Security in Computing & Information Technology

COSC2536/2537

Assignment 1

Name: Duncan Do

Student Number: s3718718

Question 1

a) [Double Transposition Cipher]

Step 1: Find a row with "T", "H", "I", and "S"

	1	2	3	4	5	6	7	
1	S	O	G	I	U	N	B	<- has "I"
2	C	N	U	O	D	L	M	<- has none
3	I	X	O	T	S	I	N	<- has "T", "I" and "S"
4	C	R	H	I	N	P	E	<- has "H" and "I"
5	H	N	W	R	T	O	A	<- has "T" and "H"
6	R	O	S	A	T	N	P	<- has "T" and "S"
7	H	A	I	I	T	S	S	<- has "T", "H", "I" and "S" (2x)
8	O	B	O	F	E	D	U	<- has none
9	O	O	T	S	P	I	I	<- has "T", "I" and "S"
10	E	L	M	X	N	A	P	<- has none
11	E	S	A	T	L	R	N	<- has "T", and "S"

Row 7 is the only row with the right combination of letters. However, because there are duplicates of some letters, we will have to order the columns to satisfy all possible combinations of T H I S.

Step 2: Move row 7 to the top.

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

Step 3: Creating all column combinations to have "T H I S" as the first word.

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

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

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

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

From the first combination of "T H I S", the first line is clearly "This is a". Thus, I only need to do is swap the Is and Ss.

After looking at all the combinations, the first is the only one with legible words. (E.g. Column, row)

Step 4: Changing the row order to make words and sentences

a)

	5	1	4	6	3	7	2			5	1	4	6	3	7	2
7	T	H	I	S	I	S	A	"->"	7	T	H	I	S	I	S	A
1	U	S	I	N	G	B	O	"->"	10	N	E	X	A	M	P	L
2	D	C	O	L	U	M	N	"->"	1	U	S	I	N	G	B	O
3	S	I	T	I	O	N	X	"->"	2	D	C	O	L	U	M	N
4	N	C	I	P	H	E	R	"->"	3	S	I	T	I	O	N	X
5	T	H	R	O	W	A	N	"->"	4	N	C	I	P	H	E	R
6	T	R	A	N	S	P	O	"->"	5	T	H	R	O	W	A	N
8	E	O	F	D	O	U	B	"->"	6	T	R	A	N	S	P	O
9	P	O	S	I	T	I	O	"->"	8	E	O	F	D	O	U	B
10	N	E	X	A	M	P	L	"->"	9	P	O	S	I	T	I	O
11	L	E	T	R	A	N	S	"->"	11	L	E	T	R	A	N	S

Adding row 10 to the end of 7
will create "This is an exampl"

b)

	5	1	4	6	3	7	2			5	1	4	6	3	7	2
7	T	H	I	S	I	S	A	"->"	7	T	H	I	S	I	S	A
1	U	S	I	N	G	B	O	"->"	10	N	E	X	A	M	P	L
10	N	E	X	A	M	P	L	"->"	8	E	O	F	D	O	U	B
2	D	C	O	L	U	M	N	"->"	1	U	S	I	N	G	B	O
3	S	I	T	I	O	N	X	"->"	2	D	C	O	L	U	M	N
4	N	C	I	P	H	E	R	"->"	3	S	I	T	I	O	N	X
5	T	H	R	O	W	A	N	"->"	4	N	C	I	P	H	E	R
6	T	R	A	N	S	P	O	"->"	5	T	H	R	O	W	A	N
8	E	O	F	D	O	U	B	"->"	6	T	R	A	N	S	P	O
9	P	O	S	I	T	I	O	"->"	9	P	O	S	I	T	I	O
11	L	E	T	R	A	N	S	"->"	11	L	E	T	R	A	N	S

Row 8 is the only row that can
finish the "E" in example. It
also adds "of", which makes
logical sense in a sentence.

c)

	5	1	4	6	3	7	2			5	1	4	6	3	7	2
7	T	H	I	S	I	S	A	"->"	7	T	H	I	S	I	S	A
10	N	E	X	A	M	P	L	"->"	10	N	E	X	A	M	P	L
8	E	O	F	D	O	U	B	"->"	8	E	O	F	D	O	U	B
1	U	S	I	N	G	B	O	"->"	11	L	E	T	R	A	N	S
2	D	C	O	L	U	M	N	"->"	1	U	S	I	N	G	B	O
3	S	I	T	I	O	N	X	"->"	2	D	C	O	L	U	M	N
4	N	C	I	P	H	E	R	"->"	3	S	I	T	I	O	N	X
5	T	H	R	O	W	A	N	"->"	4	N	C	I	P	H	E	R
6	T	R	A	N	S	P	O	"->"	5	T	H	R	O	W	A	N
9	P	O	S	I	T	I	O	"->"	6	T	R	A	N	S	P	O
11	L	E	T	R	A	N	S	"->"	9	P	O	S	I	T	I	O

Row 11 is the only row that can finish the "LE" in double.

d)

	5	1	4	6	3	7	2			5	1	4	6	3	7	2
7	T	H	I	S	I	S	A	"->"	7	T	H	I	S	I	S	A
10	N	E	X	A	M	P	L	"->"	10	N	E	X	A	M	P	L
8	E	O	F	D	O	U	B	"->"	8	E	O	F	D	O	U	B
11	L	E	T	R	A	N	S	"->"	11	L	E	T	R	A	N	S
1	U	S	I	N	G	B	O	"->"	9	P	O	S	I	T	I	O
2	D	C	O	L	U	M	N	"->"	1	U	S	I	N	G	B	O
3	S	I	T	I	O	N	X	"->"	2	D	C	O	L	U	M	N
4	N	C	I	P	H	E	R	"->"	3	S	I	T	I	O	N	X
5	T	H	R	O	W	A	N	"->"	4	N	C	I	P	H	E	R
6	T	R	A	N	S	P	O	"->"	5	T	H	R	O	W	A	N
9	P	O	S	I	T	I	O	"->"	6	T	R	A	N	S	P	O

Row 11 finishes with "TRANS", the only remaining row that completes an actual word is row 9. It makes "TRANSPOSITION".

e)

	5	1	4	6	3	7	2			5	1	4	6	3	7	2
7	T	H	I	S	I	S	A	"->"	7	T	H	I	S	I	S	A
10	N	E	X	A	M	P	L	"->"	10	N	E	X	A	M	P	L
8	E	O	F	D	O	U	B	"->"	8	E	O	F	D	O	U	B
11	L	E	T	R	A	N	S	"->"	11	L	E	T	R	A	N	S
9	P	O	S	I	T	I	O	"->"	9	P	O	S	I	T	I	O
1	U	S	I	N	G	B	O	"->"	4	N	C	I	P	H	E	R
2	D	C	O	L	U	M	N	"->"	1	U	S	I	N	G	B	O
3	S	I	T	I	O	N	X	"->"	2	D	C	O	L	U	M	N
4	N	C	I	P	H	E	R	"->"	3	S	I	T	I	O	N	X
5	T	H	R	O	W	A	N	"->"	5	T	H	R	O	W	A	N
6	T	R	A	N	S	P	O	"->"	6	T	R	A	N	S	P	O

Row 4 is the only one with the necessary "N" to finish "POSITION". It also adds a full word afterwards (CIPHER) that makes logical sense in the sentence.

