Computer and Network Security: Homework 1

18340013 陈琮昊

Solution1：

首先证明密钥长度可能为2：

当密钥长度为1时：

$$\begin{aligned} &\ \ ABCBABBBAC \\ &ABCBABBBAC \end{aligned}$$

可以看到有2个重合；

当密钥长度为2时：

$$\begin{aligned} &\ \ \ \ ABCBABBBAC \\ &ABCBABBBAC \end{aligned}$$

可以看到有3个重合；

当密钥长度为3时：

$$\begin{aligned} &\ \ \ \ \ \ ABCBABBBAC \\ &ABCBABBBAC \end{aligned}$$

可以看到有1个重合。

故密钥长度可能为2。

接下来再找最可能的密钥：

序号为奇数的密文中的字母有3个A、1个B和1个C，A的频率最高；序号为偶数的密文中的字母有4个B和1个C，B的频率最高。因此，最可能的密钥是AB。

Solution2:

1.证明：

$$Pr[C=c|M=m]=\frac{Pr[M=m|C=c]\cdot Pr[C=c]}{Pr[M=m]}=\frac{Pr[M=m]\cdot Pr[C=c]}{Pr[M=m]}=Pr[C=c]$$

2.设$M^{'}$为猜测:

对于第一个攻击者：

$$\begin{aligned} &Pr[(M^{'}=0\wedge M=0)\vee(M^{'}=1\wedge M=1)]=Pr[M^{'}=0\wedge M=0]+Pr[M^{'}=1\wedge M=1] \\ &=Pr[M^{'}=0]\cdot Pr[M=0]+Pr[M^{'}=1]\cdot Pr[M=1] \\ &=0.5p_0+0.5(1-p_0)=0.5 \end{aligned}$$

对于第二个攻击者：

$$
\begin{aligned}
&Pr[M=0|C=c]=\frac{Pr[M=0 \wedge C=c]}{Pr[C=c]}\\
&=\frac{Pr[M=0 \wedge M \bigoplus K=c]}{Pr[C=c \wedge (M=0 \vee M \neq 0)]}\\
&=\frac{Pr[M=0 \wedge K=c]}{Pr[(K=c \wedge M=0) \vee (K \neq c \wedge M \neq 0)]}\\
&=\frac{Pr[M=0] \cdot Pr[K=c]}{Pr[M=0] \cdot Pr[K=c]+Pr[M \neq 0] \cdot Pr[K \neq c]}\\
&=\frac{p_0 \cdot Pr[K=c]}{p_0 \cdot Pr[K=c]+(1-p_0) \cdot Pr[K \neq c]}\\
&=\begin{cases}\frac{0.4p_0}{0.4p_0+0.6(1-p_0)}=\frac{2p_0}{3-p_0}, c=0\\ \frac{0.6p_0}{0.6p_0+0.4(1-p_0)}=\frac{3p_0}{2+p_0}, c=1\end{cases}
\end{aligned}
$$

则当$c=0$时，$p_0 \geq \frac{3}{5}$时，根据最后的式子可以知道$Pr[M=0|C=c] \geq 0.5$，故估计$M'=0$，否则$M'=1$；当$c=1$时，$p_0 \geq \frac{2}{5}$时，根据最后的式子可以知道$Pr[M=0|C=c] \geq 0.5$，故估计$M'=0$，否则$M'=1$。

Solution3：

DESV：对于(M,C)枚举k，计算2^{56}次$DES_k(M)$，获得中间结果m_1。枚举k_1，计算2^{64}次$C \bigoplus k_1$，获得中间结果m_2，比对m_1和m_2，若相等则破解k和k_1，共2^{56}次DES运算。

DESW：对于(M,C)枚举k，计算2^{56}次$DES_k^{-1}(C)$，获得中间结果m_1。枚举k_1，计算2^{64}次$M \bigoplus k_1$，获得中间结果m_2，比对m_1和m_2，若相等则破解k和k_1，共2^{56}次DES运算。

Solution4:

$N=p \cdot q$,则根据欧拉函数的性质$\phi(N)=\phi(p) \cdot \phi(q)=(p-1)(q-1)$,且有$e_A \cdot d_A \equiv 1(mod \phi(n))$,由于Bob知道Alice的$(e_A,N)$,那么便可根据扩展欧几里得方法求出$e_A$的逆元$d_A$。

Solution5：

$$
\begin{gathered}
\text{由题目中的图可以得到：}\\
E(M_1,K) \bigoplus M_0=C_1\\
E(M_2,K) \bigoplus M_1=C_2\\
\text{将}M_1=M_2=M\text{代入得：}\\
E(M,K) \bigoplus M_0=C_1\\
E(M,K) \bigoplus M=C_2\\
\text{上面两式异或得：}\\
M_0 \bigoplus M=C_1 \bigoplus C_2\\
\text{则}M_0=C_1 \bigoplus C_2 \bigoplus M
\end{gathered}
$$

Solution6：

1.设h为函数:

$h(x)=\overline{0}$（其中$\overline{0}$表示0编码在n位上）

此函数显然是单向的，因为它将任何输入映射到相同的值0，但很明显，它不具有抗冲突性。

2.设g是一个抗冲突的散列函数，它将任意长度的输入映射到$n-1$位输出。假设函数h定义为:

$$
h(x)=\begin{cases}1||x, \text{如果}x\text{的长度为}n-1\\ 0||g(x), else.\end{cases}
$$

那么h是一个n位散列函数，它是抗冲突的，但不是单向的。