**网络安全问题概述**

被动攻击和主动攻击 几种类型

**对称加密和非对称加密**

他们区别，他们的特点

**数字签名**

它的作用，可以防治别人更改内容，具体案例（红头文件），

它的工作流程 ，观看图片p307图片7-6

**公钥分配**

认证机构CA的作用，

在签合同时，我们如何认定别人公司是用他们私钥加密的，我们可以用他们给的公钥，对合同解密，但是如果他不承认这个是他们公司分发的公钥怎么办，这个时候就，需要一个值得信认的机构，发一对私钥和公钥。

**网络层安全协议**

我们上面说的都是应用层的安全协定，下面的就是网络层的。

关联SA是什么东西 p313

IPSec数据报是什么？

关联SA如何建立的？p316红线

AH协议数据报结构，和ESP数据报结构

AH是用于数字签名，所以他不加密

ESP用于数字签名和加密

**运输层安全**

SSL他位于网络五层那一层之间？

Https和http区别

SSL提供的安全服务

第三层，加密SSL通话，这个部分显示在P318 图7-17中，表示了我们是如何建立https:对话的。

**防火墙**

网络层防火墙 他能干什么

应用层防火墙 他能干啥。