国家计算机软考职称
中级网络工程师培训

第14课：网络安全与应用（一）

微信/QQ383419460，每周一三五 20:30-22:00， 全程录像网盘下载

上节课考点回顾

- 1、IPV6基础知识
- 2、移动IP和IPV6
- 3、IPV6过渡技术
- 4、IPV6路由协议

第14课：网络安全与应用（一）

- ***1、网络安全基础***
- 2、信息加密技术
- 3、数字签名技术
- 4、密钥管理技术
- 5、虚拟专用网VPN
- 6、网工考题分析

第14课：网络安全与应用（一）

- **考点01：**网络安全威胁和漏洞类型：

窃听	病毒
假冒	木马
重放	诽谤
流量分析	非授权访问
破坏完整	拒绝服务

- 漏洞：物理、软件、不兼容、其他等。

第14课：网络安全与应用（一）

- **考点02：**网络安全信息数据五大特征：

- 完整性：信息数据完整不破坏。
- 保密性：信息数据需授权不泄露。
- 可用性：信息数据攻击后迅速恢复可用。
- 不可否认性：信息数据参与者补课否认不可抵赖，身份真实有效。
- 可控性：信息数据可以管控传播范围。

第14课：网络安全与应用（一）

- **考点03：**网络安全基本技术：

- 数据加密：数据按照规则打乱，重新组合。
- 数字签名：证明发送者签发，也可完整性。
- 身份认证：用户合法性，身份真实没假冒。
- 防火墙：控制内外数据进出，阻挡病毒木马。
- 入侵检测：采用异常检测特征保护网络。
- 网络隔离：内外网隔离分开使用，如网闸。

第14课：网络安全与应用（一）

- 1、网络安全基础
- ***2、信息加密技术***
- 3、数字签名技术
- 4、密钥管理技术
- 5、虚拟专用网VPN
- 6、网工考题分析

第14课：网络安全与应用（一）

- **考点04：**现代信息加密技术：对称和非对称。

- 对称
  - DES、3DES、IDEA、AES、RC4等
- 非对称
  - RSA（基于大素数分解 3人）
  - ECC（椭圆曲线密码编码学）
  - Elgamal（基于离散对数 1人）

DES数据加密标准、3DES三重DES加密、IDEA国际数据加密算法、AES高级加密标准、RC4流加密算法第四版 2人等

第14课：网络安全与应用（一）

- **考点05：**现代信息加密技术对称密钥总结表：

类型	名称说明	密钥长度	分组长度	安全性
DES	数据加密标准，速度较快，适用于加密大量数据的场合；	56	64	依赖密钥受穷举法攻击
3DES	在DES基础上，用2个不同的密钥进行3次加密，强度更高	112	64	军事级，可抗差值等相关分析
AES	高级加密标准，下一代加密算法标准，速度快，安全级别高	128、192 256	64	安全级别高，高级加密标准
IDEA	国际数据加密算法，使用 128 位密钥提供非常强的安全性	128	64	能抵抗差分密码分析的攻击
MD5	信息-摘要算法 Message-Digest 5	128	512	主要是为数字签名而设计的
SHA	安全散列算法 Secure Hash Algorithm	160	512	可实现数字签名，和MD5相似

第14课：网络安全与应用（一）

- **考点06：**公钥加密RSA：加密体系：公钥加密，私钥解密。（签名体系：私钥加密，公钥解密）

①选两个大素数p和q

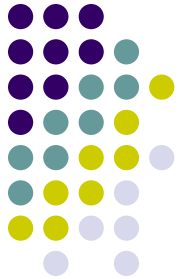
②令n=p*q，z=(p-1)(q-1)

