古典密码作业

1. 凯撒密码

phhw ph diwhu wkh wrjd sduwb

利用凯撒密码解密得到该密文对应的明文。

2. 仿射密码的频率 (统计) 分析

已知使用仿射密码加密一段明文得到密文: cqvjlvovqqtvoevvwshwbjmzrooevtzuhv, 请使用频率 (统计) 分析的方法解密该密文。

3. 希尔密码 (多表代换密码中 $\boldsymbol{C} = \boldsymbol{AM} + \boldsymbol{B}$, 其中 $\boldsymbol{B} = 0$ 的情况)

设希尔密码 $\boldsymbol{C_i} = \boldsymbol{AM_i} \pmod{26}$ 中, $\boldsymbol{A}$ 是二阶方阵, 又已知明文 dont 被加密为 elni, 求密钥矩阵 $\boldsymbol{A}$。

4. 仿射密码

设由仿射密码对一个明文加密得到的密文为:

edsgickxhuklzveqzvkxwkzukvcuh

又已知明文的前两个字符为 if, 请对该密文解密求得明文。

5. 置换密码+维吉尼亚密码

已知某密码的加密方法为: 先用置换密码对明文 $\boldsymbol{M}$ 加密, 再对该结果用维吉尼亚密码加密得到密文 $\boldsymbol{C}$。若置换密码使用的加密方式是:

密文字符位置	1	2	3	4	5	6
明文字符位置	3	5	1	2	4	6

维吉尼亚密码的加密密钥为三字母 AEF 周期地重复使用。

已知密文 $\boldsymbol{C}$ = vemaildytophtcpystnqzahj, 试求明文 $\boldsymbol{M}$。