Computer and Network Security

Homework 1

20337025 崔璨明

Problem 1

密文ABCBABBBAC中，“AB”出现的位置为1，5，距离为4，”BA“出现的位置为4，8，距离为4，公因子为{4，2，1}，已知密钥长度为1/2/3，因此最有可能的密钥长度为2。

根据密钥的长度（2），将密文分为两组：

奇数：ACABAC

偶数：BBBBC

三个字母A, B, C的出现频率分别为0.7, 0.2和 0.1，在奇数序列中A出现次数为3，BC出现次数都为1，所以奇数序列中A的明文为A，而偶数序列中B出现次数为4，C出现次数为1，所以B的明文为A，综上，密钥为$(0,1)=(a,b)$

Problem 3

当使用DESV时：

对于两组不同的明文和秘文M1,C1,M2,C2，有：

$$C_1 = DES_k(M_1) \oplus k_1$$

$$C_2 = DES_k(M_2) \oplus k_1$$

$$C_1 \oplus C_2 = \{DES_k(M_1) \oplus k_1\} \oplus \{DES_k(M_2) \oplus k_1\} = DES_k(M_1) \oplus DES_k(M_2)$$

对于满足以上条件的密钥，可以进行brute-force key search，需要编码M1 2^{56} 和M2 2^{56}次，一旦找到k，就可以找到满足条件的k_1，总时间为2^{56} DES。

当使用DESW时：

$$DES_k^{-1}(C_1) = M_1 \oplus k_1$$

$$DES_k^{-1}(C_2) = M_2 \oplus k_1$$

$$DES_k^{-1}(C_1) \oplus DES_k^{-1}(C_2) = \{M_1 \oplus k_1\} \oplus \{M_2 \oplus k_1\} = M_1 \oplus M_2$$

进行brute-force key search，需要编码C_1 2^{56} 和C_2 2^{56}次，一旦找到k，就可以找到满足条件的k_1，总时间就是2^{56} DES。

Problem 4

Bob已知N，可以将N分解为两个质数P和Q：$P \times Q = N$，对于每一组P，Q，通过$\phi(N) = (P-1)(Q-1)$ 计算欧拉函数。因为已知公钥，所以只需要求解该公式便可以求得私钥：$e_A \times d_A \ \% \ \phi(N) = 1$，Bob可以使用扩展欧几里得算法来计算。

Problem 5

$C_2 = M_1 \oplus M_2^{'}$，而$M1 = M2 = M$，所以$C_2 = M \oplus M^{'}$，由此可以计算得到$M^{'}$。又因为$C_1 = M^{'} \oplus M0$，C_1已知，由此便可以得到M_0。

Problem 6

1. 具有单向性而不具有抗碰撞性：$H(x) = \sum_{i=1}^{n} x_i$，$x_i$为x的第i位
2. 具有抗碰撞性而不具有单向性：$H(x) = A(x) \mid\mid B(x)$，$A(x)$ 为抗碰撞性的函数，$B(x)$ 为x的最后256位