希赛

系统安全分析与设计

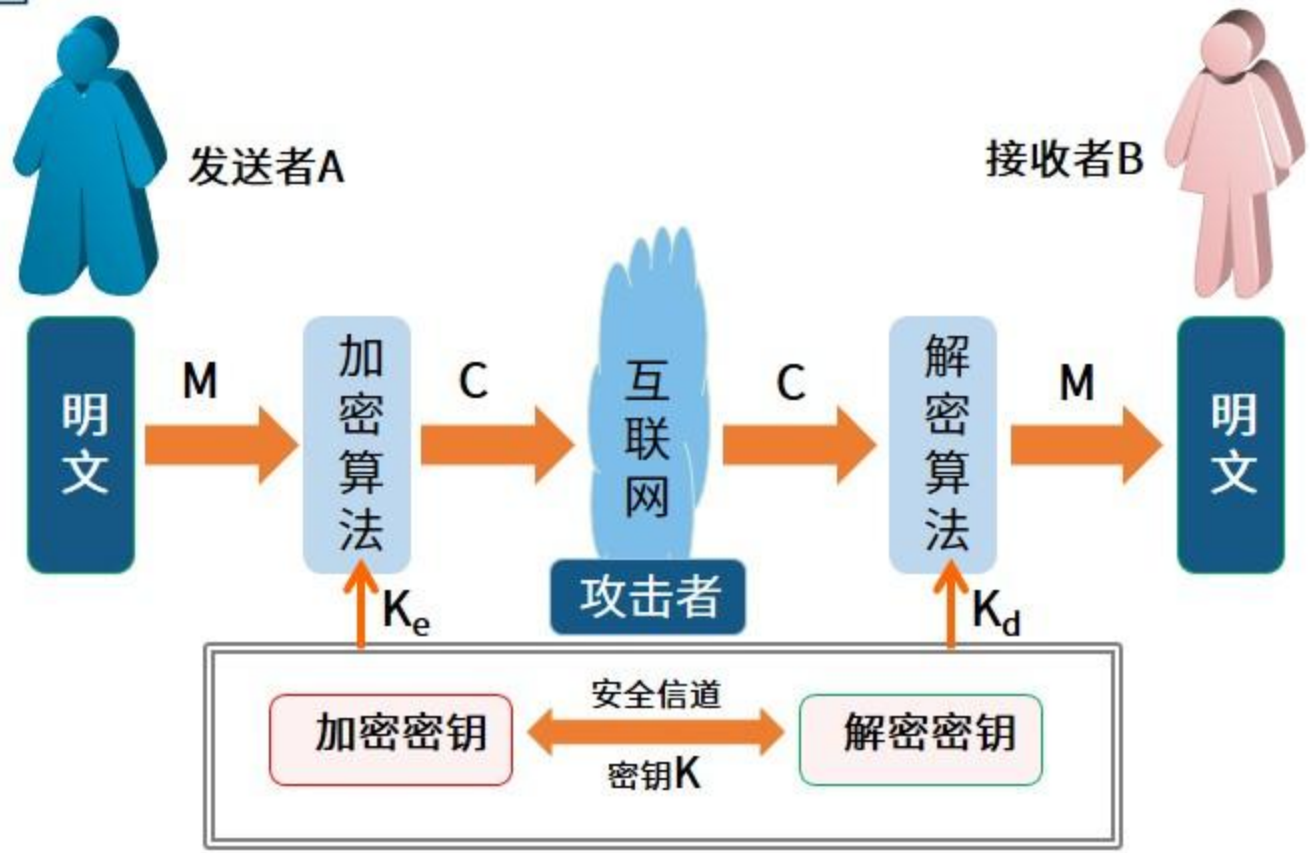
课程内容提要

希赛

- 安全基础技术
  - 对称与非对称加密（★★★）
  - 数字签名（★★★）
  - 信息摘要（★★★）
- 网络安全
  - 安全协议（★★★）
  - 网络攻击（★★）
  - 等级保护标准（★★）

对称加密技术

希赛



对称加密：$K_e=K_d$；

注：密钥K的安全传输是关键。

对称加密技术

希赛

缺陷：
- 1、加密强度不高，但效率高。
- 2、密钥分发困难。

常见对称密钥加密算法：

- ✓ DES：替换+移位、56位密钥、64位数据块、速度快、密钥易产生

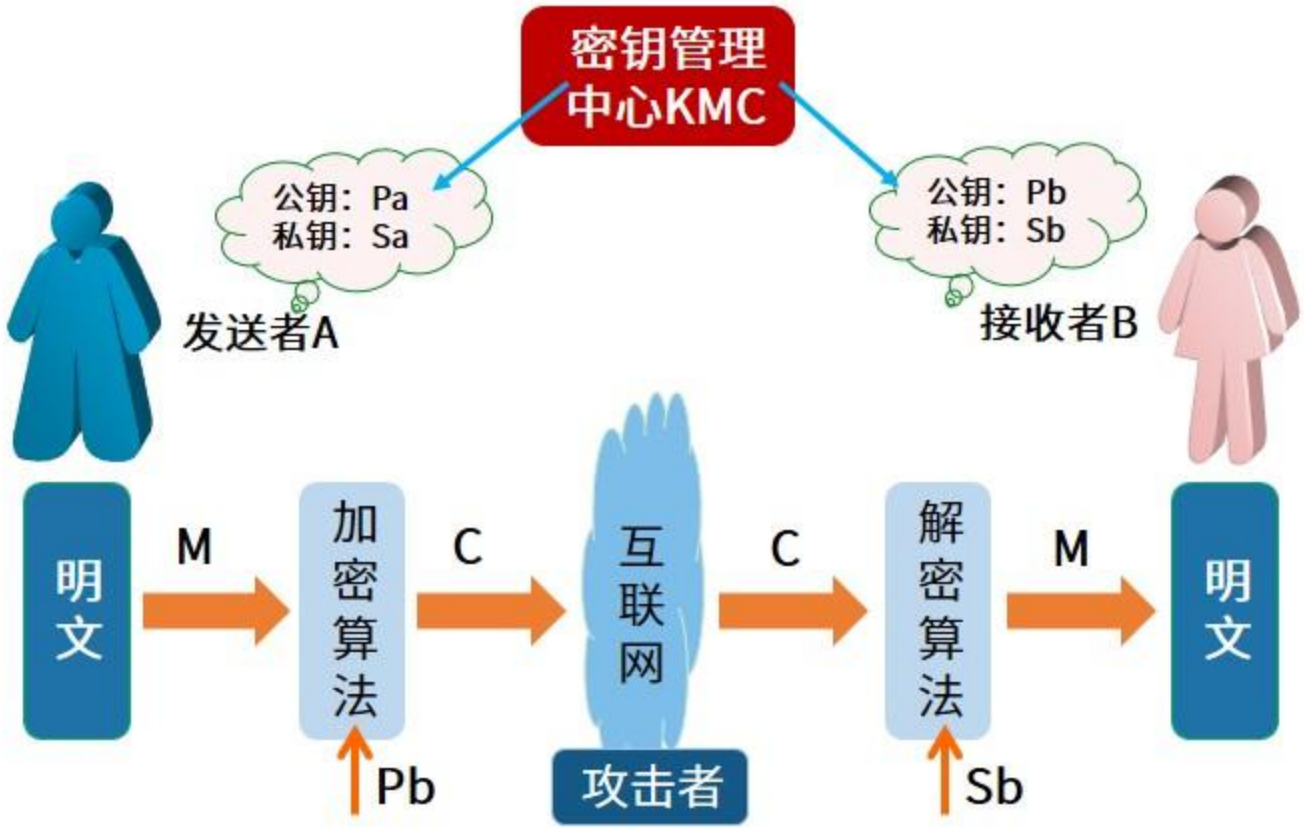
  3DES(三重DES)：两个56位的密钥K1、K2

  加密：K1加密->K2解密->K1加密

  解密：K1解密->K2加密->K1解密
- ✓ RC-5：RSA数据安全公司的很多产品都使用了RC-5。
- ✓ IDEA算法：128位密钥、64位数据块、比DES的加密性好、对计算机功能要**求相对低，PGP。**
- ✓ AES算法：高级加密标准，又称Rijndael加密法，是美国政府采用的一种区块加密标准。