f)

	5	1	4	6	3	7	2			5	1	4	6	3	7	2
7	T	H	I	S	I	S	A	"->"	7	T	H	I	S	I	S	A
10	N	E	X	A	M	P	L	"->"	10	N	E	X	A	M	P	L
8	E	O	F	D	O	U	B	"->"	8	E	O	F	D	O	U	B
11	L	E	T	R	A	N	S	"->"	11	L	E	T	R	A	N	S
9	P	O	S	I	T	I	O	"->"	9	P	O	S	I	T	I	O
4	N	C	I	P	H	E	R	"->"	4	N	C	I	P	H	E	R
1	U	S	I	N	G	B	O	"->"	1	U	S	I	N	G	B	O
2	D	C	O	L	U	M	N	"->"	2	D	C	O	L	U	M	N
3	S	I	T	I	O	N	X	"->"	3	S	I	T	I	O	N	X
5	T	H	R	O	W	A	N	"->"	5	T	H	R	O	W	A	N
6	T	R	A	N	S	P	O	"->"	6	T	R	A	N	S	P	O

Row 4 ends with "CIPHER", so now we must start a new word. Row 1, 5 and 6 make words at the start of the row. Row 1 makes the most sense as it progresses the sentence logically (Adds "USING").

g)

	5	1	4	6	3	7	2			5	1	4	6	3	7	2
7	T	H	I	S	I	S	A	"->"	7	T	H	I	S	I	S	A
10	N	E	X	A	M	P	L	"->"	10	N	E	X	A	M	P	L
8	E	O	F	D	O	U	B	"->"	8	E	O	F	D	O	U	B
11	L	E	T	R	A	N	S	"->"	11	L	E	T	R	A	N	S
9	P	O	S	I	T	I	O	"->"	9	P	O	S	I	T	I	O
4	N	C	I	P	H	E	R	"->"	4	N	C	I	P	H	E	R
1	U	S	I	N	G	B	O	"->"	1	U	S	I	N	G	B	O
2	D	C	O	L	U	M	N	"->"	5	T	H	R	O	W	A	N
3	S	I	T	I	O	N	X	"->"	2	D	C	O	L	U	M	N
5	T	H	R	O	W	A	N	"->"	3	S	I	T	I	O	N	X
6	T	R	A	N	S	P	O	"->"	6	T	R	A	N	S	P	O

Row 1 ends with an unfished word. Row 5 is the only row that makes a logical word.

h)

	5	1	4	6	3	7	2			5	1	4	6	3	7	2
7	T	H	I	S	I	S	A	"->"	7	T	H	I	S	I	S	A
10	N	E	X	A	M	P	L	"->"	10	N	E	X	A	M	P	L
8	E	O	F	D	O	U	B	"->"	8	E	O	F	D	O	U	B
11	L	E	T	R	A	N	S	"->"	11	L	E	T	R	A	N	S
9	P	O	S	I	T	I	O	"->"	9	P	O	S	I	T	I	O
4	N	C	I	P	H	E	R	"->"	4	N	C	I	P	H	E	R
1	U	S	I	N	G	B	O	"->"	1	U	S	I	N	G	B	O
5	T	H	R	O	W	A	N	"->"	5	T	H	R	O	W	A	N
2	D	C	O	L	U	M	N	"->"	2	D	C	O	L	U	M	N
3	S	I	T	I	O	N	X	"->"	3	S	I	T	I	O	N	X
6	T	R	A	N	S	P	O	"->"	6	T	R	A	N	S	P	O

Row 2 would complete a phrase; "row and column".

i)

	5	1	4	6	3	7	2			5	1	4	6	3	7	2
7	T	H	I	S	I	S	A	"->"	7	T	H	I	S	I	S	A
10	N	E	X	A	M	P	L	"->"	10	N	E	X	A	M	P	L
8	E	O	F	D	O	U	B	"->"	8	E	O	F	D	O	U	B
11	L	E	T	R	A	N	S	"->"	11	L	E	T	R	A	N	S
9	P	O	S	I	T	I	O	"->"	9	P	O	S	I	T	I	O
4	N	C	I	P	H	E	R	"->"	4	N	C	I	P	H	E	R
1	U	S	I	N	G	B	O	"->"	1	U	S	I	N	G	B	O
5	T	H	R	O	W	A	N	"->"	5	T	H	R	O	W	A	N
2	D	C	O	L	U	M	N	"->"	2	D	C	O	L	U	M	N
3	S	I	T	I	O	N	X	"->"	6	T	R	A	N	S	P	O
6	T	R	A	N	S	P	O	"->"	3	S	I	T	I	O	N	X

Row 2 ends with "COLUMN", so we will have to start a new word. Row 6 is the only one to start an actual word. This also makes sense because row 3 would finish off row 6's word.

j) Fully decrypted and translated cipher text:

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

"This is an example of a double transposition cipher using both row and column transposition."

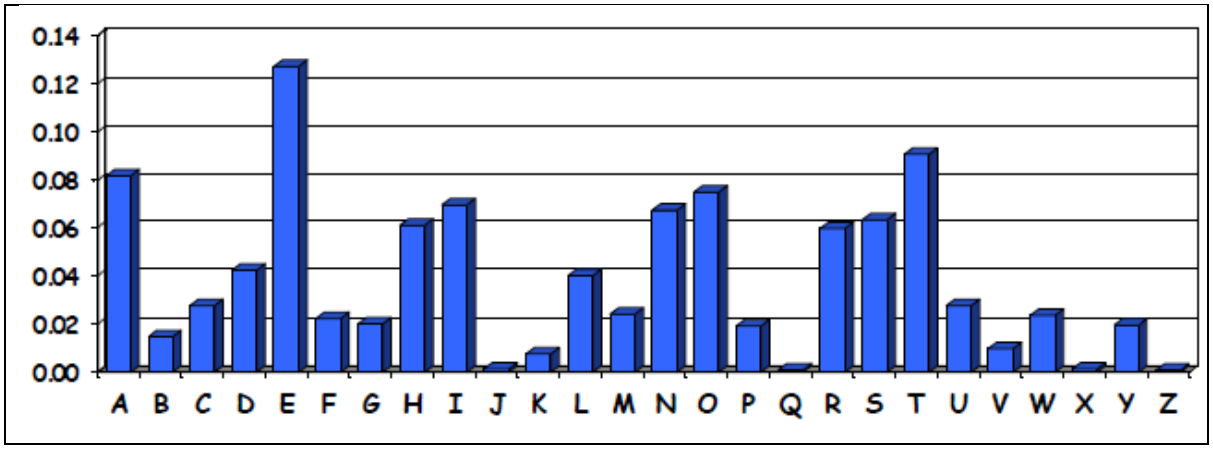
b) [Cryptanalysis on Simple Substitution Cipher]

