Scott Bebington

U21546216

COS 330 Practical Assignment 1

a)

Using the two keys (memory words) cryptographic and network security, encrypt the following message:

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

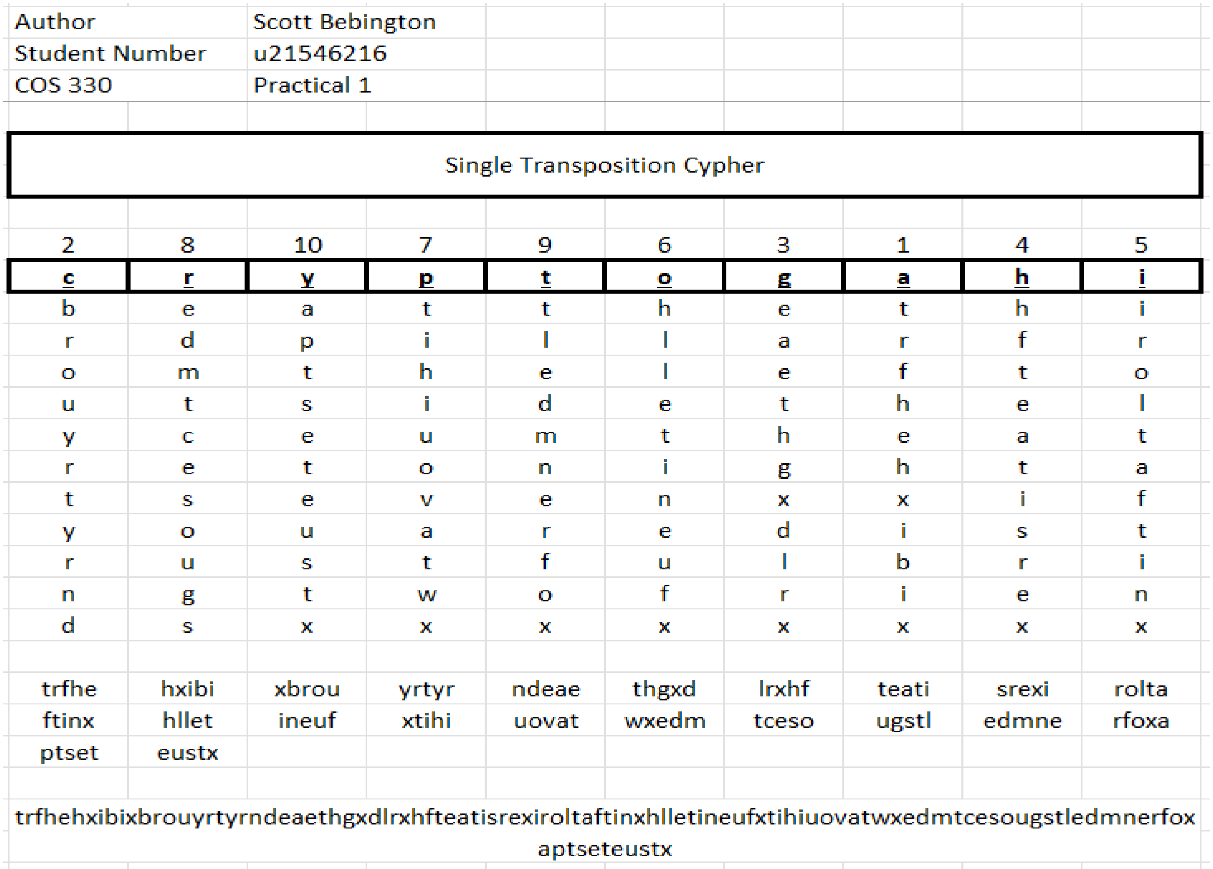
Assumptions:

Duplicate letters: I removed all duplicate letters, this was to avoid confusion as well as keeping the numbering of the letters easier.

Spacing and Punctuation: For spaces, I kept it the same format as in the document (Removed them), for full stops an xx is used in its place (Also the same as the document)

Padding: The same as the document, any open spaces at the end of the table are padded with x's

Word truncation: As the special forces document specifies that 10 letter memory words are to be used, in the case of the second memory word (Network Security), all duplicate letters and spaces were removed as well as any letters going past 10 were removed leaving the word "networkscu". For cryptography the same approach is used leaving the word "cryptogahi"



