COS 330 PRACTICAL 1

By Dylan Kapnias (u18108467)

Question 2.2

a.) Input message left to right, remove all spaces as well as remove the '.' and separate the sentence with 'XX', add additional 'X' for padding at the end. When using the first key, assume that redundant letters are removed. Read the columns in alphabetical order with accordance to the first non-redundant key, and group characters into sets of five.

2	**8**	**10**	**7**	**9**	**6**	**3**	**1**	**4**	**5**
C	**R**	**Y**	**P**	**T**	**O**	**G**	**A**	**H**	**I**
B	E	A	T	T	H	E	T	H	I
R	D	P	I	L	L	A	R	F	R
O	M	T	H	E	L	E	F	T	O
U	T	S	I	D	E	T	H	E	L
Y	C	E	U	M	T	H	E	A	T
R	E	T	O	N	I	G	H	T	A
T	S	E	V	E	N	X	X	I	F
Y	O	U	A	R	E	D	I	S	T
R	U	S	T	F	U	L	B	R	I
N	G	T	W	O	F	R	I	E	N
D	S	X	X	X	X	X	X	X	X

TRFHE HXIBI XBROU YRTYR NDEAE THGXD LRXHF TEATI SREXI ROLTA FTINX
HLLET INEUF XTIHI UOVAT WXEDM TCESO UGSTK EDMNE RFOXA PTSET EUSTX

Input the new sets of five as if a message into the matrix from left to right. When using the second key, assume redundant letters are removed, spaces are removed, and all excess letters are also removed. Read the columns in alphabetical order with accordance to the second non-redundant key, and group characters into sets of five.

4	**2**	**8**	**10**	**5**	**6**	**3**	**7**	**1**	**9**
N	**E**	**T**	**W**	**O**	**R**	**K**	**S**	**C**	**U**
T	R	F	H	E	H	X	I	B	I
X	B	R	O	U	Y	R	T	Y	R
N	D	E	A	E	T	H	G	X	D
L	R	X	H	F	T	E	A	T	I
S	R	E	X	I	R	O	L	T	A
F	T	I	N	X	H	L	L	E	T
I	N	E	U	F	X	T	I	H	I
U	O	V	A	T	W	X	E	D	M
T	C	E	S	O	U	G	S	T	K
E	D	M	N	E	R	F	O	X	A
P	T	S	E	T	E	U	S	T	X

This is the final encryption:-

BYXTT EHDTX TRBDR RTNOC DTXRH EOLTX GFUTX NLSFI UTEPE UEFIX FTOET
HYTTR HXWUR EITGA LLIES ISFRE XEIEV EMSIR DIATI MKAXH OAHXN UASNE

b.) Take the final encryption and insert it into the matrix columns from top to bottom with accordance to alphabetical order of the second non-redundant key. Then read the first decryption from left to right as if a book.

4	**2**	**8**	**10**	**5**	**6**	**3**	**7**	**1**	**9**
N	**E**	**T**	**W**	**O**	**R**	**K**	**S**	**C**	**U**
T	R	F	H	E	H	X	I	B	I
X	B	R	O	U	Y	R	T	Y	R
N	D	E	A	E	T	H	G	X	D
L	R	X	H	F	T	E	A	T	I
S	R	E	X	I	R	O	L	T	A
F	T	I	N	X	H	L	L	E	T
I	N	E	U	F	X	T	I	H	I
U	O	V	A	T	W	X	E	D	M
T	C	E	S	O	U	G	S	T	K
E	D	M	N	E	R	F	O	X	A
P	T	S	E	T	E	U	S	T	X

TRFHE HXIBI XBROU YRTYR NDEAE THGXD LRXHF TEATI SREXI ROLTA FTINX
HLLET INEUF XTIHI UOVAT WXEDM TCESO UGSTK EDMNE RFOXA PTSET EUSTX

Take the first decryption and insert it into the matrix columns from top to bottom with accordance to alphabetical order of the first non-redundant key. Then read the final decryption from left to right as if a book. Remove the sequence of ‘X’ at the end and add a full stop where there is a sequence of ‘XX’ to separate sentences.

2	**8**	**10**	**7**	**9**	**6**	**3**	**1**	**4**	**5**
C	**R**	**Y**	**P**	**T**	**O**	**G**	**A**	**H**	**I**
B	E	A	T	T	H	E	T	H	I
R	D	P	I	L	L	A	R	F	R
O	M	T	H	E	L	E	F	T	O
U	T	S	I	D	E	T	H	E	L
Y	C	E	U	M	T	H	E	A	T
R	E	T	O	N	I	G	H	T	A
T	S	E	V	E	N	X	X	I	F
Y	O	U	A	R	E	D	I	S	T
R	U	S	T	F	U	L	B	R	I
N	G	T	W	O	F	R	I	E	N
D	S	X	X	X	X	X	X	X	X

c.) The advantages of this technique are the ease at which it can be remembered and used, and the speed at which a message can be encrypted. Due to the ease with which a symmetric cipher can be cracked in current times, the only use cases would be where there is a lot of data that needs to be encrypted and security is not that important or not at all required.