**第7章 网络安全**

**一、单选题**

1、防火墙系统采用主要技术是下列（ ）。

A. 对通过的数据包进行加密；

B. 对通过的数据包进行过滤；

C. 对通过的数据包进行正确性检测；

D. 对通过的数据包进行完整性检测。

B

2、在数字通信中，使收发双方在时间基准上保持一致的技术是 什么技术（ ）

A．交换技术

B．同步技术

C．编码技术

D．传输技术

B

3、在公钥密码体制中，不公开的是什么（ ）

A.公钥

B.私钥

C.公钥和加密算法

D.私钥和加密算法

B

4、在企业内部网与外部网之间，用来检查网络请求分组是否合法，保护网络资源不被非法使用的技术是下列（ ）技术。

A．防病毒技术；

B．防火墙技术；

C．差错控制技术；

D．流量控制技术。

B

5、（ ）不是防火墙的作用。

A．网络的安全屏障；

B．防止内部信息的外泄；

C．对网络存取和访问进行监控审计；

D．防范病毒。

D

6、常用的加密方法主要有两种： ( ) 。

A、常规密钥体系和公钥密码体系；

B、DES 和密钥密码体系；

C、RES 和公钥密码体系 ；

D、加密密钥和解密密钥。

A

7、下列( ) 技术可以防止信息收发双方的抵赖。

A、数据加密；

B、访问控制；

C、数字签名；

D、审计 。

C

**二、判断题**

1、公开密钥密码体制中，加密密钥和解密密钥都是公开的。（ ）。

错

2、在公开密钥密码体制中，解密密钥是保密的。（ ）

对

3、网络中的安全威胁“中断”属于主动攻击。（ ）

对

4、网络安全威胁的“截获”属于主动攻击。（ ）

错

5、公钥加密体制中，没有公开的是明文。（ ）

错

**三、填空题**

1、计算机网络通信面临的4中安全威胁有截获、中断、（ ）和伪造。

2、在早期的常规密钥密码体制中，常用的两种密码是替代密码和（ ）密码。

3、公钥密码体制中( )是公开的，( )是需要保密的。

4、某种网络安全威胁是通过非法手段取得对数据的使用权，并对数据进行恶意地添加和修改，这种安全威胁属于（ ）。

**四、简答题**

1、简述主动攻击和被动攻击的区别。

2、简述对称密钥体制与公钥密码体制的特点。

3、简述因特网的网络层安全协议族IPsec 包含的主要协议。

4、简述实现报文鉴别和实体鉴别的方法。

5、简述数字签名的原理。

**五、应用题**

1、试述SSL的工作过程

2、试述防火墙的工作原理和所提供的功能。

3、试述电子邮件安全协议PGP的措施。