Cipher Text:	**U**	**M**	**Y**	**T**	**M**	**H**	**U**	**Z**	**S**	**R**	**G**	**Z**
n = 25	V	N	Z	U	N	I	V	A	T	S	H	A
n = 24	W	O	A	V	O	J	W	B	U	T	I	B
n = 23	X	P	B	W	P	K	X	C	V	U	J	C
n = 22	Y	Q	C	X	Q	L	Y	D	W	V	K	D
n = 21	Z	R	D	Y	R	M	Z	E	X	W	L	E
n = 20	A	S	E	Z	S	N	A	F	Y	X	M	F
n = 19	B	T	F	A	T	O	B	G	Z	Y	N	G
n = 18	C	U	G	B	U	P	C	H	A	Z	O	H
n = 17	D	V	H	C	V	Q	D	I	B	A	P	I
n = 16	E	W	I	D	W	R	E	J	C	B	Q	J
n = 15	F	X	J	E	X	S	F	K	D	C	R	K
n = 14	G	Y	K	F	Y	T	G	L	E	D	S	L
n = 13	H	Z	L	G	Z	U	H	M	F	E	T	M
n = 12	I	A	M	H	A	V	I	N	G	F	U	N
n = 11	J	B	N	I	B	W	J	O	H	G	V	O
n = 10	K	C	O	J	C	X	K	P	I	H	W	P
n = 9	L	D	P	K	D	Y	L	Q	J	I	X	Q
n = 8	M	E	Q	L	E	Z	M	R	K	J	Y	R
n = 7	N	F	R	M	F	A	N	S	L	K	Z	S
n = 6	O	G	S	N	G	B	O	T	M	L	A	T
n = 5	P	H	T	O	H	C	P	U	N	M	B	U
n = 4	Q	I	U	P	I	D	Q	V	O	N	C	V
n = 3	R	J	V	Q	J	E	R	W	P	O	D	W
n = 2	S	K	W	R	K	F	S	X	Q	P	E	X
n = 1	T	L	X	S	L	G	T	Y	R	Q	F	Y
Plain Text:	I am having fun											

c) [Cryptanalysis on Substitution Cipher]

XDJ MJXDGSGQGVK FJDHNS OBJECJNTK UNUQKWHW BJQHJW GN XDJ OUTX XDUX HN UNK QUNVCUVJ, JUTD QJXXJB DUW HXW GRN ZJBWGNUQHXK. XDJ MGWX GFIHGCW XBUHX XDUX QJXXJBW DUIJ HW XDJ OBJECJNTK RHXD RDHTD XDJK UZZJUB HN U QUNVCUVJ. TQJUBQK HN JNVQHWD XDJ QJXXJB "L" UZZJUBW OUB QJWW OBJECJNXQK XDUN, WUK, "U". HN XHMJW VGNJ FK, HO KGC RUNXJS XG OHNS GCX XDJ OBJECJNTHJW GO QJXXJBW RHXDHN U QUNVCUVJ, KGC DUS XG OHNS U QUBVJ ZHJTJ GO XJAX UNS TGCNX JUTD OBJECJNTK. NGR, DGRJIJB, RJ DUIJ TGMZCXJBW XDUX TUN SG XDJ DUBS RGBP OGB CW. FCX HN OUTX, RJ SGN'X JIJN NJJS XG SG XDHW WXJZ, UW OGB MGWX QUNVCUVJW XDJBJ UBJ SUXUFUWJW GO XDJ QJXXJB OBJECJNTHJW, RDHTD DUIJ FJJN TUQTCQUXJS FK QGGPHNV UX MHQQHGNW GO XJAXW, UNS UBJ XDCW IJBK DHVDQK UTTCBUXJ.

Letter Frequency			
A = 2	H = 31	O = 18	V = 14
B = 30	I = 7	P = 2	W = 31
C = 21	J = 80	Q = 25	X = 60
D = 36	K = 17	R = 11	Y = 0
E = 6	L = 1	S = 15	Z = 8
F = 7	M = 6	T = 20	
G = 34	N = 39	U = 54	



- Based on the frequency of letters in the English language, “J” (Which has a frequency of 80 in the passage) is most likely “E”

XDE MEXDGSGQGVK FEDHNS OBEECENTK UNUQKWHW BEQHEW GN XDE OUTX XDUX HN UNK QUNVCUVE, EUTD QEXXEB DUW HXW GRN ZEBWGNUQHXK. XDE MGWX GFIHGCW XBUHX XDUX QEXXEBW DUIE HW XDE OBEECENTK RHXD RDHTD XDEK UZZEUB HN U QUNVCUVE. TQEUBQK HN ENVQHWD XDE QEXXEB "L" UZZEUBW OUB QEWW OBEECENXQK XDUN, WUK, "U". HN XHMEW VGNE FK, HO KGC RUNXES XG OHNS GCX XDE OBEECENTHEW GO QEXXEBW RHXDHN U QUNVCUVE, KGC DUS XG OHNS U QUBVE ZHETE GO XEAX UNS TGCNX EUTD OBEECENTK. NGR, DGREIEB, RE DUIE TGMZCXEBW XDUX TUN SG XDE DUBS RGBP OGB CW. FCX HN OUTX, RE SGN'X EIEN NEES XG SG XDHW WXEZ, UW OGB MGWX QUNVCUVEW XDEBE UBE SUXUFUWEW GO XDE QEXXEB OBEECENTHEW, RDHTD DUIE FEEN TUQTCQUXES FK QGGPHNV UX MHQQHGNW GO XEAXW, UNS UBE XDCW IEBK DHVDQK UTTCBUXE.

- From some observation, it appears “XDE” is a common word in the passage, likely being “The”, thus “X” and “D” could be “T” and “H” respectively
- Furthermore, “X” in the passage has a frequency of 60 and “T” is the second most common letter in the English language

THE METHGSGQGVK FEHHNS OBEECENTK UNUQKWHW BEQHEW GN THE OUTT THUT HN UNK QUNVCUVE, EUTH QETTEB HUW HTW GRN ZEBWGNUQHTK. THE MGWT GFIHGCW TBUHT THUT QETTEBW HUIE HW THE OBEECENTK RHTH RHHTH THEK UZZEUB HN U QUNVCUVE. TQEUBQK HN ENVQHWH THE QETTEB "L" UZZEUBW OUB QEWW OBEECENTQK THUN, WUK, "U". HN THMEW VGNE FK, HO KGC RUNTES TG OHNS GCT THE OBEECENTHEW GO QETTEBW RHTHHN U QUNVCUVE, KGC HUS TG OHNS U QUBVE ZHETE GO TEAT UNS TGCNT EUTH OBEECENTK. NGR, HGREIEB, RE HUIE TGMZCTEBW THUT TUN SG THE HUBS RGBP OGB CW. FCT HN OUTT, RE SGN'T EIEN NEES TG SG THHW WTEZ, UW OGB MGWT QUNVCUVEW THEBE UBE SUTUFUWEW GO THE QETTEB OBEECENTHEW, RHHTH HUIE FEEN TUQTCQUTES FK QGGPHNV UT MHQQHGNW GO TEATW, UNS UBE THCW IEBK HHVHQK UTTCBUTE.

