

信息安全原理课程报告

作业一

王子腾 3180102173

【问题】

What are the differences between Transposition Cipher and Substitution Cipher? Please give some examples of them.

【解答】

换位密码技术 (Transposition Cipher) 是通过特定的映射方式, 将明文中字符的位置重新排列, 即: 明文中符号的形式和数量没有发生变化, 发生变化的是符号的位置。换位密码技术的例子有:

1). 栅栏密码(Rail Fence Cipher)

在栅栏密码中, 明文被按照对角的形式上下交替的写在假想“围栏”上, 然后通过逐行横向读取获得密文。例如, 使用三层围栏和明文“*I LOVE CRYPTOLOGY*”, 转换形式为:

I = = = E = = = P = = = O = = = =
= L = V = C = Y = T = L = G = = =
= = O = = = R = = = O = = = Y =

得到密文: *IEPOL VCYTL GOROY*

2). 路由密码 (Route Cipher)

与栅栏密码类似, 路由密码也是先确定排布层数, 写入方式为自左向右, 从上到下依次填入明文字符, 而读取密文时, 可以指定从右上角开始, 逆时针向内旋进。例如, 选择三层排布和明文“*I LOVE CRYPTOLOGY*”, 转换为:

I V R T O
L E Y O G
O C P L Y

读得密码: *OGYLP COLIV RTOYE*

替代密码技术(Substitution Cipher)的实现与前者正好相反, 这种技术通过映

射，将明文中的每单个文本字符替换为其他的符号或标识，即：明文中字符的形式发生了变化，但位置保持不变。替代密码技术的例子有：

1). 凯撒移位密码(Caesar Cipher)

将每一个字母按照统一的偏移量，根据字母表上的顺序使用其他字母替代，例如：偏移量为+3，则对应关系为：

明文： **ABCDEFGHIJKLMNOPQRSTUVWXYZ**

密文： **DEFGHIJKLMNOPQRSTUVWXYZABC**

2). 维吉尼亚密码(Vigenère Cipher)

将明文的字母按照密钥的对应关系进行不同偏移量的替代加密，其映射关系对应维吉尼亚表：

Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	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

例如：密钥为“**ZJU**”，明文为“**ABCDEF**”，则对应关系为：

A-Z, B-K, C-W, D-C, E-N, F-Z

密文为“**ZKWCNZ**”

【实验】

Design and implement a Transposition Cipher or Substitution Cipher algorithm to encrypt and decrypt strings with high security.

【环境】

语言：C

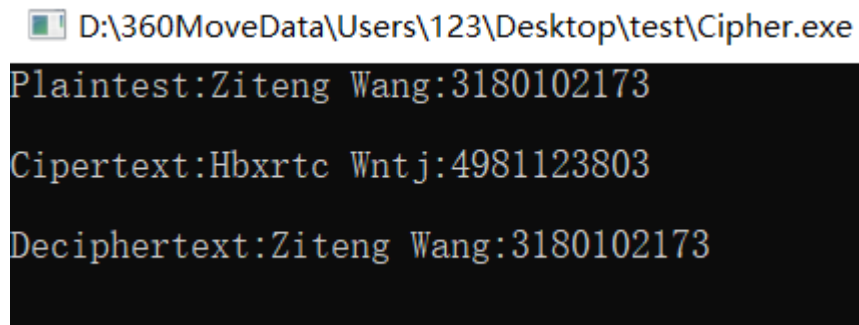
编译环境：gcc

【算法】

本算法使用换位密码技术，每一个字符由其后面的字符作为密钥，并按照后一位与'A'/'a'/'0'的偏移量进行移位替换，同时保留最后一位作为解码位。解码时，根据最后一位的偏移量，反推出前一位的字符，再带入破译出的新一位继续反推，直至所有位数都被成功解码。对于替换原则，字母间转换遵循维吉尼亚表，若密钥为数字，则按照其相对'0'的偏移量对明文进行加密，若明文为数字，则偏

移量对十取余后进行加密，非字母数字则保留。

【实验结果】



```
D:\360MoveData\Users\123\Desktop\test\Cipher.exe
Plaintext: Ziteng Wang:3180102173
Ciphertext: Hbxrtc Wntj:4981123803
Deciphertext: Ziteng Wang:3180102173
```

明文： Ziteng Wang:3180102173

密文： Hbxrtc Wntj:4981123803

译文： Ziteng Wang:3180102173

【实验心得】

通过本次查询资料并编程实验，我加深了对明文加密方式的认识，在编程过程中，遇到的一个问题是如果将全部字符串加密，那么在翻译时就失去了破译的密钥，因此选择保留最后一位，并倒序的方式依次获取偏移量，从而反加密得到正序的编码。同时，在偏移计算的同时如果没有考虑折返（如'Z'+1->'A'），则会导致乱码和溢出的现象，因此应当先判断并进行折返操作，再进行赋值。