没有机密性吗？证实你的答案。

R2. 因特网实体（路由器、交换机、DNS 服务器、Web 服务器、用户端系统等）经常需要安全通信。给出三个特定的因特网实体对的例子，它们要安全通信。

8.2 节

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？

R4. 假定某入侵者拥有一个加密报文以及该报文的解密版本。这个入侵者能够发起已知密文攻击、已知明文攻击和选择明文攻击吗？

R5. 考虑一个 8 块密码。这个密码有多少种可能的输入块？有多少种可能的映射？如果我们将每种映射视为一个密钥，则该密码具有多少种可能的密钥？

R6. 假定 N 个人中的每个人都和其他 $N-1$ 个人使用对称密钥密码通信。任两人（i 和 j）之间的所有通信对该 N 个人的组中的所有其他人都是可见的，且该组中的其他人都不应当能够解密他们的通信。则这个系统总共需要多少个密钥？现在假定使用公开密钥密码。此时需要多少个密钥？

R7. 假定 $n=10\,000$、$a=10\,023$ 和 $b=10\,004$。请你使用等同的模算术来心算 $(a \cdot b) \bmod n$。

R8. 假设你要通过加密对应于报文 1010111 的十进制数来加密该报文。该十进制数是什么？

8.3 ~ 8.4 节

R9. 散列以何种方式提供比检验和（如因特网检验和）更好的报文完整性检验？

R10. 你能够“解密”某报文的散列来得到初始报文吗？解释你的答案。

R11. 考虑 MAC 算法（图 8-9）的一种变形算法，其中发送方发送 $(m, H(m)+s)$，这里 $H(m)+s$ 是 $H(m)$ 和 s 的级联。该变形算法有缺陷吗？为什么？

R12. 一个签名的文档是可鉴别的和不可伪造的，其含义是什么？

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？

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？

R15. 假设 Alice 有一个准备发送给任何请求者的报文。数以千计的人要获得 Alice 的报文，但每个人都要确保该报文的完整性。在这种场景下，你认为是基于 MAC 还是基于数字签名的完整性方案更为适合？为什么？

R16. 在某端点鉴别协议中，使用不重数的目的是什么？

R17. 我们说一个不重数是一个在生存期中只使用一次的值，这意味着什么？其中是指谁的生存期？

R18. 基于 HMAC 的报文完整性方案易受重放攻击影响吗？如果是，能够在方案中综合一个不重数来去除这种脆弱性吗？

8.5 ~ 8.8 节

R19. 假定 Bob 从 Alice 处接收一个 PGP 报文。Bob 怎样才能确定 Alice（而不是如 Trudy）生成了该报文？PGP 为保证报文完整性使用了 MAC 吗？

R20. 在 SSL 记录中，有一个字段用于 SSL 序号。这种说法是正确还是错误？

R21. 在 SSL 握手中随机不重数的目的是什么？

R22. 假设某 SSL 会话应用了具有 CBC 的块密码。服务器以明文向客户发送了 IV。这种说法是正确还是错误？

R23. 假设 Bob 向 Trudy 发起一条 TCP 连接，而 Trudy 正在伪装她是 Alice。在握手期间，Trudy 向 Bob 发送 Alice 的证书。在 SSL 握手算法的哪一步，Bob 将发现他没有与 Alice 通信？

R24. 考虑使用 IPsec 从主机 A 向主机 B 发送分组流。通常，为该流中的每个发送分组将创建一个新 SA。这种说法是正确还是错误？

R25. 假设在图 8-28 中总部和分支机构之间通过 IPsec 运行 TCP。如果 TCP 重新传输相同的分组，则由 R1 发送的两个对应的分组将在 ESP 首部中具有相同的序号。这种说法是正确还是错误？