- “U” has a frequency of 54 in the passage and “A” is the next most common letter in the English language, thus “U” could be “A”

THE M**ETH**GSGQGVK F**EH**HNS OB**E**EC**E**NTK **A**N**A**QKWHW B**E**QH**E**W GN **THE** O**A**T**T** **THAT** HN **A**NK Q**A**NVC**A**V**E**, **EA**T**H** Q**ETTE**B **HA**W HT**W** GRN Z**E**BWGN**A**QH**T**K. **THE** MGW**T** GFIHGCW **T**B**A**H**T** **THAT** Q**ETTE**BW **HA**I**E** HW **THE** OB**E**EC**E**NTK RH**TH** R**H**HT**H** **THE**K **A**ZZ**EA**B HN **A** Q**A**NVC**A**V**E**. TQ**EA**BQK HN **E**NVQHW**H** **THE** Q**ETTE**B "L" **A**ZZ**EA**BW O**A**B QEWW OB**E**EC**E**NTQK **THA**N, W**A**K, "**A**". HN **T**HM**E**W VGN**E** FK, HO KGC R**A**N**TE**S **T**G OHNS GC**T** **THE** OB**E**EC**E**NTH**E**W GO Q**ETTE**BW RH**TH**HN **A** Q**A**NVC**A**V**E**, KGC **HA**S **T**G OHNS **A** Q**A**BV**E** ZH**E**T**E** GO **TE**A**T** **A**NS TGCN**T** **EA**T**H** OB**E**EC**E**NTK. NGR, **H**GR**E**I**E**B, R**E** **HA**I**E** TGMZC**TE**BW **THAT** T**A**N SG **THE** **HA**BS RGBP OGB CW. FC**T** HN O**A**T**T**, R**E** SGN'**T** **E**I**E**N N**EE**S **T**G SG **TH**HW W**TE**Z, **A**W OGB MGW**T** Q**A**NVC**A**V**E**W **THE**B**E** A**B**E S**ATA**F**A**W**E**W GO **THE** Q**ETTE**B OB**E**EC**E**NTH**E**W, R**H**HT**H** **HA**I**E** F**EE**N T**A**QTCQ**ATE**S FK QGGPHNV **AT** MHQQHGNW GO **TE**A**T**W, **A**NS **A**B**E** **TH**CW I**E**BK **H**HV**H**QK **A**TTCB**ATE**.

- “GO” appears a lot, this could be a common two letter word like “Of”

THE M**ETHO**S**O**Q**O**VK F**EH**HNS **F**B**E**EC**E**NTK **A**N**A**QKWHW B**E**QH**E**W **O**N **THE** **FA**T**T** **THAT** HN **A**NK Q**A**NVC**A**V**E**, **EA**T**H** Q**ETTE**B **HA**W HT**W** **O**RN Z**E**BW**O**N**A**QH**T**K. **THE** M**O**W**T** **O**FIH**O**CW **T**B**A**H**T** **THAT** Q**ETTE**BW **HA**I**E** HW **THE** **F**B**E**EC**E**NTK RH**TH** R**H**HT**H** **THE**K **A**ZZ**EA**B HN **A** Q**A**NVC**A**V**E**. TQ**EA**BQK HN **E**NVQHW**H** **THE** Q**ETTE**B "L" **A**ZZ**EA**BW **FA**B QEWW **F**B**E**EC**E**NTQK **THA**N, W**A**K, "**A**". HN **T**HM**E**W V**O**N**E** FK, H**F** K**O**C R**A**N**TE**S **TO** **F**HNS **O**C**T** **THE** **F**B**E**EC**E**NTH**E**W **OF** Q**ETTE**BW RH**TH**HN **A** Q**A**NVC**A**V**E**, K**O**C **HA**S **TO** **F**HNS **A** Q**A**BV**E** ZH**E**T**E** **OF** **TE**A**T** **A**NS T**O**CN**T** **EA**T**H** **F**B**E**EC**E**NTK. N**O**R, **HO**R**E**I**E**B, R**E** **HA**I**E** T**O**MZC**TE**BW **THAT** T**A**N S**O** **THE** **HA**BS R**O**BP **FO**B CW. FC**T** HN **FA**T**T**, R**E** S**O**N'**T** **E**I**E**N N**EE**S **TO** S**O** **TH**HW W**TE**Z, **A**W **FO**B M**O**W**T** Q**A**NVC**A**V**E**W **THE**B**E** A**B**E S**ATA**F**A**W**E**W **OF** **THE** Q**ETTE**B **F**B**E**EC**E**NTH**E**W, R**H**HT**H** **HA**I**E** F**EE**N T**A**QTCQ**ATE**S FK Q**OO**PHNV **AT** MHQQH**O**NW **OF** **TE**A**T**W, **A**NS **A**B**E** **TH**CW I**E**BK **H**HV**H**QK **A**TTCB**ATE**.

- “**FA**T**T**” could become “Fact”. Thus “T” could be “C”

THE M**ETHO**S**O**Q**O**VK F**EH**HNS **F**B**E**EC**E**N**C**K **A**N**A**QKWHW B**E**QH**E**W **O**N **THE** **FACT** **THAT** HN **A**NK Q**A**NVC**A**V**E**, **EACH** Q**ETTE**B **HA**W HT**W** **O**RN Z**E**BW**O**N**A**QH**T**K. **THE** M**O**W**T** **O**FIH**O**CW **T**B**A**H**T** **THAT** Q**ETTE**BW **HA**I**E** HW **THE** **F**B**E**EC**E**N**C**K RH**TH** R**H**H**CH** **THE**K **A**ZZ**EA**B HN **A** Q**A**NVC**A**V**E**. **C**Q**EA**BQK HN **E**NVQHW**H** **THE** Q**ETTE**B "L" **A**ZZ**EA**BW **FA**B QEWW **F**B**E**EC**E**NTQK **THA**N, W**A**K, "**A**". HN **T**HM**E**W V**O**N**E** FK, H**F** K**O**C R**A**N**TE**S **TO** **F**HNS **O**C**T** **THE** **F**B**E**EC**E**N**C**H**E**W **OF** Q**ETTE**BW RH**TH**HN **A** Q**A**NVC**A**V**E**, K**O**C **HA**S **TO** **F**HNS **A** Q**A**BV**E** ZH**ECE** **OF** **TE**A**T** **A**NS **CO**CN**T** **EACH** **F**B**E**EC**E**N**C**K. N**O**R, **HO**R**E**I**E**B, R**E** **HA**I**E** **CO**MZC**TE**BW **THAT** **CA**N S**O** **THE** **HA**BS R**O**BP **FO**B CW. FC**T** HN **FACT**, R**E** S**O**N'**T** **E**I**E**N N**EE**S **TO** S**O** **TH**HW W**TE**Z, **A**W **FO**B M**O**W**T** Q**A**NVC**A**V**E**W **THE**B**E** A**B**E S**ATA**F**A**W**E**W **OF** **THE** Q**ETTE**B **F**B**E**EC**E**N**C**H**E**W, R**H**H**CH** **HA**I**E** F**EE**N **CA**Q**C**CQ**ATE**S FK Q**OO**PHNV **AT** MHQQH**O**NW **OF** **TE**A**T**W, **A**NS **A**B**E** **TH**CW I**E**BK **H**HV**H**QK **ACC**B**ATE**.

