第二次阶段性测试

班级：_____ _____

_____

1、TLS 连接和 TLS 会话的区别是什么？

答：TLS 连接指的是客户端和服务器之间建立的一种安全通信链路。它是通过 TLS 协议进行加密和认证的。TLS 连接的建立包括握手过程，其中包括了密钥交换、身份验证和协商加密算法等步骤。

TLS 会话指的是在 TLS 连接建立后，客户端和服务器之间的一段时间内的通信。TLS 会话包括了握手阶段和数据传输阶段。简而言之，TLS 连接是建立在客户端和服务器之间的安全通信链路，而 TLS 会话是建立在 TLS 连接之上的一段时间内的通信。

2、为何 Base64 转换在电子邮件应用中的作用很大？

答：Base64 是一种将二进制数据转换为可打印字符的编码方案。在电子邮件应用中，Base64 转换起到了重要的作用，主要是因为电子邮件协议旨在传输文本数据，而不是二进制数据。由于邮件通常包含附件、图片等二进制数据，因此需要一种方法将这些二进制数据转换为文本数据进行传输。

Base64 编码可以确保转换后的文本数据只包含可打印字符，不会导致数据在传输过程中被错误解析或丢失。Base64 编码后的文本数据可以直接嵌入到电子邮件的文本部分中，而不会破坏邮件的格式。这使得在电子邮件中传输二进制数据变得更加方便和可靠。

因此，Base64 转换在电子邮件应用中广泛应用于附件传输、图片嵌入和编码非文本内容等场景，提高了邮件传输的可靠性和兼容性。

3、IPSec 中传输模式和隧道模式有何不同？

答：传输模式用于直接保护两个主机之间的通信。在传输模式下，IP 数据报的原始 IP 头部被保留，只有 IP 数据报的有效负载即传输层以上的数据被加密

和认证。传输模式适用于主机到主机的通信，提供了点对点的安全性。

隧道模式用于保护整个 IP 数据报。在隧道模式下，整个 IP 数据报被加密和认证，然后再封装在一个新的 IP 数据报中。新的 IP 数据报具有不同的源 IP 和目的 IP 地址，用于在网络中的两个端点之间建立安全隧道。隧道模式适用于网络到网络的通信，提供了网络层的安全性。

简而言之，传输模式适用于主机到主机的通信，只保护 IP 数据报的有效负载；而隧道模式适用于网络到网络的通信，保护整个 IP 数据报并在新的 IP 数据报中封装。

4、数据包过滤防火墙与状态检测防火墙有何不同？

答：数据包过滤防火墙是一种基于网络层和传输层信息对数据包进行过滤和控制的防火墙。它通过检查数据包的源 IP 地址、目的 IP 地址、端口号等信息，并根据预定义的规则决定是否允许或拒绝数据包的传输。数据包过滤防火墙通常基于访问控制列表进行配置，对于每个数据包都会进行独立的过滤决策。

状态检测防火墙是一种结合了数据包过滤和会话状态追踪的防火墙。它不仅检查单个数据包的头部信息，还维护和跟踪网络会话的状态。状态检测防火墙可以识别和管理网络连接的状态，包括建立、终止和数据传输等阶段。通过维护会话状态，状态检测防火墙可以对相关的数据包进行更精细的控制和审查。

简而言之，数据包过滤防火墙主要基于单个数据包的信息进行过滤和控制，而状态检测防火墙则维护并追踪会话状态，并根据会话状态对数据包进行控制。

5、基于公钥加密的两种不同的密钥分发方法是什么？

答：第一种方法是证书颁发机构签发的证书。在这种方法中，公钥由 CA 进行认证，并将其与实体的身份相关联。实体向 CA 提供公钥的证明，并通过数字签名保证证书的完整性。其他实体可以使用 CA 的公钥验证证书的有效性，并使用证书中的公钥进行加密和认证。

第二种方法是密钥交换协议，在这种方法中，通信双方通过协商生成共享的对称密钥，而无需事先共享公钥，允许两个实体在不直接传输密钥的情况下生成共享密钥。生成的共享密钥可以用于对称加密算法进行加密和解密。