古典密码作业答案

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。

解: 凯撒密码的加密公式为 $y = x+3 \bmod 26$, 即每个字母向前循环移动 3 位

对应的解密公式为 $x = y-3 \bmod 26$, 即每个字母向后循环移动 3 位

故该凯撒密码解密对应的明文为 meet me after the toga party

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。

解: 统计密文中个字母出现的频率, 其中出现频率最高的两个字母分别为 v 出现 8 次, o 出现 4 次, 故可假设 v 是 e 密文, o 是 t 的密文。

设该仿射密码的解密函数为 $x = k_1y + k_2 \bmod 26$, 这里 $k_1, k_2 \in [0, 25]$, 故可得方程组

$$\begin{cases} 4 = 21\ k_1+k_2 \bmod 26 \\ 19 = 14\ k_1+k_2 \bmod 26 \end{cases}$$

解的 $k_1 = 9, k_2 = 23$, 解密函数为 $x = 9y + 23 \bmod 26$, 相应的解密密文为:

please tell me the ending about the movie

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 $\boldsymbol{A}$。

解: 设 $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, 由于 dont 被加密为 elni, 则有 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 3 & 13 \\ 14 & 19 \end{bmatrix} = \begin{bmatrix} 4 & 13 \\ 11 & 8 \end{bmatrix} \bmod 26$

从而可得方程组 $\begin{cases} 4 =3a+14b \bmod 26 \\ 19 =13a+19b \bmod 26' \end{cases}$ $\begin{cases} 11 =3c+14d \bmod 26 \\ 8=13c+19d \bmod 26 \end{cases}$

解得 a = 10, b = 13, c = 9, d = 23, 故密钥矩阵 $A = \begin{bmatrix} 10 & 9 \\ 13 & 23 \end{bmatrix}$。

4. 仿射密码

设由仿射密码对一个明文加密得到的密文为:

edsgickxhuklzveqzvkxwkzukcvuh

又已知明文的前两个字符为 if, 请对该密文解密求得明文。

解: 设该仿射密码的解密方程为 $x = k_1y + k_2 \bmod 26$, 这里 $k_1, k_2 \in [0, 25]$。由 ed 解密为 if 可得方程组

$$\begin{cases} 8 = 4\,k_1 + k_2 \bmod 26 \\ 5 = 3\,k_1 + k_2 \bmod 26 \end{cases}$$

解得 $k_1 = 3, k_2 = 22$。故解密方程为 $x = 3y + 22 \bmod 26$。相应的明文为: if you can read this thank a teacher

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 ***M*** 加密, 再对该结果用维吉尼亚密码加密得到密文 ***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 ***C*** = vemaildytophtcpystnqzahj, 试求明文 ***M***。

解: 将密文 ***C*** 转换成数字为

v	e	m	a	i	l	d	y	t	o	p	h	t	c	p	y	s	t	n	q	z	a	h	j
21	4	12	0	8	11	3	24	19	14	15	7	19	2	15	24	18	19	13	16	25	0	7	9

将 ***C*** 周期性地使用维吉尼亚解密密钥 AEF (0 4 5) 解密得到

v	e	m	a	i	l	d	y	t	o	p	h	t	c	p	y	s	t	n	q	z	a	h	j
21	4	12	0	8	11	3	24	19	14	15	7	19	2	15	24	18	19	13	16	25	0	7	9
21	0	7	0	4	6	3	24	14	14	11	2	19	24	10	24	14	14	13	12	20	0	3	5

再进行置换密码的解密得到

v	e	m	a	i	l	d	y	t	o	p	h	t	c	p	y	s	t	n	q	z	a	h	j
21	4	12	0	8	11	3	24	19	14	15	7	19	2	15	24	18	19	13	16	25	0	7	9
21	0	7	0	4	6	3	24	14	14	11	2	19	24	10	24	14	14	13	12	20	0	3	5
7	0	21	4	0	6	14	14	3	11	24	2	10	24	19	14	24	14	20	0	13	3	12	5

将最后一行转换成字母得明文为: have a good luck to you and me