- The last word in the passage looks to be “Accurate”. Thus “C” could be “U” and “B” could be “R”

THE METHOSOQOVK FEHHNS FREEUENCK ANAQKWHW REQHEW ON THE FACT THAT HN ANK QANVUAVE, EACH QETTER HAW HTW ORN ZERWONAQHTK. THE MOWT OFIHOUW TRAHT THAT QETTERW HAIE HW THE FREEUENCK RHTH RHHCH THEK AZZEAR HN A QANVUAVE. CQEARQK HN ENVQHWH THE QETTER "L" AZZEARW FAR QEWW FREEUENTQK THAN, WAK, "A". HN THMEW VONE FK, HF KOU RANTES TO FHNS OUT THE FREEUENCHEW OF QETTERW RHTHHN A QANVUAVE, KOU HAS TO FHNS A QARVE ZHECE OF TEAT ANS COUNT EACH FREEUENCK. NOR, HOREIER, RE HAIE COMZUTERW THAT CAN SO THE HARS RORP FOR UW. FUT HN FACT, RE SON'T EIEN NEES TO SO THHW WTEZ, AW FOR MOWT QANVUAVEW THERE ARE SATAFAWEW OF THE QETTER FREEUENCHEW, RHHCH HAIE FEEN CAQCUQATES FK QOOPHNV AT MHQQHONW OF TEATW, ANS ARE THUW IERK HHVHQK ACCURATE.

- **“FREEUENCJEW”** seems to match “frequencies”. Thus “E” would be “Q”, “N” would be “N”, “H” would be “I”, and “W” would be “S”

THE METHOSOQOVK FEHINS FREQUENCK ANAQKSIS REQIES ON THE FACT THAT IN ANK QANVUAVE, EACH QETTER HAS ITS ORN ZERSONAQITK. THE MOST OFIIOUS TRAIT THAT QETTERS HAIE IS THE FREQUENCK RITH RHICH THEK AZZEAR IN A QANVUAVE. CQEARQK IN ENVQISH THE QETTER "L" AZZEARS FAR QESS FREQUENTQK THAN, SAK, "A". IN TIMES VONE FK, IF KOU RANTES TO FINS OUT THE FREQUENCIES OF QETTERS RITHIN A QANVUAVE, KOU HAS TO FINS A QARVE ZIECE OF TEAT ANS COUNT EACH FREQUENCK. NOR, HOREIER, RE HAIE COMZUTERS THAT CAN SO THE HARS RORP FOR US. FUT IN FACT, RE SON'T EIEN NEES TO SO THIS STEZ, AS FOR MOST QANVUAVES THERE ARE SATAFASES OF THE QETTER FREQUENCIES, RHICH HAIE FEEN CAQCUQATES FK QOOPINV AT MIQQIONS OF TEATS, ANS ARE THUS IERK HIVHQK ACCURATE.

- **“CAQCUQATES”** and “QETTERS” indicates that “Q” is “L”

THE METHOSOLOVK FEHINS FREQUENCK ANALKSIS RELIES ON THE FACT THAT IN ANK LANVUAVE, EACH LETTER HAS ITS ORN ZERSONALITK. THE MOST OFIIOUS TRAIT THAT LETTERS HAIE IS THE FREQUENCK RITH RHICH THEK AZZEAR IN A LANVUAVE. CLEARLK IN ENVLISH THE LETTER "L" AZZEARS FAR LESS FREQUENTLK THAN, SAK, "A". IN TIMES VONE FK, IF KOU RANTES TO FINS OUT THE FREQUENCIES OF LETTERS RITHIN A LANVUAVE, KOU HAS TO FINS A LARVE ZIECE OF TEAT ANS COUNT EACH FREQUENCK. NOR, HOREIER, RE HAIE COMZUTERS THAT CAN SO THE HARS RORP FOR US. FUT IN FACT, RE SON'T EIEN NEES TO SO THIS STEZ, AS FOR MOST LANVUAVES THERE ARE SATAFASES OF THE LETTER FREQUENCIES, RHICH HAIE FEEN CALCULATES FK LOOPINV AT MILLIONS OF TEATS, ANS ARE THUS IERK HIVHLK ACCURATE.

- “K” is at the end of words that would spell “Frequently, “Any” etc. if it was “Y”

THE METHOSOLOVY FEHINS FREQUENCY ANALYSIS RELIES ON THE FACT THAT IN ANY LANVUAVE, EACH LETTER HAS ITS ORN ZERSONALITY. THE MOST OFIIOUS TRAIT THAT LETTERS HAIE IS THE FREQUENCY RITH RHICH THEY AZZEAR IN A LANVUAVE. CLEARLY IN ENVLISH THE LETTER "L" AZZEARS FAR LESS FREQUENTLY THAN, SAY, "A". IN TIMES VONE FY, IF YOU RANTES TO FINS OUT THE FREQUENCIES OF LETTERS RITHIN A LANVUAVE, YOU HAS TO FINS A LARVE ZIECE OF TEAT ANS COUNT EACH FREQUENCY. NOR, HOREIER, RE HAIE COMZUTERS THAT CAN SO THE HARS RORP FOR US. FUT IN FACT, RE SON'T EIEN NEES TO SO THIS STEZ, AS FOR MOST LANVUAVES THERE ARE SATAFASES OF THE LETTER FREQUENCIES, RHICH HAIE FEEN CALCULATES FY LOOPINV AT MILLIONS OF TEATS, ANS ARE THUS IERY HIVHLY ACCURATE.

- “R**HICH HA**I**E F**E**EN”** seems to be “Which have been”. Thus, “R” would be “W”, “I” would be “V” and “F” would be “B”

THE M**ETHO**S**OLO**V**Y BEHIN**S **FREQUENCY ANALYSIS RELIES ON THE FACT THAT IN ANY LAN**V**UAV**E**, EACH LETTER HAS ITS OWN** Z**ERSONALITY**. **THE** M**OST OBVIOUS TRAIT THAT LETTERS HAVE IS THE FREQUENCY WITH WHICH THEY A**ZZ**EAR IN A LAN**V**UAV**E**. CLEARLY IN EN**V**LISH THE LETTER** "L" **A**ZZ**EARS FAR LESS FREQUENTLY THAN, SAY,** "**A**". **IN TI**M**ES** V**ONE BY, IF YOU WANTE**S **TO FIN**S **OUT THE FREQUENCIES OF LETTERS WITHIN A LAN**V**UAV**E**, YOU HA**S **TO FIN**S **A LAR**V**E** Z**IECE OF TEAT AN**S **COUNT EACH FREQUENCY**. **NOW, HOWEVER, WE HAVE CO**MZ**UTERS THAT CAN S**O **THE HAR**S **WOR**P **FOR US**. **BUT IN FACT, WE S**O**N'T EVEN NEE**S **TO S**O **THIS STE**Z, **AS FOR** M**OST LAN**V**UAV**E**S THERE ARE S**A**TABASES OF THE LETTER FREQUENCIES, WHICH HAVE BEEN CALCULATE**S **BY LOO**P**IN**V **AT** M**ILLIONS OF TE**A**TS, AN**S **ARE THUS VERY HI**V**HLY ACCURATE**.

