仿射密码

Affine Cipher

刘卓

1 模逆元

模逆元 *(Modular Multiplicative Inverse)*。如果存在 $A \cdot C = 1 \bmod B$, ，则 C 是 B 模下 A 的模逆。记 $C = A^{-1} \bmod B$。 如果 A^{-1} 存在, 则 A 在 B 模下是可逆的。

例 1

另 $B = 26$，找到 26 以内的所有 A 逆。

模 26 的逆:

$$\begin{aligned} 1^{-1} &\equiv 1(\mathrm{mod}26) & 3^{-1} &\equiv 9(\mathrm{mod}26) \\ 9^{-1} &\equiv 3(\mathrm{mod}26) & 5^{-1} &\equiv 21(\mathrm{mod}26) \\ 21^{-1} &\equiv 5(\mathrm{mod}26) & 7^{-1} &\equiv 15(\mathrm{mod}26) \\ 15^{-1} &\equiv 7(\mathrm{mod}26) & 11^{-1} &\equiv 19(\mathrm{mod}26) \\ 19^{-1} &\equiv 11(\mathrm{mod}26) & 17^{-1} &\equiv 23(\mathrm{mod}26) \\ 23^{-1} &\equiv 17(\mathrm{mod}26) & 25^{-1} &\equiv 25(\mathrm{mod}26) \end{aligned}$$

其他 26 以内的数不存在。

2 最大公约数

最大公约数 (greatest common divisor)。让 d, n 为整数。当 d 除 n 或者 n 被 d 除时，表示为 $d|n$，读作 “d 整除 n”。如果存在一个整数 r, 使得 $n = d \cdot r$。所以 d 是 n 的约数 (divisor)。

设两个非零整数 m, n，他们的共同约数是正整数 d, 则 $d|m$ 和 $d|n$。

他们的最大公约数 (GCD) 是拥有一个共同约数 d，使得 d 大于其他约数。记作 $d = gcd(m, n)$。

如果 $gcd(m, n) = 1$ 则称 m, n 互素 (coprime)。

a 在 n 模下是可逆的当且仅当 $gcd(a, n) = 1$。

例 2

寻找 60 和 42 的最大公约数。

解:

$$60 = 2^2 + 3^1 + 5^1$$

$$42 = 2^1 + 3^1 + 7^1$$

使用素因数分解法，gcd 是所有共同的质数和最小的次方相乘。$gcd = 2^1 + 3^1 = 6$

3 仿射密码

仿射密码 (Affine cipher) 是一种替换密码。它需要几个条件：

1. a 和 b 是整数；
2. a 和 26 互素，即 $gcd(a, 26) = 1$；
3. $0 \leq b \leq 25$；

加密过程是 $y = E(x) = ax + b \bmod 26$
解密过程是 $x = D(y) = a^{-1}(y - b) \bmod 26$

例 3
加密明文 $SWORD$，令 $a = 9, b = 15$
解：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

明文	S	W	O	N	D
x	18	22	14	17	3
$y = ax + b \bmod 26$	21	5	11	12	16
密文	V	F	L	M	Q

例 4
解：
解密 $SYLNH$，令 $a = 19, b = 13$
$a^{-1} = 11$

明文	S	Y	L	N	H
y	18	24	11	13	7
$x = a^{-1}(y - b) \bmod 26$	3	17	4	0	12
密文	D	R	E	A	N

例 5

加密 I CAN PLAY，令 $a = 7, b = 25$

```
Plaintext = 'ICANPLAY'#字母需要大写
a = 7
b = 25

Ciphertext = ''
for i in Plaintext:
    x = ord(i) -65
    y = (a*x + b)%26
    Ciphertext += chr(y+ 65)
```

输出：DNZMAYZL

例 6

如果已知明文开头是 GO，并用仿射密码加密。破解密文 $EKTWQMRVRVWQMTF$。

解：

已知：

$$G \to E$$
$$O \to K$$

$G = 6, O = 14$ 为 x, 代入 $ax + b = y \bmod 26$, 等于 $y, 4 = E, 10 = K$，解二元一次方程。

$$\begin{cases} 6a + b = 4 \\ 14a + b = 10 \end{cases} \bmod 26.$$

$$\begin{cases} 6a + b = 4 \\ 14a + b = 10 \end{cases} \bmod 26 \quad \Rightarrow \quad \begin{cases} a = 4 \\ b = 6 \end{cases} \bmod 26 \quad or \begin{cases} a = 17 \\ b = 6 \end{cases} \bmod 26$$

然后 $gcd(4, 6) \neq 1, (4, 6)$ 不是互素，而 $gcd(17, 6) = 1$, 所以 $a = 17, b = 6$。

根据 $x = a^{-1}(y - b) \bmod 26$，明文为 GONE WITH THE WIND