非对称加密技术

希赛



非对称加密： $K_e \neq K_d$；

注：密钥必须成对使用（公钥加密，相应的私钥解密）。

非对称加密技术

希赛

缺陷：加密速度慢

常见非对称密钥加密算法：

RSA：2048位（或1024位）密钥、计算量极大、难破解

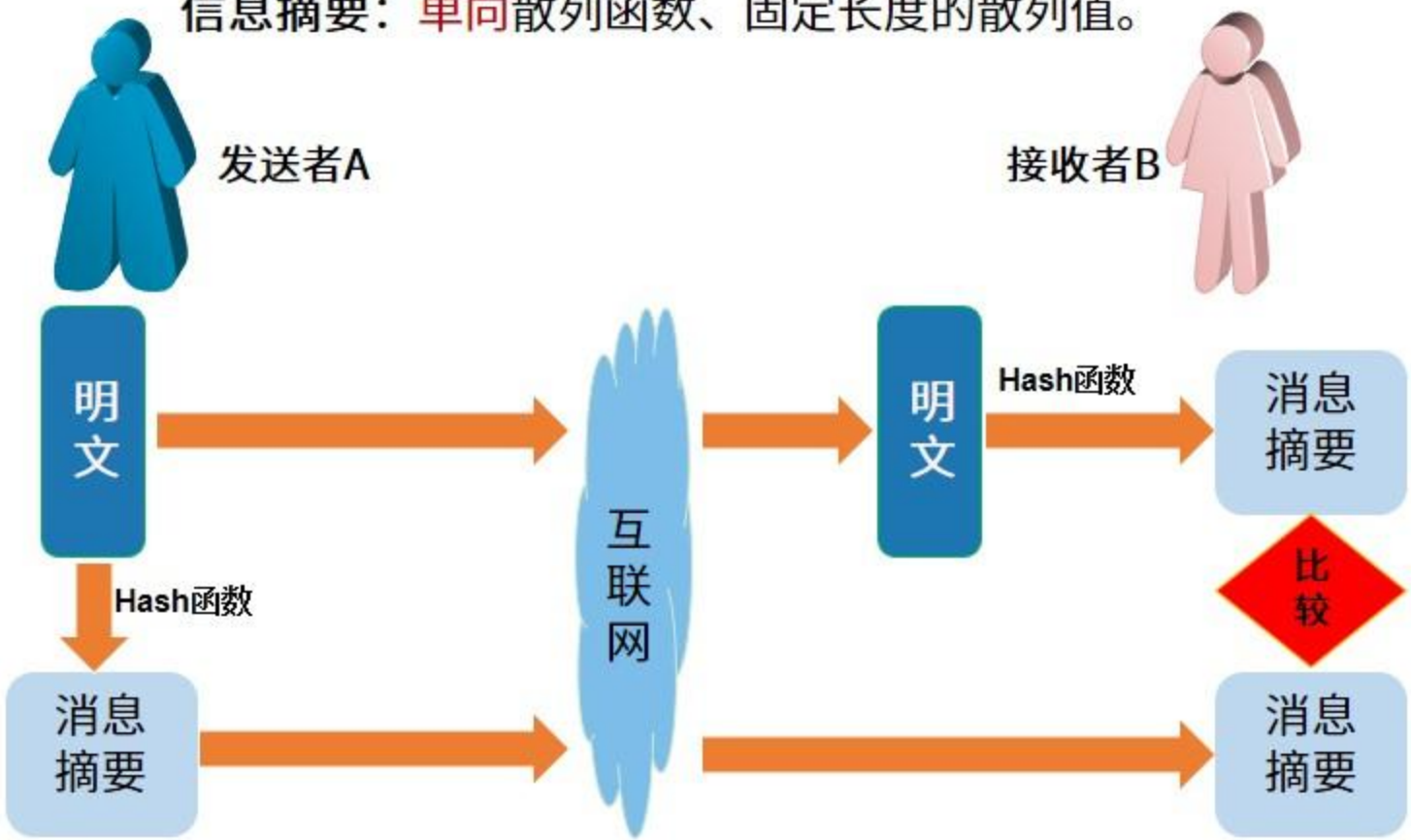
Elgamal：安全性依赖于计算有限域上离散对数这一难题。

ECC：椭圆曲线算法

信息摘要

希赛

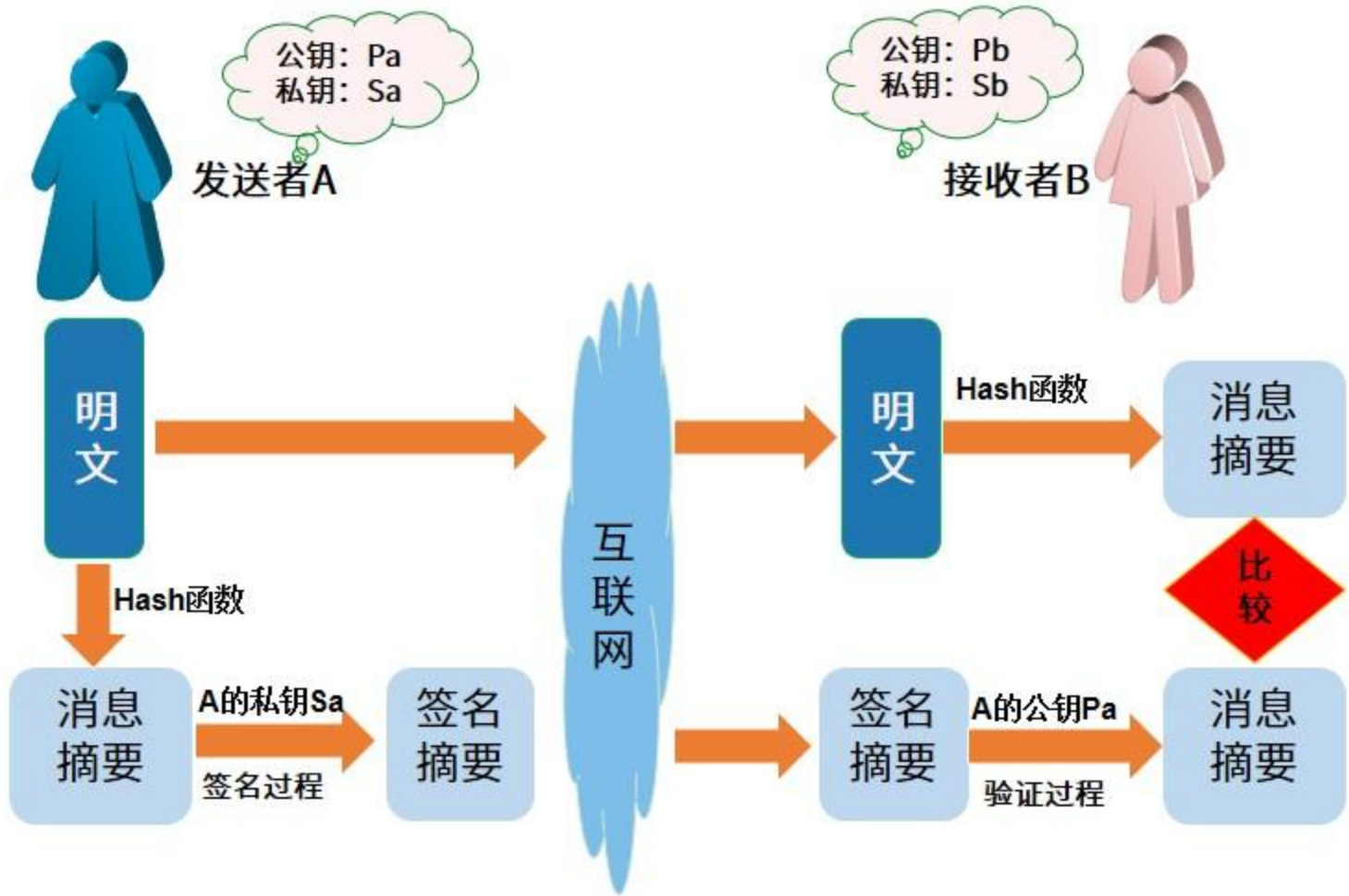
信息摘要：单向散列函数、固定长度的散列值。



数字摘要：由单向散列函数加密成固定长度的散列值。常用的消息摘要算法有MD5，SHA等，市场上广泛使用的MD5，SHA算法的散列值分别为128和160位，由于SHA通常采用的密钥长度较长，因此安全性高于MD5。

数字签名

希赛


公钥：Pa
私钥：Sa
发送者A
公钥：Pb
私钥：Sb
接收者B
明文
Hash函数
消息摘要
比较
互联网
明文
Hash函数
消息摘要
A的私钥Sa
签名过程
签名摘要
签名摘要
A的公钥Pa
验证过程
消息摘要

