Programming Practice: Cipher

1. A classical cipher is substitution cipher that letters are one-to-one systematically mapped to other letters. The mapping is called the code book of a substitution cipher. For example, the following is a code book mapping uppercase English letters to themselves

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

   This cipher technique is also called mono-alphabetic substitution cipher. With this code book, "UNIVERSITY" is encoded into "FZDLOTKDUW". Write a C program to perform the following steps:
   1. Input an English text;
   2. Remove white spaces and punctuation symbols;
   3. Convert all lower case letters to upper case letters;
   4. Encode the text using the above code book;
   5. Output the original text and the encoded text;
   6. Generate the decode book, which is an inverse function of the code book;
   7. Decode the encoded text and output the decoding result.

   Assume the maximum characters in the input length is 10,000.

```
D:\>substitution_cipher < FCU.txt
>>>> The input original text:

International School of Technology and Management
Feng Chia University

--------------------------------------------------------------------------------
>>>> The encoded text:

DZUOTZNUDBZNHKIRBBHBYUOIRZBHBAWNZQXNZNAOXOZUYOZAIRDNFZDLOTKDUW

--------------------------------------------------------------------------------
>>>> The decoded text:

INTERNATIONALSCHOOLOFTECHNOLOGYANDMANAGEMENTFENGCHIAUNIVERSITY

--------------------------------------------------------------------------------
```

2. A more complicated cipher technique is poly-alphabetic substitution cipher. It is more difficult to break a poly-alphabetic substitution cipher. A Vigenère square with a keyword is used to encode a text of English letters. The first row of a Vigenère square is 26 English letters in the alphabetical order, then each of the following row is the cyclic left rotation of the row right on the top of it. A Vigenère square is given as the following tables:

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

In fact, a Vigenère square can be viewed as 26 code books indexed on the letters of the first column. A keyword can be any English word, it will be repeatedly concatenate itself until the same length as the encoded text. The encoded text and the repeated keyword is aligned and then a code to book is selected. Selection of the code book is to match the aligned letter of the keyword with the fist letter of the code book. With the selected code book, the letter of the encoded text is then translated to a ciphered letter. For example, if the keyword is "FENGCHIA" and the text is "PROGRAMMINGAPPLICATIONSFORENGINEERS" (Programming Applications for Engineers), the encoding of the text is shown as below.

Input Text	P	R	O	G	R	A	M	M	I	N	G	A	P	P	L	I	C	A	T	I	O	N	S	F	O	R	E	N	G	I	N	E	E	R	S
Keyword	F	E	N	G	C	H	I	A	F	E	N	G	C	H	I	A	F	E	N	G	C	H	I	A	F	E	N	G	C	H	I	A	F	E	N
Encoded Text	U	V	B	M	Y	H	U	M	N	R	T	G	R	W	T	I	H	E	G	O	Q	U	A	F	T	V	R	T	I	P	V	E	J	V	F

The encoded text is "UVBMTHUMNRTGRWTIHEGOQUAFTVRTIPVEJVF". Write a C program to perform the following steps:

1. Input a keyword and an English text;
2. Remove white spaces and punctuation symbols;
3. Convert all lower case letters to upper case letters;
4. Encode the text using the Vigenère square and
5. Output the original text and the encoded text;
6. Decode the encoded text and output the decoding result.

