密码学第二次作业

朱哲昊

March 2023

1 第一题

1.【Caesar 密码】仿射 Caesar 密码，即 Caesar 密码的一种推广，具有如下定义：对于每一个明文 p，用密文 C 代替，其中 $C = E([a,b],p) = (ap + b) mod\, 26$。对加密算法的一个基本要求是算法是单射的，即如果 $p \neq q$，则有 $E(k,p) \neq E(k,q)$。否则，就会因为有很多的明文映射成相同的密文而不能解密。仿射 Caesar 密码并不是对所有的 a 都满足上述的一对一映射，例如 $E([2,3],0) = E([2,3],13) = 3$。

1) a 共有 11 种合法取值，分别为 3、5、7、9、11、15、17、19、21、23、25 。

2) b 共有 25 种合法取值。

3) 仿射 Caesar 密码的密钥 $[a,b]$ 共有 275 种合法取值。

4) 若用仿射 Caesar 密码加密英文文本得到一份密文，发现其中频率最高的字母为 H，次高的字母为 Y，则密钥 $[a,b]$ 最有可能的取值为 20，5 。

图 1: 第一题

2 第二题

充分性证明 当 $gcd(k, p) = 1$ 时，则有整数 x, y 满足 $x * k + y * p = 1$
假设不"一一映射"，有 a, b 使得 $ak \equiv bk \bmod p$，即 $t = a - b, tk \equiv 0 \bmod p \Rightarrow \exists m, tk = mp$
在 $xk + yp = 1$ 两边同时乘 t，得到 $t * x * k + t * y * p = m * p * x + t * y * p = (x * m + t * y) * p = 1$ 这些数都是整数，显然不成立，即必有"一一映射"。

必要性证明 假设 $gcd(k, p) = d \neq 1$，则存在 $x, y, xk + yp = d$
则存在 $p = td, k = t'd$，取两个数 $a, a + t$，$ak - (a + t)k = -tk = -pk/d = -pt' \equiv 0 \bmod p$
与"一一映射"相矛盾，故假设不成立，有 $gcd(k, p) = 1$

3 第三题

3.1 破译

助记词句转成密钥就是 $thefalnvsmyboizdcgrwpjkqux$，明文就是 $loveistheonethingthattranscendstimeandspace$
对照表：

$$thefalnvsmyboizdcgrwpjkqux$$

$$abcdefghijklmnopqrstuvwxyz$$

3.2 单表代替的安全性和一般破译

安全性不高，只要有大量的样本明文密文就可以破译，通过一些边缘信息比如说密钥助记词句也可以获得密钥
一般破译方法就是通过一些相关信息得到密钥，得不到密钥也可以进行一系列猜测验证，若有大量的密文，也可以采用字母频率攻击
一定的明文 + 密文，也可以通过猜测密钥的方式来破译

3.3 密钥助记句子很长的原因

要使用完整的一句话，以方便用户的记忆，但是这句话又得尽可能多的覆盖 26 个字母，所以这句话就会很长，一般是 12 到 24 个单词组成的句子

4 第四题

4.1 密文：

dr th hoa dikeb xprvarl iaph dma alhs pnbtmba dryu gkdzhd mathgl

4.2 矩阵及密文

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

密文：da lb bgl dikec xpaare csuh bgs asdb nnfrmkd bgr qxdsqg fkalbes

4.3 推广性结论

密钥的不同会给密文带来很大的变化，也会给矩阵带来很大的变化，

4.4 选做

因为对于矩阵 M 中的任意行或列，进行平移，都不影响其加密的特性，故而 playfair keyspace=

$$\frac{25!}{25} = 24! \approx 2^{79}$$

5 第五题

1. 密文为：yybt yy rd foaa
m->12,e->4,e->4,t->19
矩阵为 M，第一步 $(12 \quad 4) * M \bmod 26 = (24 \quad 24)$ 同理 $(4 \quad 19) * M \bmod 26 = (1 \quad 19)$ 就可以得出对应的密文
2. 先求矩阵的逆矩阵

$$\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$$

再将 yybt 拆成 yy 和 bt 两部分，也就是 $(14 \quad 24)$ 和 $(4 \quad 19)$ 与逆矩阵分别相乘，得到 $(12 \quad 4)$ 和 $(4 \quad 19)$ 就相当于恢复了 meet 字符串

5.1 已知明文的攻击方案

明文密文长度为 L，L 为一个集合 S 中所有元素的倍数，任意取出 S 中的元素，假设为 n，那么在明文和密文中取对应的 n*n 的内容（且必须要整段整段 n 长的拿出来），构成两个矩阵，判断明文矩阵的行列式是否为与 26 互素的数，若是，则求次矩阵的逆元，这个逆矩阵右乘密文矩阵就是密钥矩阵

5.2 选择明文攻击

找出 n*n 的明文序列，内容是单位阵，对应的密文阵就是密钥矩阵

6 第 6 题

4 23 15 11 0 13 0 19 8 14 13

7 0 13 3 7 0 13 3 7 0 13

11 23 2 14 7 13 13 22 15 14 0

密文：lxcohnnwpoa

6.1 流密钥加密

15 11 4 0 18 4 21 12 4 5 8 5 19 24

9 0 1 7 23 15 21 14 11 11 2 8 9 13

24 11 5 7 15 19 16 0 15 16 10 13 2 11

密文：ylfhptqapqkncl

6.2 寻找另一个密钥流

15 11 4 0 18 4 21 12 4 5 8 5 19 24

8 3 14 13 19 7 0 21 4 12 14 13 4 24

19 18 10 13 1 3 5 9 0 7 6 8 11 0

密钥流：[19 18 10 13 1 3 5 9 0 7 6 8 11 0]

6.3 选做

vernam 密码就是转换成二进制数后按位异或，密钥位数不够，用前面的顶上了，将最后得出的二进制转换成字符串形式

密文：J&@GW?\$X4KQW - B$@9

7 第七题

7.1

1. 偶偶奇奇，奇奇偶偶，偶偶奇偶，偶偶偶奇，奇偶偶偶，偶奇偶偶，偶偶偶偶
2. 综合算下来有 $7 * 13 * 13 * 13 * 13 = 199927$ 种

7.2

把这个矩阵转一下，发现条件和第一小问一样，答案一样为 199927 种

7.3

13*13*13*13=28561 种

7.4

13*13*13*13*(7+2+1)=285610 种