练习题

希赛

请依据已学习的加密解密技术，以及信息摘要，数字签名技术解决以下问题：

请设计一个安全邮件传输系统，要求：

该邮件以加密方式传输，邮件最大附件内容可达2GB，发送者不可抵赖，若邮件被第三方截获，第三方无法篡改。

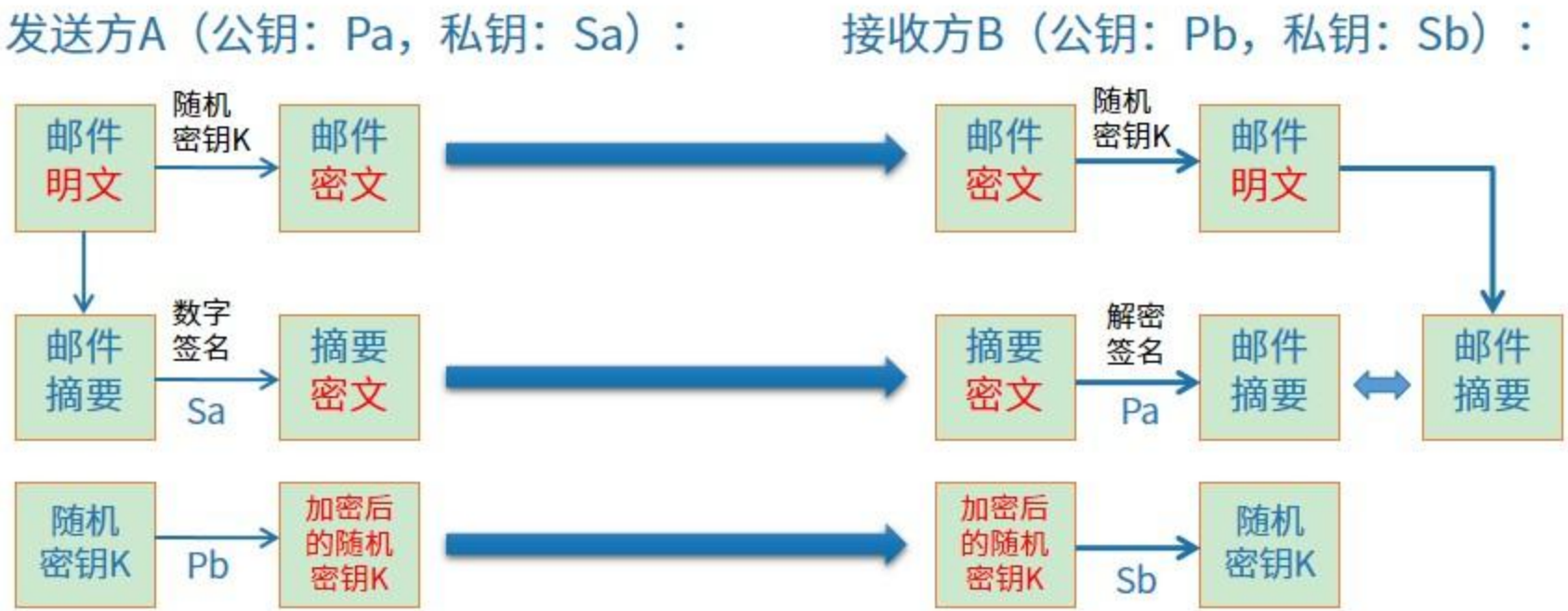
练习题

希赛

加密解密技术　　对称加密　　数字签名

该邮件以加密方式传输，邮件最大附件内容可达2GB，发送者不可抵赖，若邮件被第三方截获，第三方无法篡改。

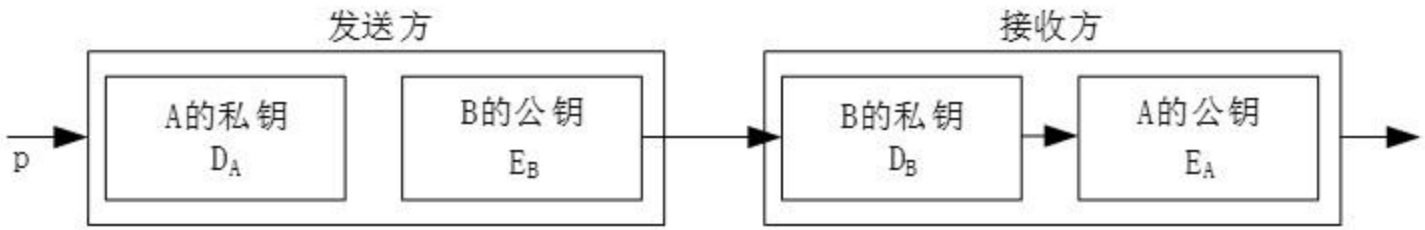
信息摘要技术



练习题

希赛

某数字签名系统如下图所示。网上传送的报文是（　），如果A否认发送，作为证据的是（　）。



A．P　　B．DA（P）　　C．EB（DA（P））　　D．DA

A．P　　B．DA（P）　　C．EB（DA（P））　　D．DA

数字证书内容

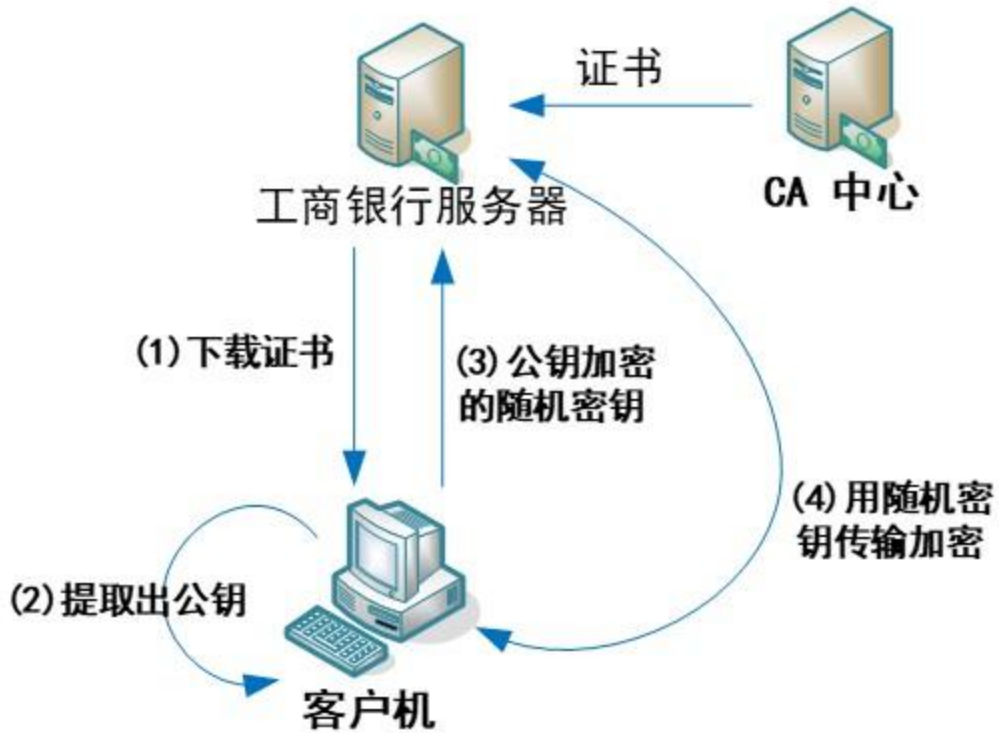
希赛

◆ 数字证书内容

- 证书的版本信息；
- 证书的序列号，每个证书都有一个唯一的证书序列号；
- 证书所使用的签名算法；
- 证书的发行机构名称，命名规则一般采用X.500格式；
- 证书的有效期，现在通用的证书一般采用UTC时间格式，它的计时范围为1950-2049；
- 证书所有人的名称，命名规则一般采用X.500格式；
- 证书所有人的公开密钥；
- 证书发行者对证书的签名。