③符合公式e*d=1（mod z），e公钥，d私钥。

mod为模运算，也就是取余数计算，例如：

e*d=1（mod z）可变形为（e*d）/ z余数为1

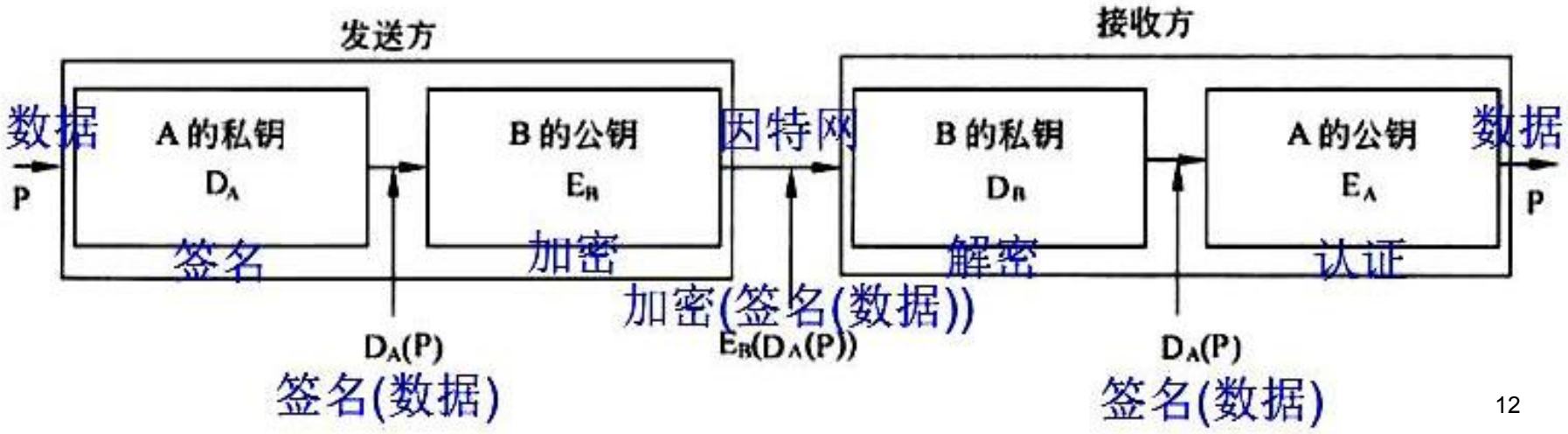
第14课：网络安全与应用（一）



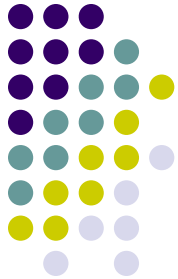
- 1、网络安全基础
- 2、信息加密技术
- ***3、数字签名技术***
- 4、密钥管理技术
- 5、虚拟专用网VPN
- 6、网工考题分析

第14课：网络安全与应用（一）

- **考点07：**数字签名技术：数字签名用于确认发送者身份和消息完整性。满足三个条件：①接收者能够核实发送者。②发送者事后不能抵赖。③接收者不能伪造签名。
- 下图为基于公钥的签名和加密体系示意图：



第14课：网络安全与应用（一）



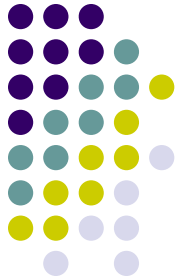
- 1、网络安全基础
- 2、信息加密技术
- 3、数字签名技术
- ***4、密钥管理技术***
- 5、虚拟专用网VPN
- 6、网工考题分析

第14课：网络安全与应用（一）

- **考点08：**密钥管理体系：KMI、PKI、SPK
- KMI：密钥管理基础结构，第三方KDC，秘密物理通道，适用于封闭的内网使用。
- PKI：公钥基础结构，不依赖秘密物理通道。适用于开放的外网。
- SPK：适用于规模化专用网。

- 口诀：男人在外面PK(I)，女人在家里KM(I)。

第14课：网络安全与应用（一）

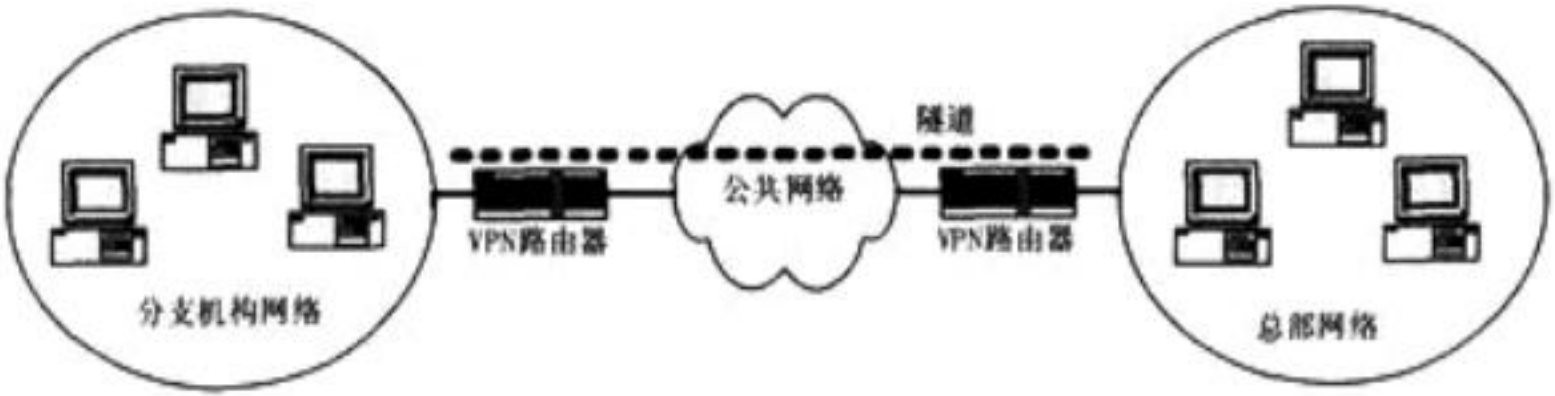


- 1、网络安全基础
- 2、信息加密技术
- 3、数字签名技术
- 4、密钥管理技术
- ***5、虚拟专用网VPN***
- 6、网工考题分析

第14课：网络安全与应用（一）

- **考点09：**VPN技术：虚拟专用网，①建立在公网上。②虚拟性，没有专用物理连接。③专用性，非VPN用户无法访问。

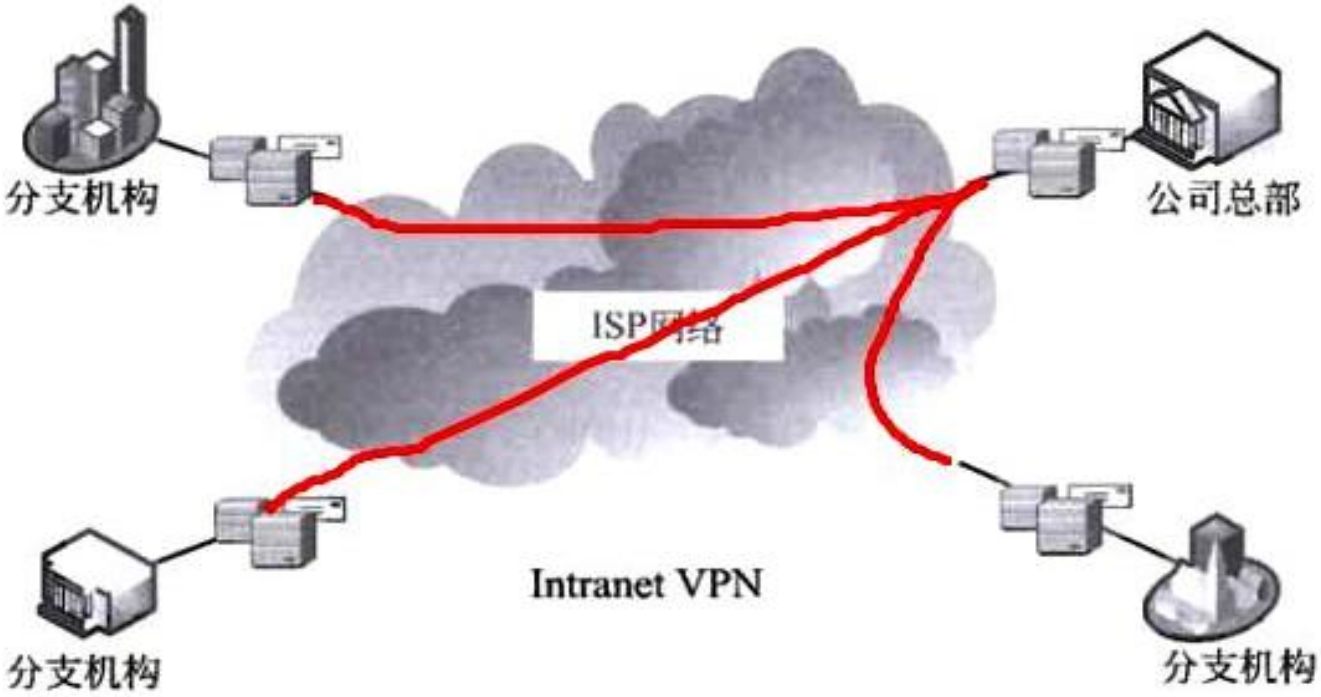
- VPN四个关键技术：①隧道技术。②加解密技术。③密钥管理技术。④身份认证技术。



第14课：网络安全与应用（一）

- **考点10：**VPN三种应用解决方案：

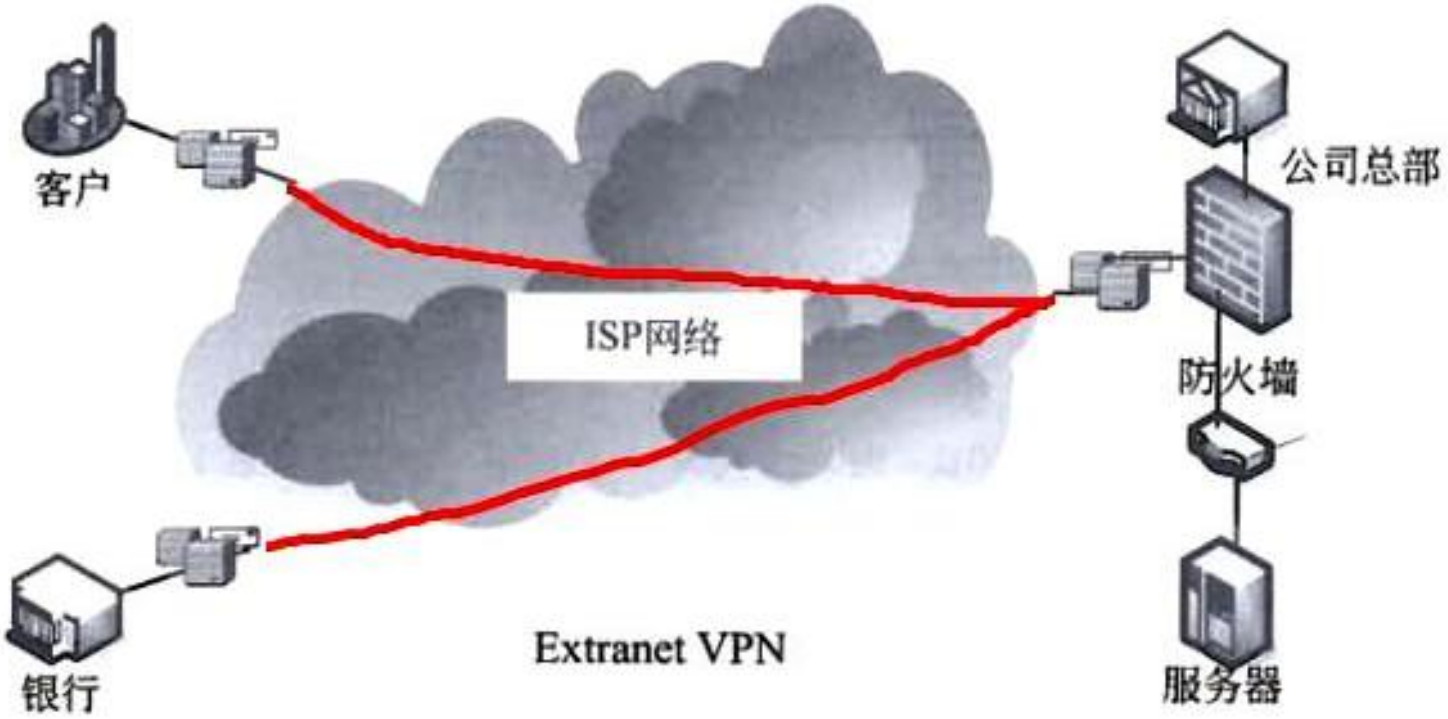
①内联网VPN（Intranet VPN）：企业内部用于连通总部和分布各个LAN。



第14课：网络安全与应用（一）

- **考点11：**VPN三种应用解决方案：

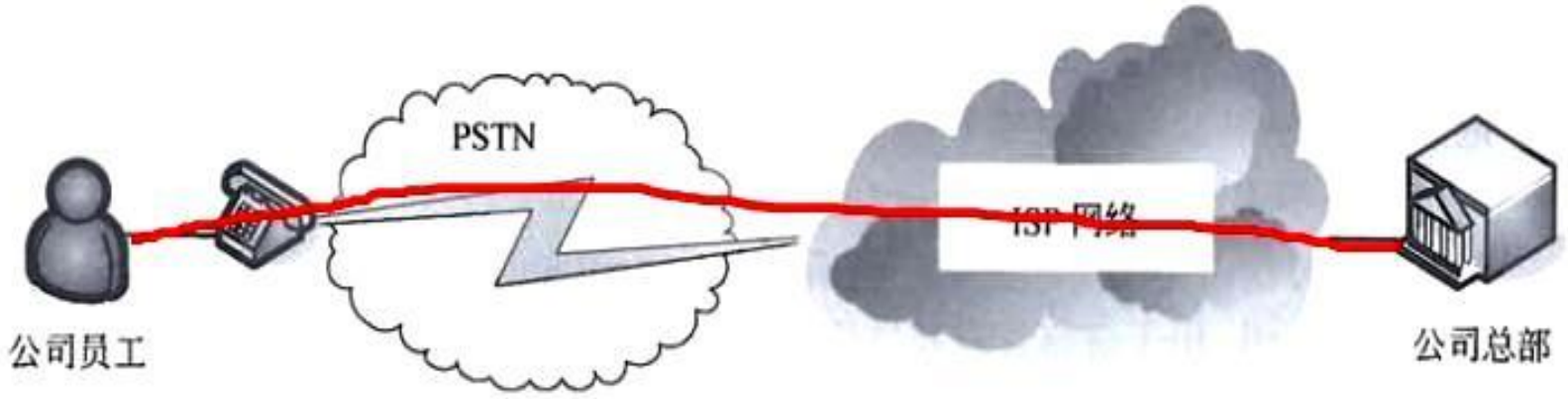
②外联网VPN（Extranet VPN）：企业外部用于实现企业与客户、银行、供应商互通。



第14课：网络安全与应用（一）

- **考点12：**VPN三种应用解决方案：

③远程接入VPN（Access VPN）：解决远程用户出差访问企业内部网络。



Access VPN

第14课：网络安全与应用（一）

- **考点13：**VPN在七层协议中使用的技术汇总：

VPN
- 二层：PPP、PPTP、L2TP
- 三层：IPSec、GRE
- 四层：SSL/TLS

PPP点对点协议、PPTP点对点隧道协议
L2TP第二层隧道协议、IPSec IP安全性、
GRE通用路由封装协议、SSL/TLS安全套接层。

第14课：网络安全与应用（一）

- **考点14：**PPP、PPTP、L2TP技术对比汇总：

PPP
- LCP：链路控制协议（2层）
- NCP：网络控制协议（3层）

PPP
- PAP：口令认证协议（明文）
- CHAP：挑战握手协议（密文）

PPTP
- PAC：PPTP接入集中器
- PNS：PPTP网络服务器

L2TP
- LAC：L2TP访问集中器
- LNS：L2TP网络服务器

第14课：网络安全与应用（一）

- **考点15：**PPTP与L2TP的区别比较：

①PPTP要求IP网络，L2TP适用各种网络。
②PPTP只能建立1条隧道，L2TP建立多条。
③PPTP包头占用6字节，L2TP占用4字节
④PPTP不支持隧道验证，L2TP支持。