- “SO” appears a lot, which would be fine if “S’ONT” didn’t appear. Thus, “S” would be “D”

THE M**ETHODOLO**V**Y BEHIND FREQUENCY ANALYSIS RELIES ON THE FACT THAT IN ANY LAN**V**UAV**E, EACH LETTER HAS ITS OWN** Z**ERSONALITY**. **THE** M**OST OBVIOUS TRAIT THAT LETTERS HAVE IS THE FREQUENCY WITH WHICH THEY A**ZZ**EAR IN A LAN**V**UAV**E**. CLEARLY IN EN**V**LISH THE LETTER** "L" **A**ZZ**EARS FAR LESS FREQUENTLY THAN, SAY,** "**A**". **IN TI**M**ES** V**ONE BY, IF YOU WANTED TO FIND OUT THE FREQUENCIES OF LETTERS WITHIN A LAN**V**UAV**E**, YOU HAD TO FIND A LAR**V**E** Z**IECE OF TE**A**T AND COUNT EACH FREQUENCY**. **NOW, HOWEVER, WE HAVE CO**MZ**UTERS THAT CAN DO THE HARD WOR**P **FOR US**. **BUT IN FACT, WE DON'T EVEN NEED TO DO THIS STE**Z, **AS FOR** M**OST LAN**V**UA**V**ES THERE ARE DATABASES OF THE LETTER FREQUENCIES, WHICH HAVE BEEN CALCULATED BY LOO**P**IN**V **AT** M**ILLIONS OF TE**A**TS, AND ARE THUS VERY HI**V**HLY ACCURATE**.

- “M” and “P” make words such as “Methodology”, “Looking”, “Most” and “Computers” work; thus, they stay the same
- In saying that, if that is true; we can see that “Z” would be “P” for “Computers” and “Personality”, “V” would be “G” for “Looking”, “English” and “Methodology”, and “P” would be “K” for “Looking and “Work”

THE METHODOLOGY BEHIND FREQUENCY ANALYSIS RELIES ON THE FACT THAT IN ANY LANGUAGE, EACH LETTER HAS ITS OWN PERSONALITY. THE MOST OBVIOUS TRAIT THAT LETTERS HAVE IS THE FREQUENCY WITH WHICH THEY APPEAR IN A LANGUAGE. CLEARLY IN ENGLISH THE LETTER "L" **APPEARS FAR LESS FREQUENTLY THAN, SAY,** "**A**". **IN TIMES GONE BY, IF YOU WANTED TO FIND OUT THE FREQUENCIES OF LETTERS WITHIN A LANGUAGE, YOU HAD TO FIND A LARGE PIECE OF TE**A**T AND COUNT EACH FREQUENCY. NOW, HOWEVER, WE HAVE COMPUTERS THAT CAN DO THE HARD WORK FOR US. BUT IN FACT, WE DON'T EVEN NEED TO DO THIS STEP, AS FOR MOST LANGUAGES THERE ARE DATABASES OF THE LETTER FREQUENCIES, WHICH HAVE BEEN CALCULATED BY LOOKING AT MILLIONS OF TE**A**TS, AND ARE THUS VERY HIGHLY ACCURATE**.

- In logical sense “L” would be “Z” for the A to Z comparison in the sentence, that leaves “A” in the passage, which fits into “**TE**A**T(S)**”, making “A” “X”

THE METHODOLOGY BEHIND FREQUENCY ANALYSIS RELIES ON THE FACT THAT IN ANY LANGUAGE, EACH LETTER HAS ITS OWN PERSONALITY. THE MOST OBVIOUS TRAIT THAT LETTERS HAVE IS THE FREQUENCY WITH WHICH THEY APPEAR IN A LANGUAGE. CLEARLY IN ENGLISH THE LETTER "Z" APPEARS FAR LESS FREQUENTLY THAN, SAY, "A". IN TIMES GONE BY, IF YOU WANTED TO FIND OUT THE FREQUENCIES OF LETTERS WITHIN A LANGUAGE, YOU HAD TO FIND A LARGE PIECE OF TEXT AND COUNT EACH FREQUENCY. NOW, HOWEVER, WE HAVE COMPUTERS THAT CAN DO THE HARD WORK FOR US. BUT IN FACT, WE DON'T EVEN NEED TO DO THIS STEP, AS FOR MOST LANGUAGES THERE ARE DATABASES OF THE LETTER FREQUENCIES, WHICH HAVE BEEN CALCULATED BY LOOKING AT MILLIONS OF TEXTS, AND ARE THUS VERY HIGHLY ACCURATE.

Question 2 [Application of Hash Algorithm]

i) 1) Since Trudy knows the range of the bids, she can calculate the hash values of $95 to $103 using the SHA-256 Algorithm as well.
2) She can then compare her calculated hash values of $95, $103 and the intervals between with Alice and Bob hash values.
3) Once she determines the bids of Alice and Bob, all Trudy needs to do is bit slightly higher than both
4) Trudy wins the auction

ii) To prevent people like Trudy, the auction process can be modified in how they encode the bids into has values. Have bidders add a number to the bid amount (E.g. $100 + 51 = 151) and encode that using SHA-256. Once bidding is over, have the bidders send their additional number to the auctioneer; who will then subtract the number from the hashed value to find the bid amount. This way, if people like Trudy figure out bidder’s hashed values; they still won’t know the actual bid without knowledge of the additional umber

Question 3 [RSA Encryption algorithm]

a) Generating the Public Key

$p = 443$

$q = 503$

$n = 443 \times 503 = 222{,}829$

$\varphi(n) = (443 - 1) \times (503 - 1) = 442 \times 502 = 221{,}884$

$e = 3 \quad (221{,}884 \div 3 = 73{,}961.33) \therefore \gcd(221884, 3) = 1$

Public Key: $(222829, 3)$

b) Generating the Private Key

$\varphi(n) = 221{,}884$

$e = 3$

$d \times 3 = 1 \bmod 221{,}884$

$d = 147{,}923$

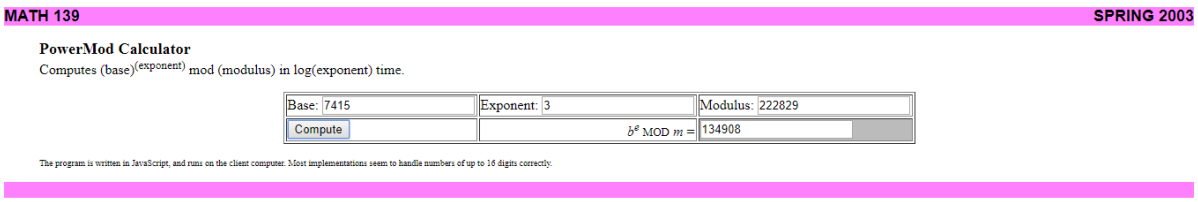
c) Encrypting the Message with the Public Key

$n = 222{,}829$

$e = 3$

$M = 7415$

$C = 7415^3 \bmod 222{,}829$



$C = 134908$

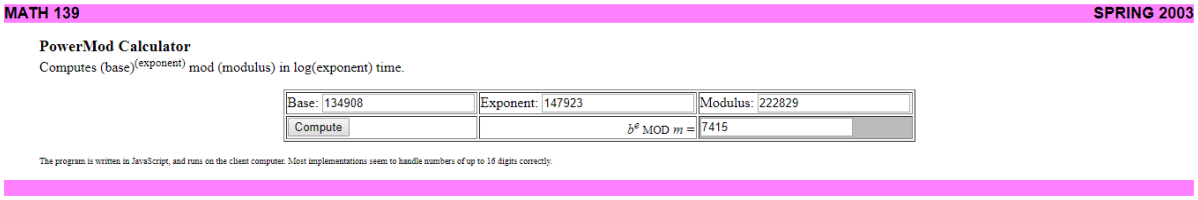
d) Decrypting the Message with the Private Key