PKI公钥体系

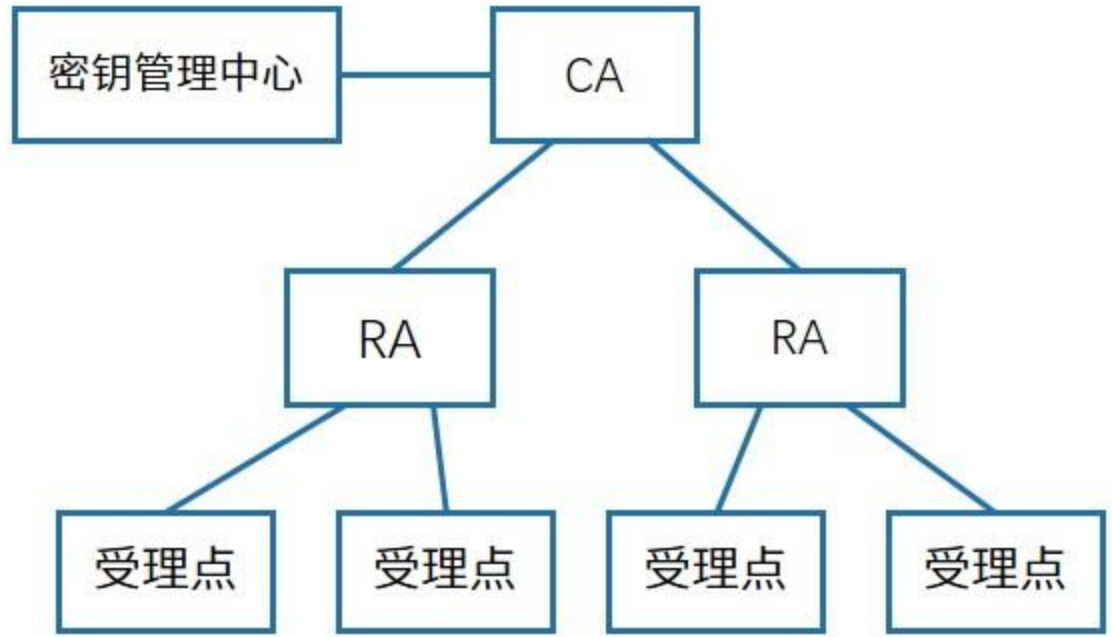
希赛



PKI公钥体系

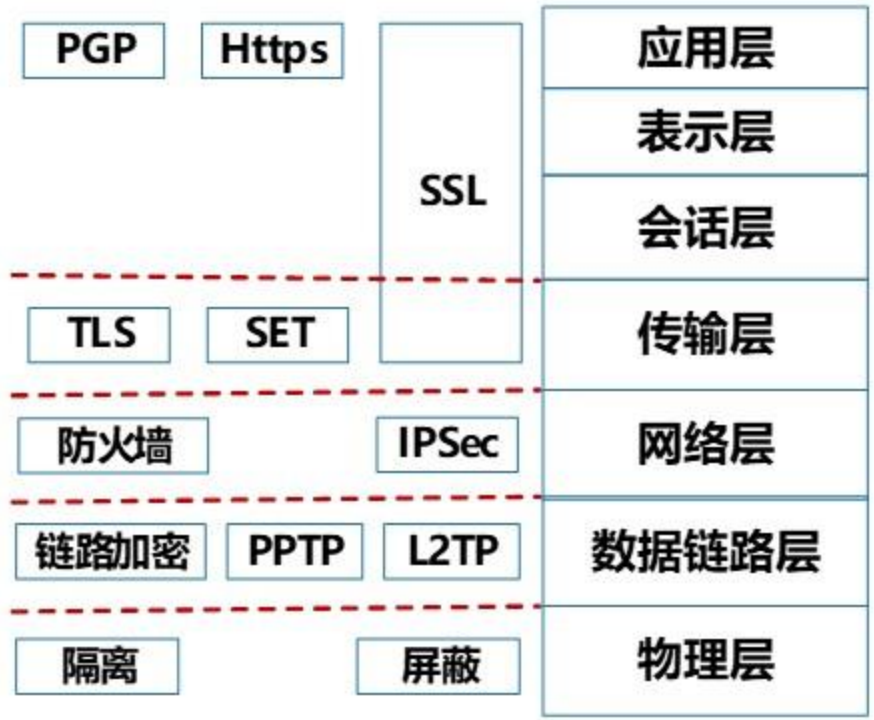
希赛

- CA（Certificate Authority）
  认证中心
- RA（Registration Authority）
  注册审批机构
- 证书受理点
- 密钥管理中心-KMC



