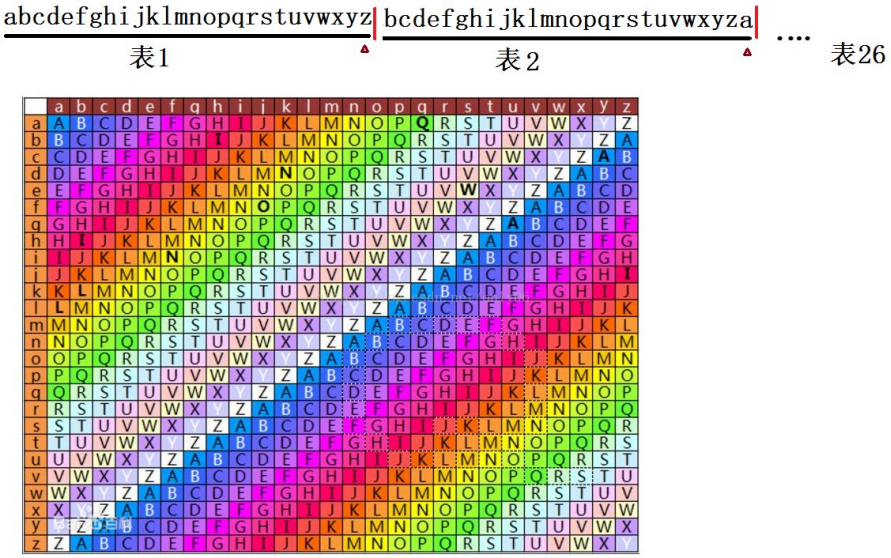
Vigenere 密码破解

1.Vigenere 密码

Vigenere 密码在单一恺撒密码的基础上扩展出多表密码，称为“维吉尼亚”密码。于 1586 年由法国密码学家 Blaise de Vigenere 发明。Vigenere 密码使用一个字符串作为密钥，字符串中的每一个字符都作为移位替换密码的密钥并确定一个替换表。（即确定了使用多表中的哪个表,即上述提到的 i 的作用）

在通常的 Vigenere 密码中，替换表由 26 个英文字母组成，为周期循环。若看成一维表，由于共 26 个字母，每个字母可做一个 i 指定一个替换表，即共 26 个替换表即本总密文表长度为 26*26。注意：Vigenere 密码的 26 个密码表，每个表相对前一个表发生一次左移。若看成二维表，则可能更容易对比。左侧的 a-z 为密钥，上方的为明文，由此(i,j)确定下此环境时的相应密文。可将 a-z 看做 0-26 更容易计算。



2.密文

KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
CWHJVLNHIQIBTKHJVNPIST

(1)使用 MATLAB 程序对密文进行 Kasiski 测试，查找出出现次数很高的密文

片段为：KFT、HJV，综合分析后可得出密钥长度为 6，因此可将密文分为 6 组。

```
sub_str: KFT    80    98    254
maxcd: 2
sub_str: HJV    108    126    264    318    330
maxcd: 6
```

(2)对每组密文进行频率统计，频率出现最高的字母最有可能对应 E。但是由于分组后密文较短（密文长度为 57），频率统计并不能得出明显的对应关系。因此对每组密文进行密钥穷举,过程如下：

(a)对于每一组密文,使用 A—Z 共 26 个密钥进行穷举,共得到6×26条明文。

(b)然后对每条明文进行频率统计得到P_i，并计算与自然语言P_j的互重合指数$MCI=\sum_{i=j=1}^{26}p_ip_j$。

(c)最后查找每个分组中使 MCI 值最大或接近 0.065 的的密钥，得到正确密钥为：CRYPTO。

```
分组 1      密钥 C      明文 3      MCI 0.064551
分组 2      密钥 R      明文 44     MCI 0.070476
分组 3      密钥 Y      明文 77     MCI 0.058709
分组 4      密钥 P      明文 94     MCI 0.065968
分组 5      密钥 T      明文 124    MCI 0.055784
分组 6      密钥 O      明文 145    MCI 0.070419
key为: CRYPTO
fx >>
```

3.明文

ILEARNEDHOWTOCALCULATETHEAMOUNTOFPAPERNEEDEDFORAROOMWHENIWASATSCHOOLY
OUMULTIPLYTHESQUAREFOOTAGEOFTHEWALLSBYTHECUBICCONTENTSOFTHEFLOORANDCE
ILINGCOMBINEDANDDOUBLEITYOUTHENALLOWHALFTHETOTALFOROPENINGSSUCHASWIND
OWSANDDOORSTHENYOUALLOWTHEOTHERHALFFORMATCHINGTHEPATTERNTHENYOUDOUBLE
THEWHOLETHINGAGAINTOGIVEAMARGINOFERRORANDTHENYOUORDERTHEPAPER