COS330 Practical 1 – u22561154

For the encryption, I have decided to leave out all the letters that are redundant and take out all the spaces between the words. Taking out the redundant letters because when we are doing the alphabetize the first 10-letter memory words and it would cause a conflict if there were two of the same letter and you don't know which number to assign them to, so taking out the redundant words works for this case. Taking out the space allows there to be no blank in the alphabetize memory words. We would also leave out the punctuation marks out of the 10-letter memory word so that the 10 letters will only contain alphabets and no other characters. Homogenize the 10-letter memory word.

A)

2	**9**	**10**	**7**	**8**	**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 WXTLE DMNER FOXED

MTCES OUGSA PTSET EUSTX

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	T	L	E
D	M	N	E	R	F	O	X	E	D
M	T	C	E	S	O	U	G	S	A
P	T	S	E	T	E	U	S	T	X

BYXTT EHLES TRBDR RTNOM TTXRH EOLTX

OUUTX NLSFI UDMPE UEFIX FTRST HYTTR

HXWFO EITGA LLITX GSFRE XEIEV NCSIR

DIATI EDAXH OAHXN UAEEE

Above is the complete cypher text for the encryption.

B) Cipher text to decrypt:

BYXTT EHLES TRBDR RTNOM TTXRH EOLTX

OUUTX NLSFI UDMPE UEFIX FTRST HYTTR

HXWFO EITGA LLITX GSFRE XEIEV NCSIR

DIATI EDAXH OAHXN UAEEE

Then we put it in the table using the memory work **Network Security**:

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	T	L	E
D	M	N	E	R	F	O	X	E	D
M	T	C	E	S	O	U	G	S	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 WXTLE DMNER FOXED

MTCES OUGSA PTSET EUSTX

Then we use the above text and place it in the table with the memory word **Cryptographic**:

2	**9**	**10**	**7**	**8**	**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

Then we read the message from left to right and decrypt the message:

The message:

Be at the third pillar from the left outside the lyceum theatre tonight at seven. If you are distrustful bring two friends.

C) Personally I think, Internal Network Communications, when communication happens within a controlled and secure environment, such as within a company's internal network, symmetric encryption is efficient due to its speed. I also think, communication through the internet, such as, real time messaging when the messages are encrypted because symmetric encryption is much faster than asymmetric encryption.