

## 第 16 章安全性和保密性

### 16.1 加密和解密

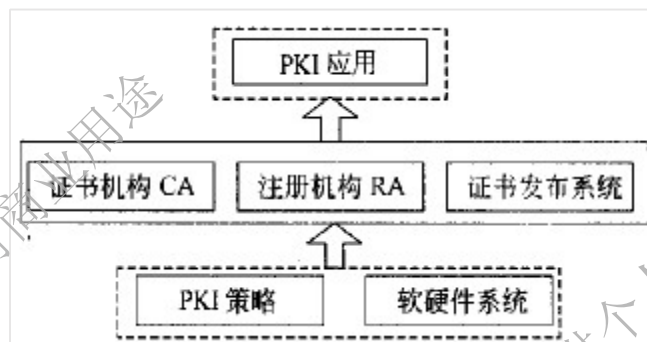
1. 【2009 年题 52】公司总部与分部之间需要传输大量数据, 在保障数据安全的同时又要兼顾密钥算法效率, 最合适的加密算法是( )。  
A. RC-5      B. RSA      C. ECC      D. MD5
2. 【2016 年题 38】DES 加密算法的密钥长度为 56 位, 三重 DES 的密钥长度为( ) 位。  
A. 168      B. 128      C. 112      D. 56

### 16.2 数字签名与数字水印

1. 【2018 年题 38】数字签名首先需要生成消息摘要, 然后发送方用自己的私钥对报文摘要进行加密, 接收方用发送方的公钥验证真伪。生成消息摘要的目的是(64), 对摘要进行加密的目的是(65)。  
(64) A. 防止窃听  
B. 防止抵赖  
C. 防止篡改  
D. 防止重放  
(65) A. 防止窃听  
B. 防止抵赖  
C. 防止篡改  
D. 防止重放

### 16.3 数字证书与密钥管理

1. 【2012 年题 8】下图所示 PKI 系统结构中, 负责生成和签署数字证书的是( ), 负责验证用户身份的是( )。



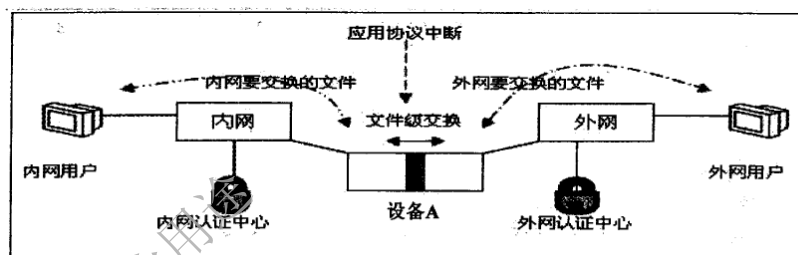
2. 【2013 年题 35】以下关于第三方认证服务的叙述中, 正确的是( )。  
A. Kerberos 认证服务中保存数字证书的服务器叫 CA  
B. 第三方认证服务的两种体制分别是 Kerberos 和 PKI

- C. PKI 体制中保存数字证书的服务器叫 KDC  
D. Kerberos 的中文全称是“公钥基础设施”

## 16.4 网络安全协议

- 【2011 年题 47】在网络管理中要防止各种安全威胁。在 SNMP 中, 无法预防的安全威胁是( )。
  - 篡改管理信息: 通过改变传输中的 SNMP 报文实施未经授权的管理操作
  - 通信分析: 第三者分析管理实体之间的通信规律, 从而获取管理信息
  - 假冒合法用户: 未经授权的用户冒充授权用户, 企图实施管理操作
  - 消息泄露: SNMP 引擎之间交换的信息被第三者偷听
- 【2011 年题 48】以下安全协议中, 用来实现安全电子邮件的协议是( )。
  - IPsec
  - L2TP
  - PGP
  - PPTP
- 【2014 年题 43】下列安全协议中( )是应用层安全协议。
  - IPSec
  - L2TP
  - PAP
  - HTTPS
- 【2017 年题 10】下面可提供安全电子邮件服务的是( )。
 

A.RSA      B.SSL      C.SET      D.S/MIME
- 【2017 年题 40】在网络规划中, 政府内外网之间应该部署网络安全防护设备。在下图中部署的设备 A 是( ), 对设备 A 的作用描述错误的是( )。



- (1) A.IDS      B.防火墙      网闸      D.UTM  
(2) A. 双主机系统, 即使外网被黑客攻击瘫痪也无法影响到内网  
B. 可以防止外部主动攻击  
C. 采用专用硬件控制技术保证内外网的实时链接  
D. 设备对外网的任何响应都是对内网用户请求的应答

## 16.7 网络安全体系

1. 【2010 年题 53】ARP 攻击造成网络无法跨网段通信的原因是( )。
  - A. 发送大量 ARP 报文造成网络拥塞
  - B. 伪造网关 ARP 报文使得数据包无法发送到网关
  - C. ARP 攻击破坏了网络的物理连通性
  - D. ARP 攻击破坏了网关设备
2. 【2013 年题 36】采用 Kerberos 系统进行认证时, 可以在报文中加入( )来防止重放攻击。
  - A. 会话密钥
  - B. 时间戳
  - C. 用户 ID
  - D. 私有密钥
3. 【2014 年题 42】下列攻击方式中, ( )不是利用 TCP/IP 漏洞发起的攻击。
  - A. SQL 注入攻击
  - B. Land 攻击
  - C. Ping of Death
  - D. Teardrop 攻击
4. 【2016 年题 39】下列攻击方式中, 流量分析属于( )方式。
  - A. 被动攻击
  - B. 主动攻击
  - C. 物理攻击
  - D. 分发攻击

## 16.10 其他

1. 【2017 年题 11】如果管理距离为 15, 则( )。
  - A. 这是一条静态路由
  - B. 这是一台直连设备
  - C. 该路由信息比较可靠
  - D. 该路由代价较小