Assume the maximum characters in the input length is 10,000. You may use MDOS

pipeline command to input (<) and output (>) the original text and the encoded text. Sample input C_Programming.txt and MacArthur_Prayer.txt (the first word is the keyword). Sample output:

```
D:\>vigenere_square < C_Programming.txt
**** The keyword is: FENGCHIA

>>>> The input original text:

Programming Applications for Engineers

--------------------------------------------------------------------------------

>>>> The encoded text:

UVBMTHUMNRTGRWTIHEGOQUAFTVRTIPVEJVF

--------------------------------------------------------------------------------

>>>> The decoded text:

PROGRAMMINGAPPLICATIONSFORENGINEERS

--------------------------------------------------------------------------------
```

```
D:\>vigenere_square < MacArthur_Prayer.txt
**** The keyword is: DOUGLASMACARTHUR

>>>> The input original text:

General MacArthur's Prayer for His Son by Douglas MacArthur
Build me a son, O Lord, who will be strong enough to know when
he is weak; and brave enough to face himself when he is afraid;
one who will be pround and unbending in honest defeat and humble
and gentle in victory.
Build me a son whose wishes will not take the place of deeds;
a son who will know Thee -- and that to know himself is the
foundation stone of knowledge.
Lead him, I pray, not in the path of ease and comfort, but under
the stress and spur of difficulties and challenge. Here let him
learn to stand up in the storm; here let him learn compassion for
those who fail.
Build me a son whose heart will be clear, whose goal will be high,
a son who will master himself before he seeks to master other men,
one who will reach into the future, yet never forget the past.
And after all these things are his, add, I pray, enough of a sense
of humor, so that he may always be serious, yet never take himself
too seriously. Give him humility, so that he may always remember
the simplicity of true greatness, the open mind of true wisdom,
and the meekness of true strength.
Then I, his father, will dare to whisper, "I have not lived in
vain!"

--------------------------------------------------------------------------

>>>> The encoded text:

JSHKCADYAEAIMOOIVDLGJEJROTHZLZIEEMXUFGDMSOATTYNYXFVATLVYECSFGVFFURQNZWAXLDEJMYIEJSHUFGZFOMNFPDBVQVYODWWMKCNUUYUMHSHUFGZFOHATXOCDVSFLHHWZHGIJTMLRLRITPWZAWKLCU
LJIRIHJLNVGNDEEWPHXLBBUYEKFDGFVTAUEGVOSMLWMNFGVGAFVLBPONTGDYDUZEKGVDGITHHGEEYIJALMNLZFTZTLMKGTYXWFRFSILOEWPSCSFGDBFZWFRVNGITJEVTUXKKONZZKFAWJIDLLFWLGNNPFGGNF
AKBVHJWCHKZFCZOYLVWNYCHOXNTMABRCYEHACEWVYVLTZAFGAJXHHUFCGLZRLNUVUEWLLKKSMZCEKEAPDJIBLFIRCLQIUGLVIVLHHUFVURWEFSEJEIXSYKKWGRPAJZTQSKTUXLSWHZSEKFOTMYXYYCHHBOXLW
MRPCFFWUJVWITQOJFHQSVPOIWDWFHFIDPMGAJHUQYRGYNPAJFWKLCULWCHOLCSOKQGQACPPFCESBORHSEOPWYHDCCOAUYEEJTIOSVEMVVICLKSEKQEMSKHTUJWSLUEHWDMGNFGLQYRKCRWRWMCJIEMVNYHTOZ
FRWKEVNVOLLWRFAKETZQPCSKTUXRIHYXLLDFHGSVMOCEJGUXPHAEAFDZIYUPHBIARHGRAUEELLIWKIGUCSGFHCTYXTUPDZQGJSTQSGRZHBMPHHHKGEJFAMEYBTMVOTNUZSWDIQUJEFAZYSBOXHMYINIKRZIKK
ONNPMSKANWRRZLVPSGHPRLTEUIDISCTLHSUQTJGEIRVTAHVVGNNPOHQNOIEWVZKUIYCTSVAMCNUMOYDHSETPSKAFVRLXZNIHBAZSTZQNKHZLMUKKSLCTLDPATEKHDBZVDYXTHSHEPOKEPPVGWHBLIF

--------------------------------------------------------------------------

>>>> The decoded text:

GENERALMACARTHURSPRAYERFORHISSONBYDOUGLASMACARTHURBUILDMEASONOLORDWHOWILLBESTRONGENOUGHTOKNOWWHENHEISWEAKANDBRAVEENOUGHTOFACEHIMSELFWHENHEISAFRAIDONEWHOWILLB
EPROUNDANDUNBENDINGINHONESTDEFEATANDHUMBLEANDGENTLEINVICTORYBUILDMEASONWHOSEWISHESWILLNOTTAKETHEPLACEOFDEEDSASONWHOWILLKNOWTHEEANDTHATTOKNOWHIMSELFISTHEFOUND
ATIONSTONEOFKNOWLEDGELEADHIMIPRAYNOTINTHEPATHOFEASEANDCOMFORTBUTUNDERTHESTRESSANDSPUROFDIFFICULTIESANDCHALLENGEHERELETHIMLEARNTOSTANDUPINTHESTORMHERELETHIMLE
ARNCOMPASSIONFORTHOSEWHOFAILBUILDMEASONWHOSEHEARTWILLBECLEARWHOSEGOALWILLBEHIGHASONWHOWILLMASTERHIMSELFBEFOREHESEEKSTOMASTEROTHERMENONEWHOWILLREACHINTOTHEFUT
UREYETNEVERFORGETTHEPASTANDAFTERALLTHESETHINGSAREHISADDIPRAYENOUGHOFASENSEOFHUMORSOTHATHEMAYALWAYSBESERIOUSYETNEVERTAKEHIMSELFTOOSERIOUSLYGIVEHIMHUMILITYSOTH
ATHEMAYALWAYSREMEMBERTHESIMPLICITYOFTRUEGREATNESSTHEOPENMINDOFTRUEWISDOMANDTHEMEEKNESSOFTRUESTRENGTHTHENIHISFATHERWILLDARETOWHISPERIHAVENOTLIVEDINVAIN

--------------------------------------------------------------------------
```