传统加密技术

1. 用 Vigenere 算法加密某明文，已知密钥是：zelda，加密所得密文为：AVPDTGSQWHDATOD，请问该密文对应的明文是？

答：将字母转化为对应数字，并根据解密公式$m_i = C_i - k_{i\,mod\,5}\ (mod\ 26)$，可得对应明文为：breath of the wild

2. 已知密码体制为普莱菲尔密码（Playfair Cipher），密钥为：davidbowie，明文为 ground control to major tom，请问该明文对应的密文为？

答：根据密钥可得密钥矩阵为：

$$\begin{bmatrix} d & a & v & i/j & b \\ o & w & e & c & f \\ g & h & k & l & m \\ n & p & q & r & s \\ t & u & x & y & z \end{bmatrix}$$

明文分为两个一组后为： gr ou nd co nt ro lt om aj or to mx

根据加密规则。密文为： ln wt to fw td nc gy fg vb cn dg kz

分组密码与 DES

给定比特串A，记$\bar{A}$为A的按位取反。证明以下有关 DES 算法的结论：

（1）如果$Y = DES_k(X)$，那么$\bar{Y} = DES_{\bar{k}}(\bar{X})$。其中，$X$为明文，$Y$为$X$经过 DES 加密得到的密文，$k$为密钥。(提示：对于任意的比特串 A 和 B，$\overline{\mathrm{A} \oplus \mathrm{B}} = \bar{\mathrm{A}} \oplus \mathrm{B}$)

(2)假设攻击者 Malice 可以进行选择明文攻击，获得X及$\bar{X}$的密文。若 Malice 对 DES 加密进行穷举攻击(Brute-force attack)，则可以根据（1）中的结论将搜索空间减半至2^{55}。

解答：

第一问：

（1）容易验证，DES 中的初始置换，逆初始置换，E 表代换，S 盒，P 盒均与互补性无关，即：

如果$\mathrm{N} = \mathrm{PO}(\mathrm{A})$，则$\overline{\mathrm{N}} = \mathrm{PO}(\overline{\mathrm{A}})$，$\mathrm{PO}$为某种置换/代换操作。

（2）根据子密钥生成规则，左循环移位得到的子密钥仍然是互补的，即：

如果 $\mathrm{KG}(\mathrm{K}) = (\mathrm{k}_1, \mathrm{k}_2, \ldots, \mathrm{k}_{16})$，则$\mathrm{KG}(\overline{\mathrm{K}}) = (\bar{\mathrm{k}}_1, \bar{\mathrm{k}}_2, \ldots, \bar{\mathrm{k}}_{16})$。

（3）由$\overline{\mathrm{A} \oplus \mathrm{B}} = \overline{\mathrm{A}} \oplus \mathrm{B}$可证$\mathrm{A} \oplus \mathrm{B} = \overline{\mathrm{A}} \oplus \overline{\mathrm{B}}$。

下面考虑 DES 加密的第i轮：

对于未取反的加密过程：

$$\begin{gathered} \mathrm{L_i} = \mathrm{R_{i-1}}, \\ \mathrm{R_i} = \mathrm{L_{i-1}} \oplus \mathrm{F}(\mathrm{R_{i-1}}, \mathrm{k_i}) \end{gathered}$$

对于取反后的加密过程：

$$\begin{gathered} \overline{\mathrm{L_i}} = \overline{\mathrm{R_{i-1}}}, \\ \overline{\mathrm{R_i}} = \overline{\mathrm{L_{i-1}}} \oplus \mathrm{F}(\overline{\mathrm{R_{i-1}}}, \overline{\mathrm{k_i}}) \end{gathered}$$

要证明 $Y = DES_k(X) \rightarrow \overline{Y} = DES_{\bar{k}}(\bar{X})$，

等价于证明 $\overline{\mathrm{L_{i-1}} \oplus \mathrm{F}(\mathrm{R_{i-1}}, \mathrm{k_i})} = \overline{\mathrm{L_{i-1}}} \oplus \mathrm{F}(\overline{\mathrm{R_{i-1}}}, \overline{\mathrm{k_i}})$ (*)

而根据$\overline{\mathrm{A} \oplus \mathrm{B}} = \overline{\mathrm{A}} \oplus \mathrm{B}$

$$\overline{L_{i-1} \oplus F(R_{i-1}, k_i)} = \overline{L_{i-1}} \oplus F(R_{i-1}, k_i)$$

所以要证(*)等价于证明

$$F(R_{i-1}, k_i) = F(\overline{R_{i-1}}, \overline{k_i}) \quad (**)$$

这里，F 函数可进一步写为

$$F(R, k) = P(S(E(R) \oplus k)),$$

则根据（1），要证(**)等价于证明

$$E(R_{i-1}) \oplus k_i = \overline{E(R_{i-1})} \oplus \overline{k_i}$$

根据（3），结论成立。

第二问：

根据按位取反的性质，原密钥搜索空间 K （|K|=2^{56}）可以分为 K1，K2 两部分，其中 K1 中的每一个元素按位取反后都能在 K2 中找到其对应，且 |K1|=|K2|=2^{55},K1∩K2=∅,K1∪K2=K。

根据此划分，只需要在 K1 中搜索密钥，对于 k∈K1，

如果$DES_k(X) = Y$，则 k 是密钥，

如果$DES_k(\bar{X}) = \bar{Y}$，则$\bar{k}$ 是密钥。

综上，搜索的密钥空间可减半至2^{55}。

有限域

1. **求有限域 $GF(2)$ 上多项式$\boldsymbol{f(x) = x^6 + x^4 + x^3 + 1}$，和$\boldsymbol{g(x) = x^4 + x^2 + 1}$的和$\boldsymbol{f(x) + g(x)}$与乘积$\boldsymbol{f(x)g(x)}$。**

和：$x^6 + x^3 + x^2$

乘积：$x^{10} + x^7 + x^5 + x^3 + x^2 + 1$

和：

$$
\begin{array}{r}
x^6 + x^4 + x^3 + 1 \\
+(x^4 + x^2 + 1) \\
\hline
x^6 + x^3 + x^2
\end{array}
$$

积：

$$
\begin{array}{r}
x^6 + x^4 + x^3 + 1 \\
\times(x^4 + x^2 + 1) \\
\hline
x^6 + x^4 + x^3 + 1 \\
x^8 + x^6 + x^5 + x^2 \\
x^{10} + x^8 + x^7 + x^4 \\
\hline
x^{10} + x^7 + x^5 + x^3 + x^2 + 1
\end{array}
$$

2. **求有限域$GF(2^8)$的不可约多项式为$p(x) = x^8 + x^4 + x^3 + x + 1$，求多项式$f(x) = x^6 + x^4 + x^3 + 1$和$g(x) = x^4 + x^2 + 1$在$GF(2^8)$下的乘积$f(x)g(x)$。**

答案：

$$
\begin{aligned}
f(x)g(x) &= (x^6 + x^4 + x^3 + 1)(x^4 + x^2 + 1) \\
&= (x^{10} + x^8 + x^7 + x^4) + (x^8 + x^6 + x^5 + x^2) + (x^6 + x^4 + x^3 + 1) \\
&= x^{10} + x^7 + x^5 + x^3 + x^2 + 1
\end{aligned}
$$

$$f(x)g(x)\ mod\ p(x) = x^7 + x^6 + 1$$