网络安全－各个网络层次的安全保障

希赛



网络安全 – 各个网络层次的安全保障

希赛

PGP（Pretty Good Privacy）：优良保密协议。针对邮件和文件的混合加密系统。

SSL（Secure Sockets Layer）：安全套接字协议。工作在传输层至应用层。

TLS（Transport Layer Security）：传输层安全协议。

SET（Secure Electronic Transaction）：安全电子交易协议。电子商务，身份认证。普遍的说法是将其归为应用层。

IPSEC（Internet Protocol Security）：互联网安全协议。对IP包加密。

练习题

希赛

IP安全性（IP Security，IPSec）提供了在局域网、广域网和互联网中安全通信能力。关于IP安全性下列说法不正确的是（　）。

A IPSec可提供同一公司各分支机构通过的安全连接

B IPSec可提供远程安全访问

C IPSec可提高电子商务的安全性

D IPSec能在IP的新版本IPv6下工作，但不适应IP目前的版本IPv4

网络安全 – 网络威胁与攻击

希赛

被动攻击：收集信息为主，破坏保密性。

主动攻击：主动攻击的类别主要有：中断（破坏可用性），篡改（破坏完整性），伪造（破坏真实性）。

攻击类型	攻击名称	描述
被动攻击	窃听（网络监听）	用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。
	业务流分析	通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从而发现有价值的信息和规律。
	非法登录	有些资料将这种方式归为被动攻击方式。

网络安全 – 网络威胁与攻击

希赛

攻击类型	攻击名称	描述
主动攻击	假冒身份	通过欺骗通信系统（或用户）达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。黑客大多是采用假冒进行攻击。
	抵赖	这是一种来自用户的攻击，比如：否认自己曾经发布过的某条消息、伪造一份对方来信等。
	旁路控制【旁路攻击】	密码学中是指绕过对加密算法的繁琐分析，利用密码算法的硬件实现的运算中泄露的信息。如执行时间、功耗、电磁辐射等，结合统计理论快速的破解密码系统。
	重放攻击	所截获的某次合法的通信数据拷贝，出于非法的目的而被重新发送。加时间戳能识别并应对重放攻击。
	拒绝服务（DOS）	对信息或其他资源的合法访问被无条件的阻止。

练习题

希赛

信息安全的威胁有多种，其中（ ）是指通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

A 窃听　　B 信息泄露　　C 旁路控制　　D 业务流分析

安全保护等级

希赛

计算机信息系统安全保护等级划分准则（GB 17859-1999）

✓ **用户自主保护级**：适用于普通内联网用户

系统被破坏后，对公民、法人和其他组织权益有损害，但不损害国家安全社会秩序和公共利益。

✓ **系统审计保护级**：适用于通过内联网或国际网进行商务活动，需要保密的非重要单位

系统被破坏后，对公民、法人和其他组织权益有严重损害，或损害社会秩序和公共利益，但不损害国家安全。

✓ **安全标记保护级**：适用于地方各级国家机关、金融机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位

系统被破坏后，对社会秩序和公共利益造成严重损害，或对国家安全造成损害。

✓ **结构化保护级**：适用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研机构和国防建设等部门

系统被破坏后，对社会秩序和公共利益造成特别严重损害，或对国家安全造成严重损害。

✓ **访问验证保护级**：适用于国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位

系统被破坏后，对国家安全造成特别严重损害。

安全保护等级

希赛

	公民、法人和其他组织权益	社会秩序和公共利益	国家安全
用户自主保护级	损害		
系统审计保护级	严重损害	损害	
安全标记保护级		严重损害	损害
结构化保护级			严重损害
访问验证保护级			特别严重损害

安全防范体系的层次

希赛

安全防范体系的层次划分：

（1）**物理环境的安全性**。包括通信线路、物理设备和机房的安全等。

（2）**操作系统的安全性**。主要表现在三个方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制和系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

（3）**网络的安全性**。网络层的安全问题主要体现在计算机网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等。

