韦尔南密码

Vernam Cipher

刘卓

1 余商定理

余商定理 *(Quotient-Remainder Theorem)*。给定一个整数 A 和一个正整数 B。存在整数 q, r，使得 $A = B \cdot q + r$ 其中 $0 \leq r \leq B$。

例 1

$$\underbrace{521}_{A} = \underbrace{26}_{B} \times \underbrace{20}_{(\text{商}q)} + \underbrace{1}_{(\text{余}r)}$$

$$521 = 1 \bmod 26$$

例 2

$$\begin{aligned} \underbrace{-521}_{A} &= -26 \times 20 - 1 \\ &= 26 \times (-20) + (-1) \\ &= 26 \times (-20) + 26 + (-1) - 26 \\ &= \underbrace{26}_{B} \times \underbrace{-21}_{q} + \underbrace{25}_{r} \end{aligned}$$

$$-521 = 25 \bmod 26$$

例 3

$$\begin{aligned} 785 &= 521 + 264 \pmod{26} \\ &= 1 + 4 \pmod{26} \\ &= 5 \pmod{26} \end{aligned}$$

例 4

$$\begin{aligned} 139 \times 787 \pmod{26} &= (26 \times 5 + 9) \times (26 \times 30 + 7) \pmod{26} \\ &= 9 \times 7 \pmod{26} \\ &= 63 \pmod{26} \\ &= 11 \pmod{26} \end{aligned}$$

2 加密过程

1. 转化明文，从 0 开始，按字母表顺序给每个字母分别编号；

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

2. 选取两组短密钥 U 和 V，然后计算长密钥 K：

$$K(i) = U(i) + v(i) \bmod 26$$

其中 $1 \leq i \leq n$, n 为明文长度

3. 计算密文 C:

$$C(i) := M(i) + K(i) \bmod 26$$

然后使用对应的字母替代明文字母；

例 5

设密钥 $U, V = (3,1,2), (7,3,8,4,5)$, 加密明文 $NO\ MORE\ AMMO$

解：

U	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
V	7	3	8	4	5	7	3	8	4	5	7	3	8	4	5
$K = U + V \bmod 26$	10	4	10	7	6	9	6	9	6	8	8	5	11	5	7

明文	N	0	M	0	R	E	A	M	M	O
M	13	14	12	14	17	4	0	12	12	14
K	10	4	10	7	6	9	6	9	6	8
$C = M + K \bmod 26$	23	18	22	21	23	13	6	21	18	22
密文	X	S	W	V	X	N	G	V	S	W

例 6

```
Plaintext = 'MYNAMEISBOB'#字母需要大写
U = [3,1,2,5,5,7,7,5,7]
V = [5,4,2,3,5,6,4,23,99,12]

def lcm(x, y):
   #  最小公倍数
   if x > y:
       greater = x
   else:
       greater = y

   while(True):
       if((greater % x == 0) and (greater % y == 0)):
           lcm = greater
           break
       greater += 1

   return lcm

K_len = lcm(len(U),len(V))
K = [0 for i in range(K_len)]

for i in range(K_len):
    K[i] = (U[i%len(U)] + V[i%len(V)])%26

#print(K)#密钥

Ciphertext = ''
for i in range(len(Plaintext)):
    M_i = ord(Plaintext[i]) -65 #大写字母 -65 ASCII表
    K_i = K[i%len(K)]
    C_i = (M_i+K_i)%26
    Ciphertext += chr(C_i+ 65)

print(Ciphertext)
```

输出：UDRIWRTUDDH

例 7

解密例 6 的加密字符 $UDRIWRTUDDH$

```
Ciphertext = 'UDRIWRTUDDH' #已知
U = [3,1,2,5,5,7,7,5,7]  #已知
V = [5,4,2,3,5,6,4,23,99,12] #已知

K_len = lcm(len(U),len(V))
K = [0 for i in range(K_len)]

for i in range(K_len):
    K[i] = (U[i%len(U)] + V[i%len(V)])%26

print(K)#密钥

Plaintext = ''
for i in range(len(Ciphertext)):
    C_i = ord(Ciphertext[i]) -65 #大写字母 -65 ASCII表
    K_i = K[i%len(K)]
    M_i = (C_i - K_i)%26

    Plaintext += chr(M_i+ 65)
print(Plaintext)
```

输出：MYNAMEISBOB