# Problem 1

在原密文$ABCBABBBAC$中，出现了2个相同的密文$AB$，距离为4，因此可以猜测，密钥长度应为4的因子，故密钥长度不可能为3，密钥长度只可能是1或2。

当密钥长度为1时，原密文划分为$A|B|C|B|A|B|B|B|A|C$，而密文中$A:B:C=3:5:2$。因为密钥长度为1，因此$A$、$B$、$C$也只能解密成不同的字母，故无法满足$A:B:C=7:2:1$。因此密钥长度不可能是1,只可能是2。

当密钥长度为2时，假设密钥对应的编号为$\alpha\beta$，原密文解密后的序列为：
$(-\alpha)\%3\ (1-\beta)\%3|(2-\alpha)\%3\ (1-\beta)\%3|(-\alpha)\%3\ (1-\beta)\%3|(1-\alpha)\%3\ (1-\beta)\%3|(-\alpha)\%3\ (2-\beta)\%3$

经统计：

有4个$(1-\beta)\%3$、3个$(-\alpha\%3)$、1个$(2-\alpha)\%3$、1个$(2-\beta)\%3$和1个$(1-\alpha)\%3$。

又因为原文中$A:B:C=7:2:1$，因此$(1-\beta)\%3=(-\alpha)\%3=0$，解得$\alpha=0,\beta=1$。将$\alpha=0,\beta=1$代入到$(2-\alpha)\%3$、$(2-\beta)\%3$和$(1-\alpha)\%3$中得$(2-\alpha)\%3=2$、$(2-\beta)\%3=1$和$(1-\alpha)\%3=1$，确实满足$A:B:C=7:2:1$。因此最可能的密钥为$AB(01)$。

# Problem 2

## 1.

对$Perfect\ secrecy$有$Pr[M=m|C=c]=Pr[M=m]$，而
$Pr[M=m|C=c]=\frac{Pr[(M=m)\wedge(C=c)]}{Pr[C=c]}=Pr[M=m]$，因此有
$Pr[(M=m)\wedge(C=c)]=Pr[M=m]Pr[C=c]$。

所以$Pr[C=c|M=m]=\frac{Pr[(C=c)\wedge(M=m)]}{Pr[M=m]}=\frac{Pr[C=c]Pr[M=m]}{Pr[M=m]}=Pr[C=c]$。

## 2.

- 第一个攻击者：

设第一个攻击者猜测$M=0$的概率为$p'$，猜测$M=1$的概率为$p''$。因为第一个攻击者是随机猜测的，因此$p'=p''=0.5$。故第一个攻击者猜测正确的概率为$p_{success}=p_0*p'+p_1*p''=0.5*(p_0+p_1)$，又因为$p_0+p_1=1$，因此$p_{success}=0.5$。

- 第二个攻击者：

由于明文取0或1这一事件与密钥取0或1这一事件是相互独立的，故有：
$p(M=0,K=0)=p(M=0)p(K=0)=0.4p_0$

$p(M=1,K=0)=p(M=1)p(K=0)=0.4p_1$

$p(M=0,K=1)=p(M=0)p(K=1)=0.6p_0$

$p(M=1,K=1)=p(M=1)p(K=1)=0.6p_1$

故可以得到对应的密文取值的概率：

$p(C=0)=p(M=0,K=0)+p(M=1,K=1)=0.4p_0+0.6p_1$

$p(C=1)=p(M=1,K=0)+p(M=1,K=0)=0.4p_1+0.6p_0$

可以得到明文与密文取值的联合概率：
$p(M=0,C=0)=p(M=0,K=0)=0.4p_0$

$p(M=0,C=1)=p(M=0,K=1)=0.6p_0$

$p(M=1,C=0)=p(M=1,K=1)=0.6p_1$

$p(M=1,C=1)=p(M=1,K=0)=0.4p_1$

故有密文和明文取值的条件概率：
$p(M=0|C=0)=\frac{p(M=0,C=0)}{p(C=0)}=\frac{0.4p_0}{0.4p_0+0.6p_1}$

