第八章答案

R1. 报文机密性和报文完整性之间的区别是什么？你能具有机密性而没有完整性吗？你能具有完整性而没有机密性吗？证实你的答案。

机密性是攻击者截获原始明文消息的密文加密后无法确定原始明文消息的属性。消息完整性是接收方可以检测发送的消息(无论是否加密)在传输过程中是否被更改的属性。

因此，这两者是不同的概念。在传输中更改的加密消息可能仍然是机密的(攻击者无法确定原始明文)，但是如果未检测到错误，则不会具有消息完整性。同样，在传输(和检测)过程中被修改的消息可能是明文发送的，因此不会是机密的。

R3. 从服务的角度，对称密钥系统和公开密钥系统之间一个重要的差异是什么？

对称密钥系统和公开密钥系统之间的一个重要区别是，在对称密钥系统中，发送方和接收方必须知道相同的(秘密)密钥。在公开密钥系统中，加密和解密密钥是不同的。全世界(包括发送方)都知道加密密钥，但是只有接收方知道解密密钥。

R13. 公钥加密的报文散列以何种方式比使用公钥加密报文提供更好的数字签名？

公钥签名的消息摘要“更好”，因为只需要加密(使用私钥)短消息摘要，而不需要加密整个消息。由于使用 RSA 这样的技术进行公钥加密的开销很大，因此需要对少量数据进行签名(加密)，而不是对大量数据进行签名。

R14. 假设 certifier. com 生成一个用于 foo. com 的证书。通常整个证书将用 certifier. com 的公钥加密。这种说法是正确还是错误？

错误。为了创建证书，certifier.com 将包含一个数字签名，它是 foo.com 信息的散列(包括其公钥)，并用 certifier.com 的私钥进行签名。

R16. 在某端点鉴别协议中，使用不重数的目的是什么？

使用不重数的目的是防御回放攻击。

P8. 考虑具有 $p=5$ 和 $q=11$ 的 RSA。

a. n 和 z 是什么？

b. 令 e 为 3。为什么这是一个对 e 的可接受的选择？

c. 求 d 使得 $de=1 \pmod z$ 和 $d<160$。

d. 使用密钥（n，e）加密报文 $m=8$。令 c 表示对应的密文。显示所有工作。提示：为了简化计算使用如下事实。

$$[(a \bmod n)\cdot(b \bmod n)] \bmod n = (a\cdot b) \bmod n$$

p =5 , q = 11

a) n = p*q = 55, z = (p 1)(q 1) = 40

b) e = 3 因为 e<n,并且与 z 没有公因数

c) d = 27

d) m = 8, m^e =512 ,密文 $c = m^e \bmod n = 17$

P17. 图 8-19 显示了 Alice 必须执行 PGP 的操作，以提供机密性、鉴别和完整性。图示出当 Bob 接收来自 Alice 的包时必须执行的对应操作。