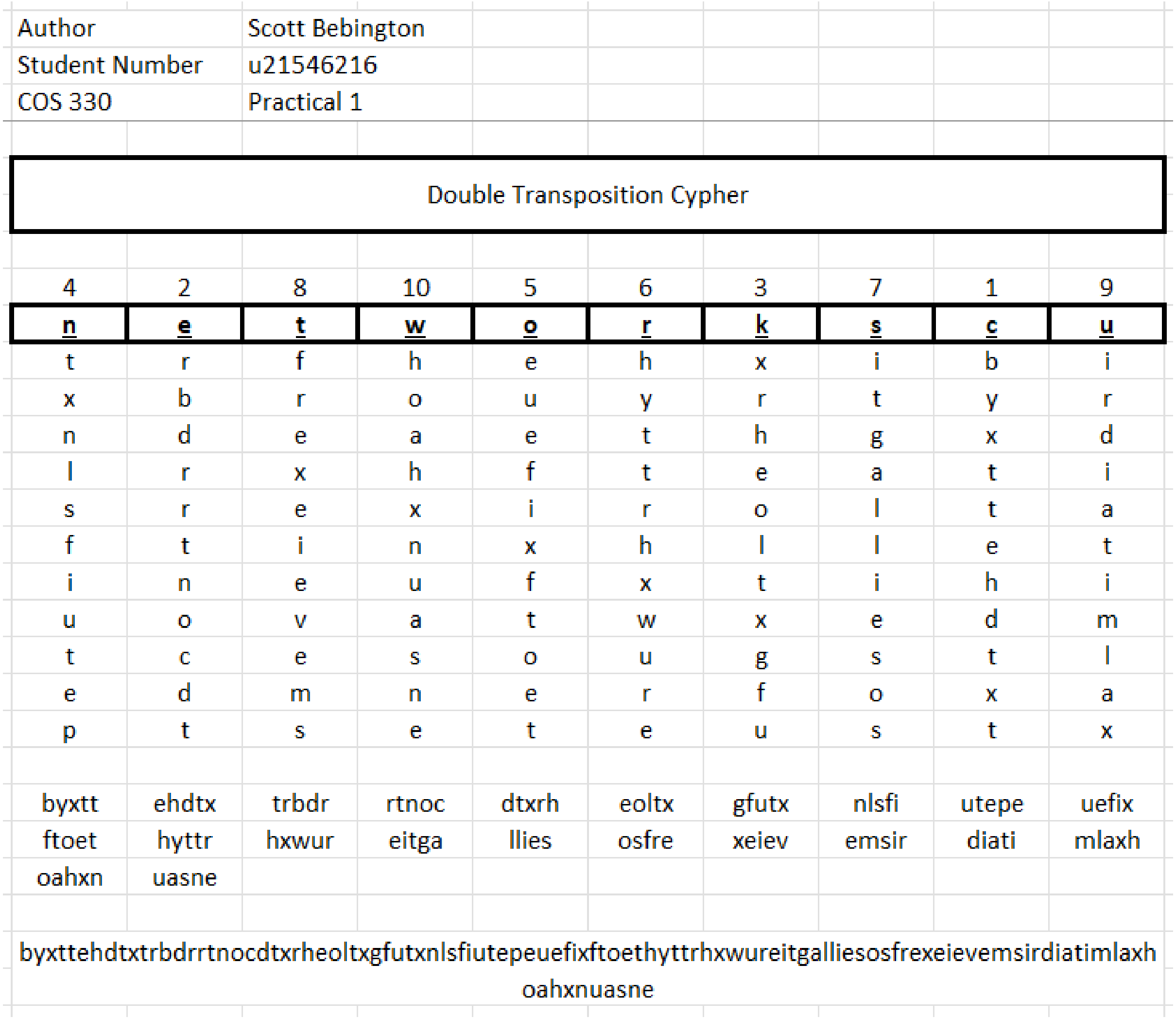
Author	Scott Bebington
Student Number	u21546216
COS 330	Practical 1

Single Transposition Cypher

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	ugstl	edmne	rfoxa
ptset	eustx								

trfhehxibixbrouyrtyrndeaethgxdlrxhfteatisrexiroltaftinxhlletineufxtihiuovatwxedmtcesougstledmnerfox
aptseteustx



Author	Scott Bebington
Student Number	u21546216
COS 330	Practical 1

Double Transposition Cypher

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	l
e	d	m	n	e	r	f	o	x	a
p	t	s	e	t	e	u	s	t	x

byxtt	ehdtx	trbdr	rtnoc	dtxrh	eoltx	gfutx	nlsfi	utepe	uefix
ftoet	hyttr	hxwur	eitga	llies	osfre	xeiev	emsir	diati	mlaxh
oahxn	uasne								

byxttehdtxtrbdrrtnocdtxrheoltxgfutxnlsfiutepeuefixftoethyttrhxwureitgalliesosfrexeievemsirdiatimlaxh
oahxnuasne

Single cypher word list:

trfhe	hxibi	xbrou	yrtyr	ndeae	thgxd	lrxhf	teati	srexi	rolta
ftinx	hllet	ineuf	xtihi	uovat	wxedm	tceso	ugstl	edmne	rfoxa
ptset	eustx								

Single cypher final string:

