西 北 师 范 大 学

教 师 授 课 教 案

课 程 名 称 ： 计算机网络

课 程 学 分 ： 3

课 程 类 别 ： 必修

授 课 班 级 ：

授 课 教 师 ：

周　　次	第 16 周	教案号	16
授课时间	（2 节/周）		
授课内容概要	**第 7 章　网络安全** 7.1　网络安全问题概述 □　　7.1.1　计算机网络面临的安全性威胁 7.1.2　计算机网络安全的内容 □　　7.1.3　一般的数据加密模型 □7.2　两类密码体制 □　　7.2.1　对称密钥密码体制 7.2.2　公钥密码体制 □7.3　数字签名 □7.4　鉴别 □　　7.4.1　报文鉴别 □　　7.4.2　实体鉴别 □ 7.6　因特网使用的安全协议 □　　7.6.1　网络层安全协议 □　　7.6.2　运输层安全协议 □　　7.6.3　应用层的安全协议破 □7.7　系统安全：防火墙与入侵检测 □　　7.7.1　防火墙 □　　7.7.2　入侵检测系统 □		
目的要求	1、了解计算机网络安全的内容，防火墙与入侵检测。 2、掌握两类密码体制，数字签名。		
重点	两类密码体制，数字签名		
难点	数字签名		
作业布置	学习报告		

<table>
<tr><td>参考书</td><td colspan="5">1、《计算机网络》（第五版），谢希仁编著，电子工业出版社。
2、《计算机网络》（第四版），Andrew S. Tanenbaum 著，潘爱民译，清华大学出版社。
3、《数据通信与计算机网络》，高传善、钱松荣、毛迪林编著，高等教育出版社。
4、《Computer Networks (Forth Edition)》，Andrew S. Tanenbaum 著，清华大学出版社。
5、《TCP/IP 协议簇》，Behrouz A.Forouzan & Sophia Chung Fegan 著，谢希仁译，清华大学出版社。</td></tr>
<tr><td>课　　型</td><td>理论课</td><td rowspan="4">学时分配</td><td>复 习</td><td>10　　分钟</td></tr>
<tr><td>主要教具</td><td>计算机、投影仪、黑板、粉笔</td><td>讲 授</td><td>80　　分钟</td></tr>
<tr><td>教学方法</td><td>启发式</td><td>指 导</td><td>分钟</td></tr>
<tr><td>教学手段</td><td>讲授</td><td>总 结</td><td>10　　分钟</td></tr>
<tr><td>备注</td><td colspan="4"></td></tr>
</table>

授 课 过 程 及 内 容	备 注
第 7 章　网络安全 7.1 网络安全问题概述 计算机网络上的通信面临以下两大类威胁： □ 一、被动攻击 □ 二、主动攻击： □　　(1) 篡改——故意篡改网络上传送的报文。 □　　(2) 恶意程序——　包括计算机病毒、计算机蠕虫、特洛伊木马和逻辑炸弹等。 □　　(3) 拒绝服务——包括分布式拒绝服务。 □ 三、　一般的数据加密模型 7.2 两类密码体制 7.2.1　　对称密钥密码体制 数据加密标准 DES 7.2.2　公钥密码体制 7.3　　数字签名 (1) 报文鉴别——接收者能够核实发送者对报文的签名； (2) 报文的完整性——发送者事后不能抵赖对报文的签名； (3) 不可否认——接收者不能伪造对报文的签名。 □ 7.4　鉴别 (1)　　报文鉴别 (2)　　实体鉴别 (3)　　摘要技术 7.6　因特网使用的安全协议 7.6.1　网络层安全协议 （1） IPsec 协议 （2） IPsec 数据报的格式 7.6.2　运输层安全协议 安全套接字层 SSL (Secure Socket Layer) □运输层安全 TLS (Transport Layer Security) 7.6.3　应用层的安全协议	

PGP (Pretty Good Privacy) 7.7　系统安全： 防火墙与入侵检测	