$n = 222{,}829$

$C = 8166$

$d = 147{,}923$

$M = 134908^{147{,}923} \bmod 222{,}829$



$M = 7415$

Question 4 [Breaking RSA Encryption algorithm]

a) Determining p and q

$C = 1602$

$n = 3901$

$e = 11$

$p \times q = 3901 \therefore p = 47, q = 83$ (Both prime)

b) Determining $\varphi(n)$

$p = 47$

$q = 83$

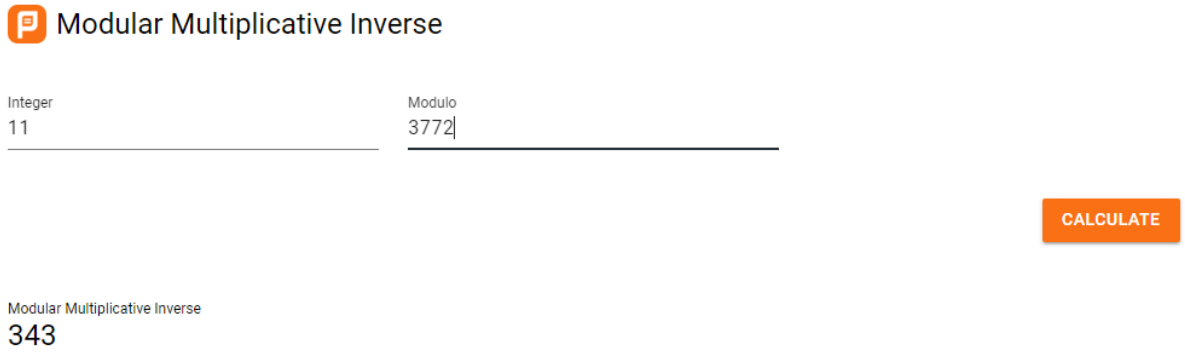
$\varphi(n) = (47 - 1) \times (83 - 1) = 46 \times 82 = 3{,}772$

c) Determining the Private Key

$\varphi(n) = 3{,}772$

$e = 11$

$d \times 11 = 1 \bmod 3{,}772$



$d = 343$

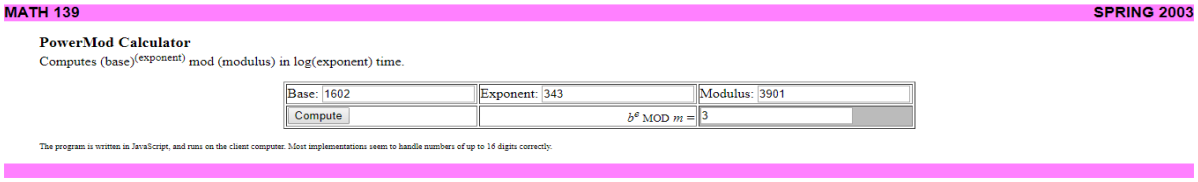
d) Decrypt the Message using the Private Key

$n = 3901$

$C = 1602$

$d = 343$

$M = 1602^{343} \bmod 3901$



$M = 3$

Question 5 [ElGamal Encryption algorithm]

a) Calculating y

$M = 59$

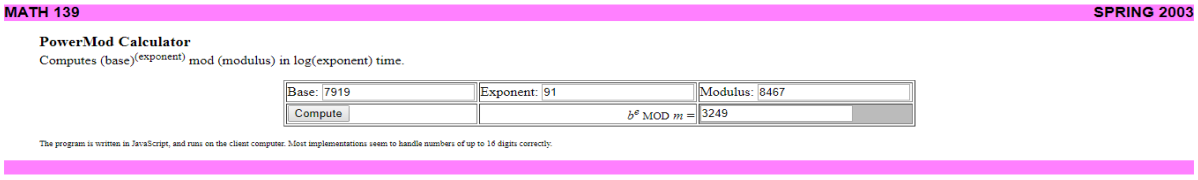
$p = 8467$

$g = 7919$

$x = 91$

$r = 51$

$y = 7919^{91} \bmod 8467$



$y = 3249$

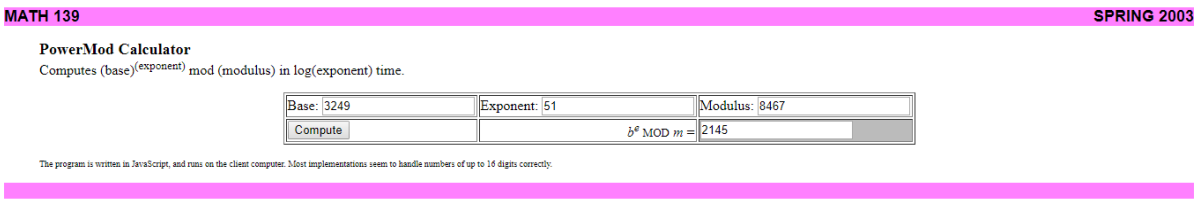
b) Calculating k

$r = 51$

$y = 3249$

$p = 8467$

$k = 3249^{51} \bmod 8467$



$k = 2145$

c) Generating the 2 cipher texts

$M = 59$

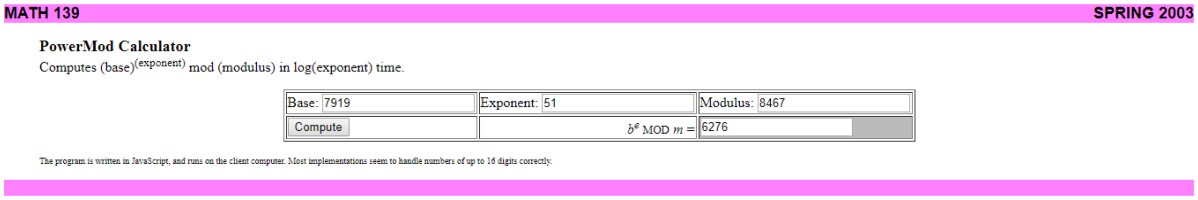
$p = 8467$

$g = 7919$

$r = 51$

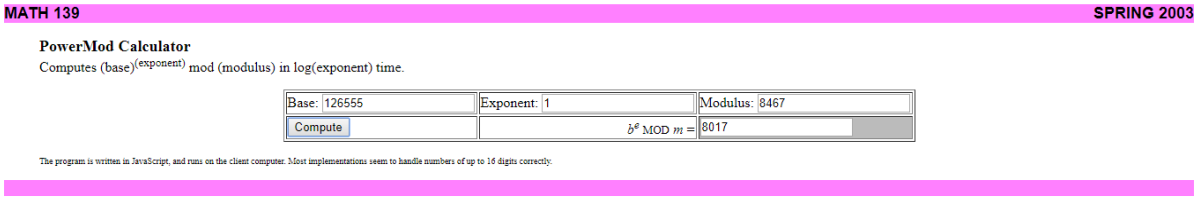
$k = 2145$

$C_1 = 7919^{51} \bmod 8467$



$C_1 = 6276$

$C_2 = 59 \times 2145 \bmod 8467$



$C_2 = 8017$

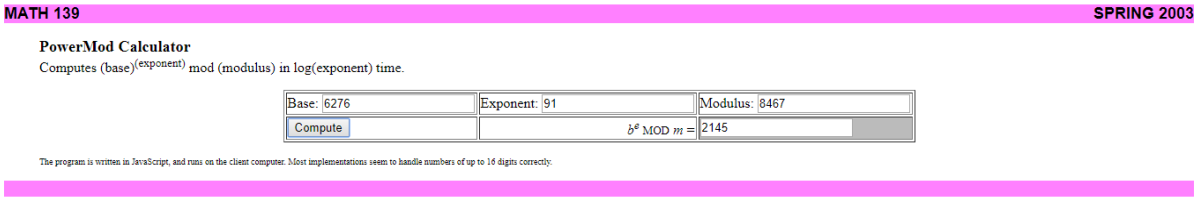
d) Decrypting the message – calculating k and its multiplicative inverse