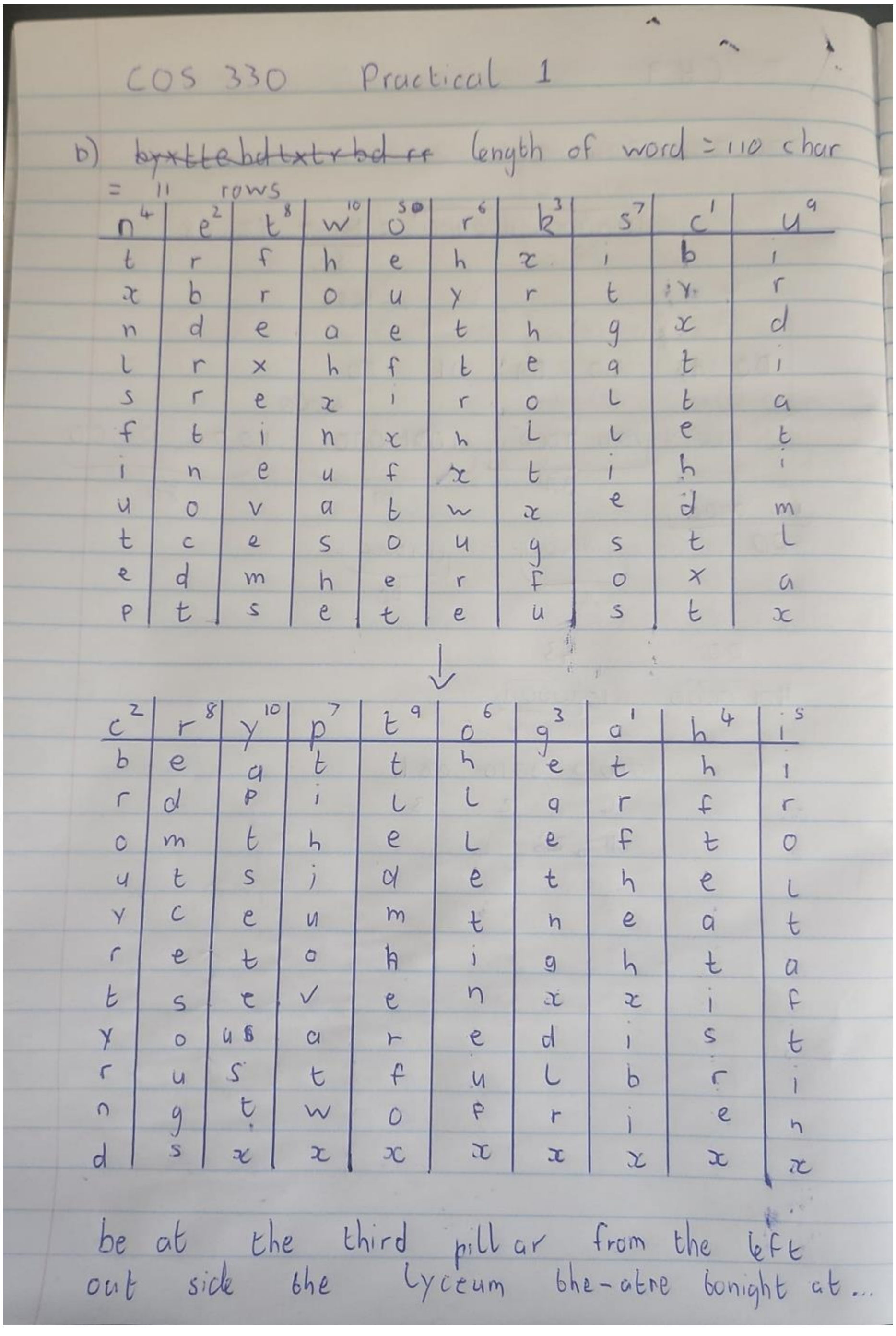
Trfhehxibixbrouyrtyrndeaethgxdlrxhfteatisrexiroltaftinxhlletineufxtihiuovatwxedmtcesougstledmn erfoxaptseteustx

Double cypher word list:

byxtt	ehdtx	trbdr	rtnoc	dtxrh	eoltx	gfutx	nlsfi	utepe	uefix
ftoet	hyttr	hxwur	eitga	llies	osfre	xeiev	emsir	diati	mlaxh
oahxn	uasne								

Double cypher final string: byxttehdtxtrbdrrtnocdtxrheoltxgfutxnlsfiutepeuefixftoethyttrhxwureitgalliesosfrexeievemsirdiatimlaxhoahxnuasne

b)



COS 330 Practical 1

b) ~~byxttebdtxtrbd rr~~ length of word = 110 char = 11 rows

n^{4}	e^{2}	t^{8}	w^{10}	o^{5}	r^{6}	k^{3}	s^{7}	c^{1}	u^{9}
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	l
e	d	m	h	e	r	f	o	x	a
p	t	s	e	t	e	u	s	t	x

↓

c^{2}	r^{8}	y^{10}	p^{7}	t^{9}	o^{6}	g^{3}	a^{1}	h^{4}	i^{5}
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	j	d	e	t	h	e	l
y	c	e	u	m	t	h	e	a	t
r	e	t	o	h	i	g	h	t	a
t	s	e	v	e	n	x	x	i	f
y	o	u s	a	r	e	d	i	s	t
r	u	s	t	f	u	l	b	r	i
n	g	t	w	o	p	r	i	e	n
d	s	x	x	x	x	x	x	x	x

be at the third pill ar from the left out side the lyceum the-atre tonight at...

c) Advantages: very simple to implement, using 2 memory words allows for an extra layer of encryption as apposed to a single memory word.

It is appropriate to use technique when only 2 parties are aware of the memory words and a quick hand written message needs to be encrypted and sent to the second party