密钥。该 DH 算法利用一个大素数 p 和另一个小于 p 的大数 g。p 和 g 都是公开的（因此攻击者将知道它们）。在 DH 中，Alice 和 Bob 每人分别独立地选择秘密密钥 S_A 和 S_B。Alice 则通过将 g 提高到 S_A 并以 p 为模来计算她的公钥 T_A。类似地，Bob 则通过将 g 提高到 S_B 并以 p 为模来计算他的公钥 T_B。此后 Alice 和 Bob 经过因特网交换他们的公钥。Alice 则通过将 T_B 提高到 S_A 并以 p 为模来计算出共享密钥 S。类似地，Bob 则通过将 T_A 提高到 S_B 并以 p 为模来计算出共享密钥 S'。

a. 证明在一般情况下，Alice 和 Bob 得到相同的对称密钥，即证明 $S = S'$。

b. 对于 $p = 11$ 和 $g = 2$，假定 Alice 和 Bob 分别选择私钥 $S_A = 5$ 和 $S_B = 12$，计算 Alice 和 Bob 的公钥 T_A 和 T_B。显示所有计算过程。

c. 接着（b），现在计算共享对称密钥 S。显示所有计算过程。

d. 提供一个时序图，显示 Diffie-Hellman 是如何能够受到中间人攻击的。该时序图应当具有 3 条垂直线，分别对应 Alice、Bob 和攻击者 Trudy。

P10. 假定 Alice 要与采用对称密钥密码体制的 Bob 使用一个会话密钥 K_S 通信。在 8.2 节中，我们知道了如何使用公开密钥密码从 Alice 向 Bob 分发该会话密钥。在本习题中，我们探讨不使用公开密钥密码而使用一个密钥分发中心（KDC）分发会话密钥的方法。KDC 是一个与每个注册用户共享独特的秘密对称密钥的服务器。对于 Alice 和 Bob 而言，$K_{A\text{-}KDC}$ 和 $K_{B\text{-}KDC}$ 表示了这些密钥。设计一个使用 KDC 向 Alice 和 Bob 分发 K_S 的方案。你的方案应当使用三种报文来分发会话密钥：一种从 Alice 到 KDC 的报文；一种从 KDC 到 Alice 的报文；最后一种是从 Alice 到 Bob 的报文。第一种报文为 $K_{A\text{-}KDC}(A, B)$。使用标记 $K_{A\text{-}KDC}$、$K_{B\text{-}KDC}$、S、A 和 B 回答下列问题。

a. 第二种报文是什么？

b. 第三种报文是什么？

P11. 计算一个不同于图 8-8 中的两个报文的第三个报文，使该报文具有与图 8-8 中的报文相同的检验和。

P12. 假定 Alice 和 Bob 共享两个秘密密钥：一个鉴别密钥 S_1 和一个对称加密密钥 S_2。扩充图 8-9，使之提供完整性和机密性。

P13. 在 BitTorrent P2P 文件分发协议中（参见第 2 章），种子将文件分割为块，并且对等方彼此重分发这些块。不使用任何保护，一个攻击者能够容易地通过假冒善意的对等方并向洪流中的一部分对等方发送假冒块来实施破坏。这些未被怀疑的对等方则重新向其他对等方发送这些假冒块，其他对等方则将再次向甚至更多的对等方重新分发这些假冒块。因此，对于 BitTorrent 来说，采用一种机制使对等方能验证一个块的完整性，从而使得假冒块无法分发，这是至关重要的。假设当某对等方加入一个洪流时，它初始从一个完全受信任的源得到一个 .torrent 文件。描述允许对等方验证块完整性的一个简单的方案。

P14. OSPF 路由选择协议使用一个 MAC 而不是数字签名来提供报文完整性。你认为选择 MAC 而未选择数字签名的原因是什么？

P15. 考虑图 8-18 中的鉴别协议，其中 Alice 向 Bob 鉴别她自己，我们看来工作正常（即我们没有发现其中有缺陷）。现在假定当 Alice 向 Bob 鉴别她自己的同时，Bob 必须向 Alice 鉴别他自己。给出一个情况，此时 Trudy 假装是 Alice，向 Bob 鉴别她自己是Alice。（提示：该协议运行的顺序，鉴别过程可由 Trudy 或 Bob 发起，能够任意地交织在一起。特别注意 Bob 和 Alice 将使用不重数这样一个事实，如果不小心的话，能够恶意地使用相同的不重数。）

P16. 一个自然的问题是我们能否使用一个不重数的公钥密码来解决 8.4 节中的端点鉴别问题。考虑下列自然的协议：①Alice 向 Bob 发送报文“I am Alice”；②Bob 选择一个不重数并将其发送给 Alice；③Alice使用她的私钥来加密该不重数并向 Bob 发送得到的值；④Bob 对接收到的报文应用 Alice 的公钥。因此，Bob 计算 R 并鉴别了 Alice。

a. 画图表示这个协议，使用本书中应用的公钥和私钥的标记法。

b. 假定未使用证书。描述 Trudy 怎样能够通过拦截 Alice 的报文，进而对 Bob 假装她是 Alice 而成为一名“中间人”。