第11章课后作业参考解答

1、在PGP中，发送方执行签名、加密、压缩操作的顺序是什么？为什么要按这样的顺序进行？

答：对未压缩的邮件正文进行散列计算后，再对散列值进行签名。然后将邮件正文和签名拼接后进行压缩后加密。

在压缩之前进行签名的主要原因有两点：一是对没压缩的消息进行签名，可便于对签名的验证，如果在压缩后再签名，则需要保存压缩后的消息或在验证时重新压缩消息，增加了处理的工作量；二是由于压缩算法ZIP在不同的实现中会在运算速度和压缩率之间寻求平衡，因而可能会产生不同的压缩结果（当然，直接解压结果是相同的），因此压缩后再进行签名就可能导致无法实现鉴别（接收方在验证签名时可能会因压缩的原因而出现验证失败）。

PGP对加密前的明文（含签名）进行压缩，而不是在加密后再压缩的主要原因也有两点：一方面因为先压缩再加密方案缩短了报文大小，从而减少了网络传输时间和存储空间；另一方面经过压缩实际上是经过了一次变换，变换后减少了明文中上下文的关系，比原始消息的冗余信息更少，再加密的安全性更高，而如果先加密，再压缩，效果会差一些。

2、在密钥信任方面，X.509和PGP有什么不同？

答：PGP主要采用以用户为中心的信任模型，也就是信任网模型（Web of Trust）。该模型中，没有一个统一的认证中心来管理用户公钥，每个人都可以作为一个CA对某个用户的公钥签名，以此来说明这个公钥是否有效（可信）。而X.509是基于一个统一的认证中心（CA）来建立密钥的信任关系。

3、PGP为什么要对加密后的报文进行Base64编码？并分析编码对传输性能的影响。

答：加密后的报文使用Base64编码将报文转换成ASCII字符串，主要考虑到很多文件系统只允许使用ASCII字符组成的报文，所以需要对密文进行Base64编码。在实际应用中，使用Base64编码转换后将导致消息大小增加33%（每3个字节的二进制数据映射成4个ASCIII字符）。由于加密前对消息进行了压缩，因此实际的性能下降幅度要小很多。

4、PGP是如何交换会话密码的？这种交换密钥方式与前面学过哪种协议类似？

答：

PGP系统中发送方产生会话密钥，并用接收方的公钥加密会话密钥，与密文拼接后一起发送给接收方；接收方用自己的私钥解密加密的会话密钥，获得会话密钥。与前面学到的SSL/TLS所采用的方法一样。