向连接的、可靠的字节流服务

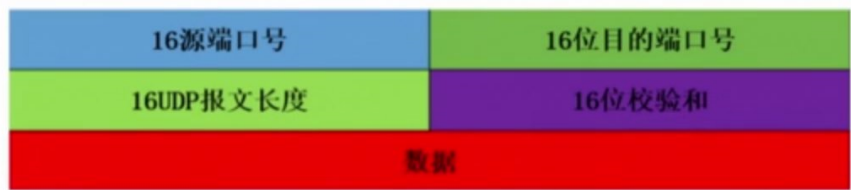
2.提供可靠性服务



### 用户数据报协议U DP :

1.用户数据报协议: 提供面向事务的简单不可靠信息传送服务

2.无连接、不可靠。协议简单、占用资源少，效率高



### 万维网( World Wide Web,WWW )

是因特网上使用最广泛的一种信息服务，是因特网的主要组成部分。用户可

以通过客户端程序(一般是浏览器)访问服务器端程序提供的页面。

### 超文本标记语言HTML

1.超文本标记语言HTML是一种制作万维网页面的标准语言，为不同的计算

机交换信息资源提供了统一的格式。

2.超文本标记语言将各种不同格式的对象(比如文本、图像、音频和视频)

组织在一个一个的网页中，HTML文件后缀为html或htm。

### 超文本传输协议HTTP

1.是用于从WWW服务器传输超文本到本地浏览器的传输协议。它可以使浏览器更加高效，使网络传输减少。

2.它不仅保证计算机正确快速地传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示(如文本先于图形)等。

### 统一资源定位符URL

1.用户在访问网站时，为了获取特定的信息资源，需要给出特定资源的地址，即统一资源定位符( Uniform Resource Locator,URL)。它是用来标识万维网中每个信息资源的地址。

2.URL由三部分组成，表示形式为:http://主机域名或IP地址[:端口号1/文件路径/文件名

## 3.2网络安全威胁

## 3.3网络安全防护与实践

## 3.4无线局域网安全防护