$x = 91$

$C_1 = 6276$

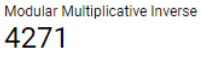
$p = 8467$

$k = 6276^{91} \bmod 8467$



$k = 2145$

$k^{-1} = 2145^{-1} \bmod 8467$



$k^{-1} = 4271$

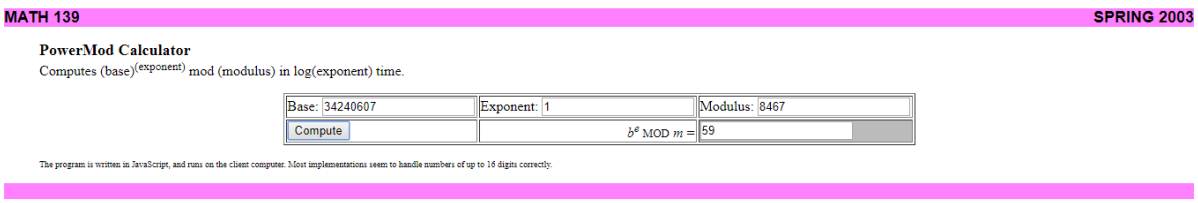
e) Decrypting the encrypted message

$C_2 = 8017$

$k^{-1} = 4271$

$p = 8467$

$m = 4271 \times 8017 \bmod 8467$



$m = 59$

Question 6 [Paillier Encryption algorithm]

a) Calculating n

$M = 1234$

$p = 61$

$q = 97$

$g = 119$

$r = 67$

$n = 61 \times 97 = 5917$

b) Calculating ƛ

$p = 61$

$q = 97$

$ƛ = \text{lcm}(61 - 1, 97 - 1) = \text{lcm}(60,96) = 480$

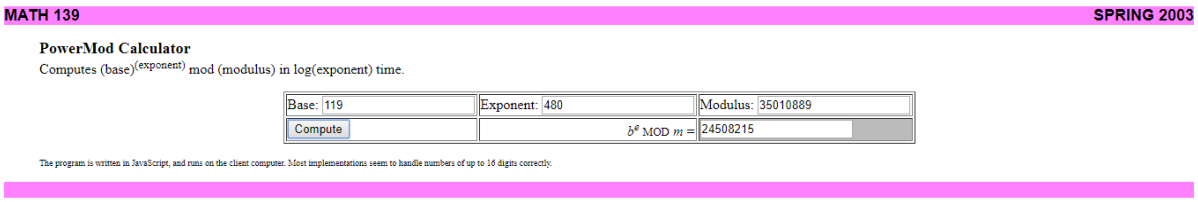
c) Calculating k

$g = 119$

$n = 5917$

$ƛ = 480$

$k = L(119^{480} \bmod 5917^2) = L(119^{480} \bmod 35010889)$



$k = L(24508215) = (24508215 - 1) \div 5917 = 4142$

d) Calculating μ

$k = 4142$

$n = 5917$

$\mu = 4142^{-1} \bmod 5917$

Modular Multiplicative Inverse

Integer: 4142

Modulo: 5917

CALCULATE

Modular Multiplicative Inverse
10

$\mu = 10$

e) Encrypting the message

$g = 119$

$M = 1234$

$r = 67$

$n = 5917$

$c = 119^{1234} \times 67^{5917} \bmod 5917^2 = (119^{1234} \bmod 35010889 \times 67^{5917} \bmod 35010889) \bmod 35010889$

MATH 139 **SPRING 2003**

PowerMod Calculator

Computes (base)$^{(exponent)}$ mod (modulus) in log(exponent) time.

Base: 119	Exponent: 1234	Modulus: 35010889
Compute	b^e MOD m =	29522434

The program is written in JavaScript, and runs on the client computer. Most implementations seem to handle numbers of up to 16 digits correctly.

MATH 139 **SPRING 2003**

PowerMod Calculator

Computes (base)$^{(exponent)}$ mod (modulus) in log(exponent) time.

Base: 67	Exponent: 5917	Modulus: 35010889
Compute	b^e MOD m =	7510496

The program is written in JavaScript, and runs on the client computer. Most implementations seem to handle numbers of up to 16 digits correctly.

$c = (29522434 \times 7510496) \bmod 35010889$

MATH 139 **SPRING 2003**

PowerMod Calculator

Computes (base)$^{(exponent)}$ mod (modulus) in log(exponent) time.

Base: 221728122467264	Exponent: 1	Modulus: 35010889
Compute	b^e MOD m =	31145362

The program is written in JavaScript, and runs on the client computer. Most implementations seem to handle numbers of up to 16 digits correctly.

$c = 31145362$

f) Decrypting the encrypted message

$\lambda = 480$

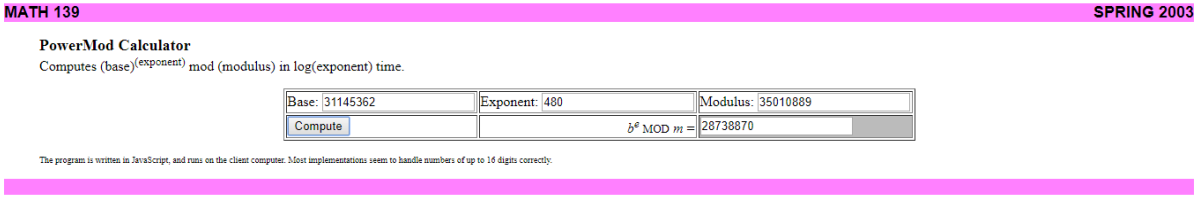
$\mu = 10$

$c = 31145362$

$n = 5917$

$k = 4142$

$M = L(31145362^{480} \bmod 5917^2) \times 10 \bmod 5917$

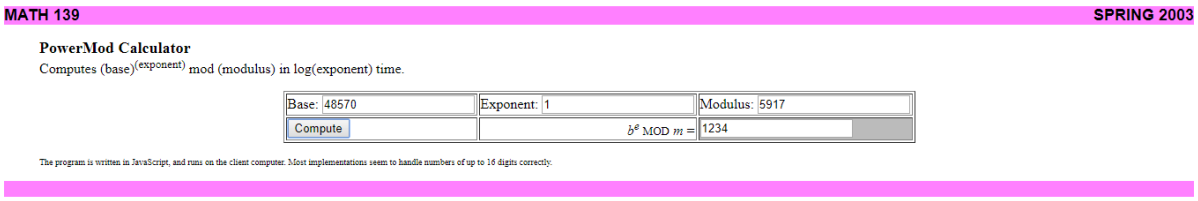


$M = L(28738870) \times 10 \bmod 5917$

$M = ((28738870 - 1) \div 5917) \times 10 \bmod 5917$

$M = 4857 \times 10 \bmod 5917$

$M = 48570 \bmod 5917$



$M = 1234$