第五章作业参考答案

1．6.1.3 节的数据认证算法是由 CBC 模式的 DES 定义的，其中初始向量取为 0，试说明使用 CFB 模式也可获得相同的结果。

解：设需认证的数据分为 64 比特长的分组，$D_1,D_2,\ldots,D_N$，其中 D_N 不够 64 比特则右边补 0，

由题设，数据认证算法相当于在 CBC 模式中初始向量取为 0，并按如下关系进行：

$O_1=E_K(D_1\oplus 0)$； $O_2=E_K(D_2\oplus O_1)$；… $O_N=E_K(D_N\oplus O_{N-1})$；

数据认证码取为 O_N 或 O_N 的最左 M 个比特

对于同样的认证数据序列，$D_1,D_2,\ldots,D_N$，使用 DES 的 CFB 模式，且取 $j=64$，IV=D_1，并从 D_2 开始加密得

$C_1=E_K(D_1)\oplus D_2=O_1\oplus D_2$，$C_2=E_K(C_1)\oplus D_3=E_K(O_1\oplus D_2)\oplus D_3=O_2\oplus D_3$，

由此可推出，对最后一个分组 D_N 加密后的密文 $C_{N-1}=O_{N-1}\oplus D_N$，则此时将 CFB 模式再进行一步，在该步中只计算 DES 的输出，则该输出值为 $E_K(C_{N-1})=E_K(O_{N-1}\oplus D_N)=O_N$。

所以可获得相同的结果。

2．有很多杂凑函数是由 CBC 模式的分组加密技术构造的，其中的密钥取为消息分组。例如将消息 M 分成分组 $M_1,M_2,\ldots,M_N$，H_0=初值，迭代关系为 $H_i=E_{Mi}(H_{i-1})\oplus H_{i-1}(i=1,2,\ldots,N)$，杂凑值取为 H_N，其中 E 是分组加密算法。

(1)设 E 为 DES，第 3 章习题 1 已证明如果对明文分组和加密密钥都逐比特取补，那么得到的密文也是原密文的逐比特取补，即如果 $Y=\mathrm{DES}_K(X)$则 $Y'=\mathrm{DES}_{K'}(X')$。利用这一结论证明在上述杂凑函数中可对消息进行修改但却保持杂凑值不变。

证：由 DES 的取反特性，如果令 M_i 和 H_{i-1} 取反，则有

$E_{M'i}(H'_{i-1})\oplus H'_{i-1}=[E_{Mi}(H_{i-1})]'\oplus H'_{i-1}=E_{Mi}(H_{i-1})\oplus H_{i-1}=H_i$

因此对任意的初始值 H_0，如果将 H_0 取反且将第一个消息分组 M_1 也取反则杂凑值不变

(2)若迭代关系改为 $H_i=E_{Hi-1}(M_i)\oplus M_i$，证明仍可对其进行上述攻击。

证：与(1)同，略。

3．考虑公钥加密算法构造杂凑函数，设算法是 RSA，将消息分组后用公开钥加密第一个分组，加密结果与第二个分组异或后，再对其加密，一直进行下去。设一消息被分成两个分组 B_1 和 B_2，其杂凑值为 $\mathrm{H}(B_1,B_2)=\mathrm{RSA}(\mathrm{RSA}(B_1)\oplus B_2)$。证明对任一分组 C_1 可选 C_2，使得 $\mathrm{H}(B_1,B_2)=\mathrm{H}(C_1,C_2)$，证明这种攻击方法，可攻击上述用公钥加密算法构造的杂凑函数。

证：攻击值如果获得两个消息分组 B_1 和 B_2，及其杂凑值 $\mathrm{H}(B_1,B_2)$，则攻击者可任选分组 C_1 并令 $C_2=\mathrm{RSA}(B_1)\oplus B_2\oplus\mathrm{RSA}(C_1)$

于是有 $\mathrm{H}(C_1,C_2)=\mathrm{RSA}(\mathrm{RSA}(C_1)\oplus(\mathrm{RSA}(B_1)\oplus B_2\oplus\mathrm{RSA}(C_1)))=\mathrm{RSA}(\mathrm{RSA}(B_1)\oplus B_2)=\mathrm{H}(B_1,B_2)$则攻击成功。

6．设 $a_1a_2a_3a_4$ 是 32 比特长的字中的 4 个字节，每一 a_i 可看作由二进制表示的 0 到 255 之间的整数，在 big－endian 结构中该字表示整数 $a_12^{24}+a_22^{16}+a_32^8+a_4$，在 little-endian 结构中该字表示整数 $a_42^{24}+a_32^{16}+a_22^8+a_1$。

(1)用 MD5 使用 little－endian 结构，因消息的摘要值不应依赖于算法所用的结构，因此在 MD5 中为了对以 big－endian 结构存储的两个字 $X=x_1x_2x_3x_4$ 和 $Y=y_1y_2y_3y_4$，进行模 2^{32} 加运算，必须对这两个字进行调整，试说明如何调整？

解：首先对 X 中的 4 个字节做如下处理：

将 x_1 和 x_4 交换，x_2 和 x_3 交换，对 Y 进行相同的处理

然后计算 $Z=X+Y \bmod 2^{32}$

最后再将 z_1 和 z_4 交换，z_2 和 z_3 交换。