（4）**应用的安全性**。由提供服务所采用的应用软件和数据的安全性产生，包括Web服务、电子邮件系统和DNS等。此外，还包括病毒对系统的威胁。

（5）**管理的安全性**。包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。

练习题

希赛

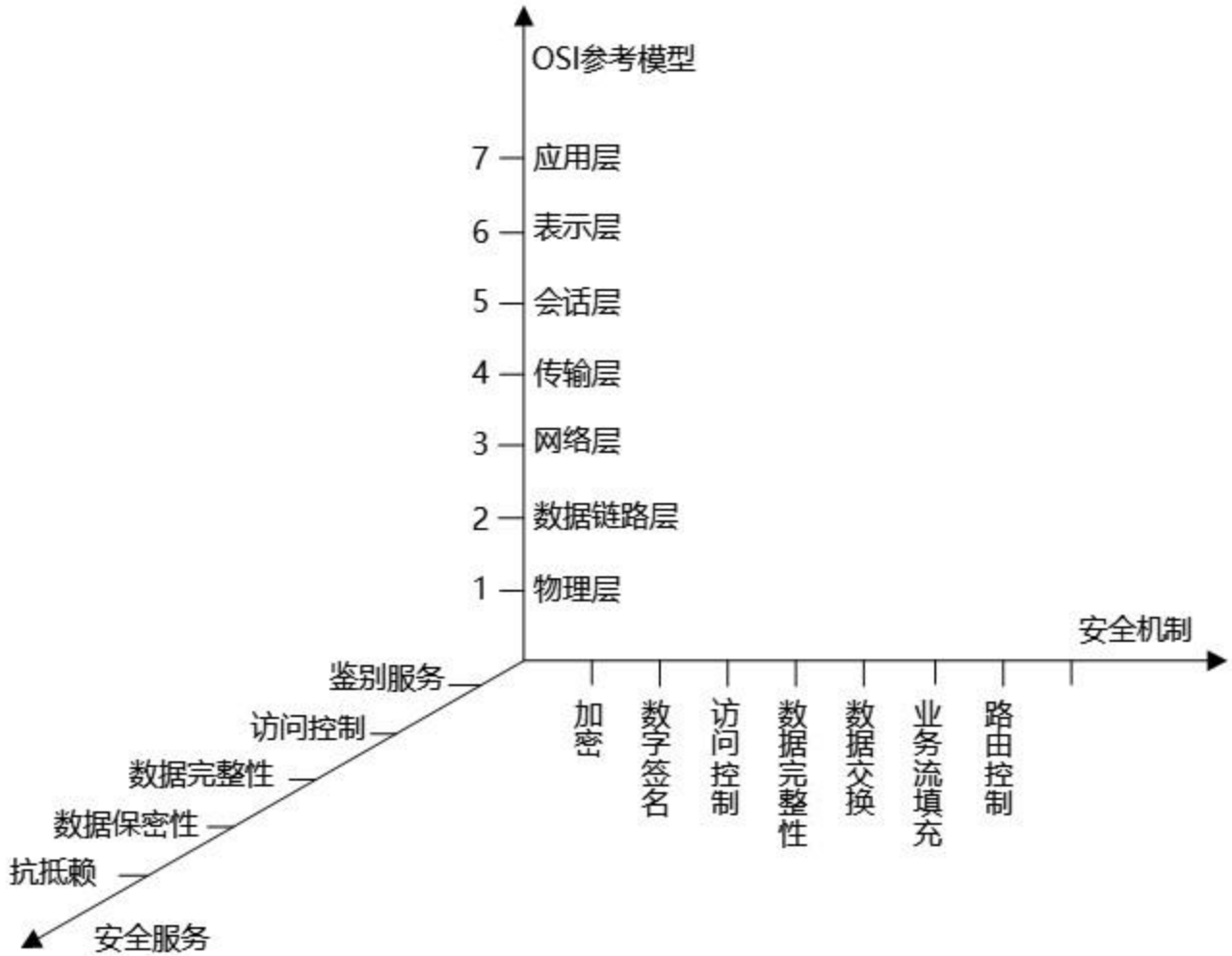
信息系统安全可划分为物理安全、网络安全、系统安全和应用安全，（ ）属于系统安全，（ ）属于应用安全。

A 机房安全　　B 入侵检测　　C 漏洞补丁管理　　D 数据库安全

A 机房安生　　B 入侵检测　　C 漏洞补丁管理　　D 数据库安全

信息安全体系结构

希赛


OSI参考模型
7 应用层
6 表示层
5 会话层
4 传输层
3 网络层
2 数据链路层
1 物理层
安全机制
加密
数字签名
访问控制
数据完整性
数据交换
业务流填充
路由控制
鉴别服务
访问控制
数据完整性
数据保密性
抗抵赖
安全服务

信息安全体系结构

希赛

- **鉴别服务**
  - ✓ 用户名+口令
  - ✓ 数字证书
  - ✓ 生物特征识别
- **访问控制**
  - ✓ **自主访问控制(DAC)**
  - ✓ 访问控制列表(ACL)
  - ✓ **强制访问控制(MAC)**
  - ✓ **基于角色的访问控制(RBAC)**
  - ✓ 基于任务的访问控制(TBAC)
- **数据完整性**
  - ✓ 阻止对媒体访问的机制：隔离，访问控制，路由控制
  - ✓ 探测非授权修改的机制：数字签名，数据重复，数字指纹，消息序列号
- **数据保密性**
  - ✓ 通过禁止访问提供机密性
  - ✓ 通过加密提供机密性
- **抗抵赖**
  - ✓ 数字签名