Programming Assignment 5: Substitutional Vigenère Square Cipher

A substitutional Vigenère square is a variance of Vigenère square combining with substitution cipher. The second row is a substitution cipher code book and each of the following row is the cyclic left rotation of the row right on the top of it. An example of a substitutional Vigenère square is shown as the following:

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

A keyword can be any English word which is repeated until the same length as the encoded text. The encoded text and the repeated keyword is aligned and then a code 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. Note that code book selection is determined by the inverse mapping of the code book, i.e., the decode 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 "STRUCTUREPROGRAMMINGDESIGNINC" (Structure Programming Design in C), the encoding of the text is shown as below.

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

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

i. Input a keyword and an English text;
ii. Output the keyword and the original text;
iii. Create the decode book;

iv. Print the first code book and the first decode book.
v. Remove white spaces and punctuation symbols in the English text and convert all lower case letters to upper case letters;
vi. Encode the text using the Vigenère square with the code book given in the above substitutional Vigenère square and output the encoded text;
vii. Decode the encoded text and output the decoded text.

A skeleton program assignment5_skeleton.c is available in iLearn. In this assignment, you must submit two files: the source code of the solution **assignment5_DXXXXXXX.c** (**80%**) and the assignment report **assignment5_DXXXXXXX.pdf** (**20%**), where **DXXXXXXX** is your student ID. The assignment report should explain the encoding and decoding algorithms in your solution. Programming assignment 5 is due by **23:59 pm, Sunday, December 10**. Submit your solution and the report to **iLearn**.

Example of program execution: