2020.11.16课后作业

B18030825 殷祥

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？

先对明文数据的摘要值进行签名，然后将明文与签名进行拼接，再对拼接后的数据进行压缩，最后用会话密钥对压缩后的数据进行加密。

如果先加密再压缩的话，加密后的数据随机性很大，压缩效果会很差，所以需要先压缩再加密。

2、在密钥信任方面，X.509和PGP有什么不同？

X.509的认证机制依赖于层次结构的证书认证机构，所有下一级的组织和个人的证书由上一级的组织负责认证，整个信任关系基本是树状结构，即Tree of Trust。

而PGP则无需这些外部约束，每个人自行决定信任谁，整个信任关系是网状结构，即Web of Trust。

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。

Base64编码的原因在于：加密后的字节流中存在很多非可见字符，为了提供文件应用的透明性，所以需要对报文base64编码成可见的ascii字符。

使用base64编码将导致整个消息大小增加33%，但好在可以通过压缩来补偿base64编码转换导致的膨胀。

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的改进的S/KEY协议（教材8.2.3节）中的会话密钥交换方法是类似吗？

先生成随机的会话密钥，然后用收件人的公钥对该会话密钥进行（非对称）加密，并将加密结果作为报文的一部分发送给收件人；收件人拿到报文后，使用自己的私钥对该加密结果进行解密就能得到会话密钥。

不一样，PGP的会话密钥交换方法是通过电子信封的方式交换的，而S/KEY协议则是一次性口令。