R26. IKE SA 和 IPsec SA 是相同的东西。这种说法是正确还是错误?

R27. 考虑 802.11 的 WEP。假定数据是 10101100 并且密钥流是 11110000。相应的密文是什么?

R28. 在 WEP 中，在每个帧中以明文发送 IV。这种说法是正确还是错误?

8.9 节

R29. 状态分组过滤器维护两个数据结构。给出它们的名字并简单地讨论它们做些什么。

R30. 考虑某传统的（无状态的）分组过滤器。该分组过滤器可能基于 TCP 标志位以及其他首部字段过滤分组。这种说法是正确还是错误?

R31. 在传统的分组过滤器中，每个接口能够具有自己的访问控制表。这种说法是正确还是错误?

R32. 为什么应用程序网关必须与分组过滤器协同工作才能有效?

R33. 基于特征的 IDS 和 IPS 检查 TCP 和 UDP 报文段的载荷。这种说法是正确还是错误?

习题

P1. 使用图 8-3 中的单码代替密码，加密报文“This is an easy problem”，并解密报文“rmij'u uamu xyj”。

P2. Trudy 使用了已知明文攻击，其中她知道了 7 个字母的（密文，明文）转换对，减少了 8.2.1 节的例子中将被检查的大约 10^9 数量级的可能替换的数量。请说明之。

P3. 考虑图 8-4 所示的多码代替密码系统。利用报文“The quick brown fox jumps over the lazy dogs”得到的明文编码，选择明文攻击足以破解所有报文吗? 为什么?

P4. 考虑图 8-5 中显示的块密码。假设每个块密码 T_i 只是反转了 8 个输入比特的次序（例如，使得 11110000 变为 00001111）。进一步假设 64 比特置乱函数不修改任何比特（使得第 m 个比特的输出值等于第 m 个比特的输入值）。

a. 对于 $n=3$ 和初始 64 比特输入等于 10100000 重复了 8 次，输出的值是多少?

b. 重复（a），但此时将初始 64 比特的最后一个比特从 0 变为 1。

c. 重复（a）和（b），但此时假定 64 比特的置乱函数反转了 64 比特的次序。

P5. 考虑图 8-5 中的块密码。对于给定的“密钥”，Alice 和 Bob 将需要 8 个表，每张表 8 比特乘以 8 比特。对于 Alice（或 Bob）来说，要存储所有 8 张表，将需要多少比特的存储器? 这个数如何与一个全表 64 比特的块密码所需的比特数进行比较?

P6. 考虑在表 8-1 中的 3 比特块密码。假定明文是 100100100。

a. 初始假设未使用 CBC。生成的密文是什么?

b. 假设 Trudy 嗅探该密文。假设她知道正在应用无 CBC 的一个 3 比特块密码（但不知道特定的密码），她能够推测到什么?

c. 现在假设使用 CBC，其中 IV = 111。产生的密文是什么?

P7. 如题：

a. 使用 RSA，选择 $p=3$ 和 $q=11$，采用对每个字母独立地加密的方法加密短语“dog”。对已加密报文应用解密算法恢复出原报文。

b. 重复（a），而此时加密“dog”作为一个报文 m。

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。

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

P9. 在这个习题中，我们探讨 Diffie-Hellman(DH) 公钥加密算法，该算法允许两个实体协商一个共享的