总结：L2TP一个字“好”，四个字“好好好好”。

第14课：网络安全与应用（一）

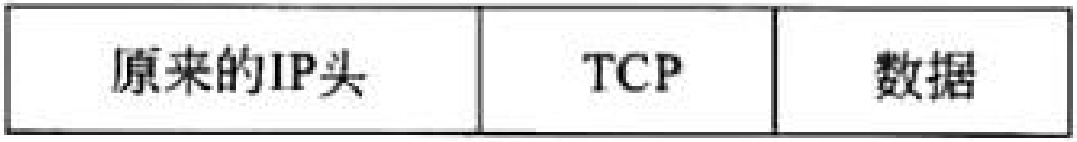
- **考点16：**IPSec：IP安全性，在IP层通过加密与数据源验证，来保证数据包传输安全。

- ①认证头AH，用于数据完整和数据源认证、防重放。
- ②封装安全负荷ESP，提供数据保密、数据完整、辅助防重放。
- ③密钥交换协议IKE，生成分发密钥。

- IPSec两种模式：传输模式和隧道模式。

第14课：网络安全与应用（一）

- 考点17：IPSec：传输模式和隧道模式。



传输模式的认证头

隧道模式的认证头

第14课：网络安全与应用（一）

- **考点18：**SSL安全套接层：和TLS（传输层安全标准）是双胞胎。在传输层上4.5层套接安全协议。SSL/TLS被称为HTTPS，工作在传输层，对传输层、应用层都可以控制。

潜伏 余则成 的故事

第14课：网络安全与应用（一）

- **考点19：**SSL和IPSec的区别比较：

- ①IPSec在网络层建立隧道，适用于固定的VPN。SSL是通过应用层的web连接建立的，适合移动用户远程访问公司的VPN。

- ②IPSec工作在网络层，灵活性小。SSL工作在传输层，灵活性大。

第14课：网络安全与应用（一）

- 1、网络安全基础
- 2、信息加密技术
- 3、数字签名技术
- 4、密钥管理技术
- 5、虚拟专用网VPN
- ***6、网工考题分析***

【章节】网工：8.1-8.8

例题01

- 高级加密标准AES支持的三种秘钥长度不包括（　　）。

A. 56　　B. 128　　C. 192　　D. 256

例题02

- 在报文摘要算法MD5中，首先要进行明文分组与填充，其中分组时明文报文摘要按照（　　）位进行分组。

A. 128　　B. 256　　C. 512　　D. 1024

例题03

- 按RSA算法，若选两奇数P=5，Q=3，公钥E=7，则私钥为（　　）。

A. 6　　B. 7　　C. 8　　D. 9

例题04

甲和乙要进行通信，甲对发送的消息附加了数字签名，乙收到该消息后利用（　　）验证该消息的真实性。

A. 甲的公钥　　B. 甲的私钥

C. 乙的公钥　　D. 乙的私钥

例题05

- 某企业打算采用IPSec协议构建VPN，由于企业申请的全球IP地址不够，企业内部网决定使用本地IP地址，这时在内外网间的路由器上应该采用（　　），IPSec协议应该采用（　　）。

A. NAT技术　　B. 加密技术

C. 消息鉴别技术　　D. 数字签名技术

A. 传输模式　　B. 隧道模式

C. 传输和隧道混合模式　　D. 传输和隧道嵌套模式

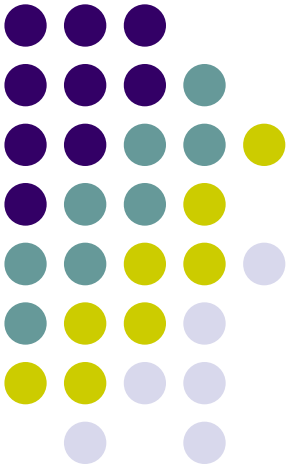
例题答案

- 例题01：A。　　例题02：C。
- 例题03：B。这里p=5，q=3。n=pq=15，z=(p-1)（q-1）=8。根据ed=1（mod z），也就是（ed）/ z余数为1。即：（7*d）/ 8 .....1，把答案6、7、8、9带入只有答案B 满足条件。
- 例题04：A。　例题05：A、B。
- **作业：01号题库16**

获取考试咨询帮助加老师
微信/QQ 383419460

大涛网络学院 出品

UU教育 2017.8月



微信/QQ383419460，每周一三五 20:30-22:00， 全程录像网盘下载