$p(M=0|C=1)=\frac{p(M=0,C=1)}{p(C=1)}=\frac{0.6p_0}{0.4p_1+0.6p_0}$

$p(M=1|C=0)=\frac{p(M=1,C=0)}{p(C=0)}=\frac{0.6p_1}{0.4p_0+0.6p_1}$

$p(M=1|C=1)=\frac{p(M=1,C=1)}{p(C=1)}=\frac{0.4p_1}{0.4p_1+0.6p_0}$

因此，当$C$、$p_0$、$p_1$满足以下条件时，对$M$进行以下猜测：

- 当$p_1>\frac{3}{2}p_0$时，猜测$M=1$。
- 当$\frac{2}{3}p_0<p_1<\frac{3}{2}p_0$且$C=0$时，猜测$M=0$。
- 当$\frac{2}{3}p_0<p_1<\frac{3}{2}p_0$且$C=1$时，猜测$M=1$。
- 当$p_1<\frac{2}{3}p_0$时，猜测$M=0$。

# Problem 3

- 破解$DESV$

设两对不同的明文-密文对$<M_1,C_1>$和$<M_2,C_2>$，有：$C_1=DES_k(M_1)\bigoplus k_1$、$C_2=DES_k(M_2)\bigoplus k_1$。

两个式子异或得：
$C_1\bigoplus C_2=[DES_k(M_1)\bigoplus k_1]\bigoplus[DES_k(M_2)\bigoplus k_1]=DES_k(M_1)\bigoplus DES_k(M_2)$。

因为$M_1$、$M_2$、$C_1$、$C_2$均已知，因此可以遍历$k$来寻找满足$C_1\bigoplus C_2=DES_k(M_1)\bigoplus DES_k(M_2)$的$k$，需要$M_1 2^{56}$和$M_2 2^{56}$的时间，复杂度为$O(2^{56})$。

因为$k_1=C_1\bigoplus DES_k(M_1)=(DES_k(M_1)\bigoplus k_1)\bigoplus DES_k(M_1)$，因此共需要$2^{56}$的$DES$操作来破解$DESV$。

- 破解$DESW$

设两对不同的明文-密文对$<M_1,C_1>$和$<M_2,C_2>$，有$DES_k^{-1}(C_1)=M_1\bigoplus k_1$、$DES_k^{-1}(C_2)=M_2\bigoplus k_1$。

两个式子异或得：$DES_k^{-1}(C_1)\bigoplus DES_k^{-1}(C_2)=(M_1\bigoplus k_1)\bigoplus(M_2\bigoplus k_1)=M_1\bigoplus M_2$。

因为$M_1$、$M_2$、$C_1$、$C_2$均已知，因此可以遍历$k$来寻找满足$DES_k^{-1}(C_1)\bigoplus DES_k^{-1}(C_2)=M_1\bigoplus M_2$，需要$C_1 2^{56}$和$C_2 2^{56}$的时间，复杂度为$O(2^{56})$。

因为$k_1=M_1\bigoplus DES_k^{-1}(M_1)=M_1\bigoplus(M_1\bigoplus k_1)$，因此共需要$2^{56}$的$DES$操作来破解$DESW$。

# Problem 5

依题意有：

$C_0=E(K,M_0)\bigoplus IV$

$C_1=E(K,M_1)\bigoplus M_0$

$C_2=E(K,M_2)\bigoplus M_1$

因为$M_1=M_2=M$，因此替换上述三个式子中的$M_1$和$M_2$：

$C_0=E(K,M_0)\bigoplus IV$

$C_1 = E(K, M) \bigoplus M_0$

$C_2 = E(K, M) \bigoplus M$

将$C_1$和$C_2$进行异或得
$C_1 \bigoplus C_2 = (E(K, M) \bigoplus M_0) \bigoplus (E(K, M) \bigoplus M) = (E(K, M) \bigoplus E(K, M)) \bigoplus (M_0 \bigoplus M) = M_0 \bigoplus M$
。

而$C_1$、$C_2$和$M$均已知，因此可以根据$C_1 \bigoplus C_2 = M_0 \bigoplus M$来解出$M_0$。

# Problem 6

1. 具备单向性但不具备抗碰撞性的哈希函数

   $H(m) = m^2 + 1$

2. 具备碰撞性但不具备抗单向性的哈希函数

   $H(m) = m^3 + 1$