8、考虑如下协议：

A->KDC: $\mathrm{ID_A} \| \mathrm{ID_B} \| \mathrm{N_1}$

KDC->A: $\mathrm{E}(\mathrm{K_a}, [K_s \| ID_B \| N_1 \| E(K_b, [K_S \| \mathrm{ID}_A])])$

A->B: $\mathrm{E}(K_b, [K_S \| ID_A])$

B->A: $\mathrm{E}(K_S, N_2)$

A->B: $\mathrm{E}(K_S, f(N_2))$

A）解释这个协议。
B）你能给出可能的攻击吗？解释它是如何完成的。
C）提出一个可能的技术躲开那种攻击，只需提供基本思路。

答：A）A 与 B 向 KDC 申请会话密钥 Ks，用于 A、B 通信。

B) 如果某人得到一个旧的 Ks，他就可以在第三步重放攻击 B，第四步截获握手，第五步冒充 A 使 B 相信他与 A 通信

C) 增加时间戳

【注：这到题目考察的是信息安全导论对称密钥认证协议的 KDC 的过程和存在的漏洞。书中有比较详细的解释，注意掌握。】

9、考虑下面的 Web 安全威胁，并说明如何通过 SSL 的相应特性来防止每一种威胁？

a．穷举密码分析攻击：对传统加密算法密钥空间完全搜索。

b．已知明文字典攻击：很多消息包含一些可预知的明文，例如 HTTP GET。攻击者首先构建一个用不用密钥加密明文消息后得到所有可能的加密密文字典。当截获到加密消息时，攻击者就从该字典中查找这些明文所对应的密文以及相应的密钥。收到的密文应该从字典中相同密钥下得某个密文相匹配。如果发现多个匹配的情况，则可以对每一种进行全密文尝试，以发现正确的加密算法。这种攻击对于密钥较小的算法特别有效（例如 40 比特的密钥）

c．重放攻击：先前的 SSL 握手消息被重放

d．中间人攻击：攻击者在密钥交换过程中，应对服务器时冒充客户端，应对客户端时冒充服务器

e．口令窃听：HTTP 数据流或者其他应用数据流中传输的口令被窃听。

f．IP 地址假冒：使用伪造的 IP 地址欺骗主机接收的伪造数据。

g．IP 劫持：中断两个主机间活动的，经过认证的连接，攻击者代替一方的主机进行通信。

h．SYN 洪泛：通过半开连接攻击 TCP。

答：a）SSL 加密算法使用 40~128 比特密钥。

b）SSL 并不会真正使用 40bit 密钥，而是会构造成 128bit 密钥，剩余密钥有 Hello message 报文中来

c）随机数

d）用公钥证书认证。

e）数据加密

f）欺骗者必须拥有密钥与伪造的 IP 地址

g）加密数据进行保护

h）SSL 没有对 SYN 洪泛进行相应保护

【注：SSL 和 IPSec 协议正是对原本的 IP 协议的升级以应对 IP 协议的不足。是信息安全导论中最重要的一部分。这道题目给出了可能会被用于攻击的手段，目的是在攻击者的角度看待 IP 协议的不足，也从侧面反映了 SSL 和 IPSec 两者使用了什么样的手段修复 IP 协议漏洞，如重放攻击，IPSec 就使用了抗重放窗口来防止重放攻击的实施。以此用来加深对安全协议的理解，让我们清楚其协议设计的目的。】