

信息安全原理作业一报告

应承峻 3170103456

【问题】

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

【解答】

Transposition Cipher（置换密码）是指通过一定规则改变字符串中字符的顺序来进行加密，而 Substitution Cipher（替代密码）是指通过一定规则将字符串中的字符替换成其他字符。因而两者的区别在于置换密码改变的是明文单元的顺序，明文单元本身不变；而替代密码改变的是明文单元本身，明文单元的保持原有的顺序。替代密码的例子有：

①凯撒密码（Caesar cipher）：将每一个字母按照一定的偏移量进行替代，例如当偏移量为 1 时，对明文“HELLO”进行加密后，得到的密文是“IFMMP”

Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext alphabet: BCDEFGHIJKLMNOPQRSTUVWXYZA

②维吉尼亚密码（Vigenère cipher）：使用一系列凯撒密码组成密码字母表的加密算法。例如，假设明文为：YING CHENG JUN 并设定 ZJU 为密钥，对于明文的第一个字母 Y 对应密钥的第一个字母 Z，于是使用表格中 Z 行字母表进行加密得到 X，类似地就可以得到其他的密文（当密钥长度短于明文时需重复使用）

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

置换密码常见的例子有：

①栅栏密码（Rail Fence Cipher）：把明文按照一定顺序排成一个矩阵，然后按另一顺序选出矩阵中的字母以形成密文，最后截成固定长度的字母组作为明文，例如明文：ZJU INFORMATION SECURITY

Z	J	U		I	N
F	O	R	M	A	T
I	O	N		S	E
C	U	R	I	T	Y

于是可以得到密文：ZFICJOOUURNR M IIAST NTEY

对密文进行还原时只需将其在按列写在表格中再按行读出即可。

②列换位密码（Columnar transposition Cipher）：在栅栏密码的基础上对列进行排列重组，解密时按照一定的顺序得到。例如按照 632415 的顺序重组，得到密文 NTEYURNRJOOU M IZFICIAST。

Z	J	U		I	N
F	O	R	M	A	T
I	O	N		S	E
C	U	R	I	T	Y

【实验内容】 Design and implement a Transposition Cipher or Substitution Cipher algorithm to encrypt and decrypt strings with high security.

【编程环境】 C++

【算法设计】

在实验中，我选择的是 Vigenère 加密算法的思路。程序中密钥是只包含大小写字母的字符串，明文可以包含所有的英文字符，但是只有大小写字母和数字会被加密，其余字符不做处理，此外密文字符的大小写与明文保持一致。

大小写明文和密钥的对应关系如下图所示：

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

当明文字符为数字时，采用的算法是数字加上当前密钥的 ASCII 码与 65 或 97（取决于密钥字符的大小写）的差值，再对 10 取模。

给定明文字符 c 和密钥字符 k，转换成密文字符 res 的伪代码如下：

```
char map(char c , char k) {
    char upper_key = k 的大写形式;
    char lower_key = k 的小写形式;
    if (c 是小写字符) {
        res = c - 'a' + lower_key;
        while (res >= 'a' + 26) res -= 26;
    } else if (c 是大写字符) {
        res = c - 'A' + upper_key;
        while (res >= 'A' + 26) res -= 26;
    } else if (数字) {
        res = (k >= 'A' && k <= 'Z') ? c + k - 'A' : c + k - 'a';
        while (res >= 58) res -= 10;
    } else res = c;
    return (char)res;
}
```

【实验结果】

密钥：ZJU

明文：Ying Cheng Jun STUDENT_ID = 3170103456

```
公钥：ZJU
明文：Ying Cheng Jun STUDENT_ID = 3170103456
密文：Xrhf Wgnhf Dtw RCOCNHS_CC = 2129152405
解密：Ying Cheng Jun STUDENT_ID = 3170103456
请按任意键继续. . .
```

程序输出密文：Xrhf Wgnhf Dtw RCOCNHS_CC = 2129152405

程序解密: Ying Cheng Jun STUDENT_ID = 3170103456

【实验心得】在本实验的实践过程中,遇到的其中一个问题是通过 Vigenère 算法对明文进行加密时,当明文字符是小写字母并且密钥字符的 ASCII 码较大时,例如明文字符是 o 密钥字符是 v,这时相加的结果会超过 char 类型的范围从而发生溢出,导致程序运行结果错误。因此需要进行强制类型转换。