Connor Carroll
Will Zhang
Dominik Gonzales
Shashank Mondrati

Activity 7.1

Substitution Ciphers: [5 points]
Read the material in the PDF, complete Exercise 1, 2, 5, 6 and 7 in the PDF linked below. Include your answers to the exercises and the activities in your submission document.
http://www.cimt.org.uk/resources/codes/codes_u1_text.pdf

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

Exercise 1:
JRQH WR ZDWFK KDUOHTXLQV. EDFN DW VHYHQ
GONE TO WATCH HARLEQUINS. BACK AT SEVEN
Exercise 2:
Since there are 26 letters in the alphabet, the alphabet can be shifted 26 times plus 1 which would make it the exact same as the normal alphabet.
Exercise 5:

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

ZHCVHYP NYDCTG SJL GCMO
JANUARY BRINGS THE SNOW
Exercise 6:
There are 3 letters which means there are 3! Different substitution ciphers or **6.**
Exercise 7:

(a) There are 4 letters which means there are 4! Different substitution ciphers or **24**.
(b) There are 5 letters for the mercurian alphabet which means there are 5! Different substitution ciphers or **120**.

Transposition Ciphers: [11 points]
Read the material in the PDF and complete Exercise 1, Activity 1 and Activity 2 in the PDF linked below. Include your answers to the exercises and the activities in your submission document.
http://www.cimt.org.uk/resources/codes/codes_u11_text.pdf
Exercise 1:
TCTES WSGHU ORAAR HESMI LYIT

(a). Count the letters
24
(b). What possibilities are there for the shape of the grid?
6x4

4x6
8x3
3x8
2x12
12x2

(c). Find the correct shape for the grid and then unscramble the message.

T	**S**	**H**	**A**	**E**	**L**
C	**W**	**U**	**A**	**S**	**Y**
T	**S**	**O**	**R**	**M**	**I**
E	**G**	**R**	**H**	**I**	**T**

No

T	**S**	**A**	**M**
C	**G**	**A**	**I**
T	**H**	**R**	**L**
E	**U**	**H**	**Y**
S	**O**	**E**	**I**
W	**R**	**S**	**T**

No

T	**H**	**E**
C	**U**	**S**
T	**O**	**M**
E	**R**	**I**
S	**A**	**L**
W	**A**	**Y**
S	**R**	**I**
G	**H**	**T**

THE CUSTOMER IS ALWAYS RIGHT

Suppose you wanted to scramble the message

A BAYONET IS WEAPON WITH A WORKER AT EACH END

This has 37 letters. The only grids with 37 spaces would have either one row or one column and would not scramble the message. Why not?

This is because you would end up with the same message at the end as there is only one element which is *being scrambled*. You must have multiple elements in both the rows and columns for the message to be scrambled.

Activity 1:

Consider what happens if you add a) 1, b) 2 dummy letters to the message above. What makes you think these are not good choices?

Since there are 37 letters in the message, if we add one we get 38. 38 only divides by 1,2,19, and 38. This gives us only 2 choices for scrambling the message, 2x19 or 19x2. These are poor choices as 2x19 would be easy to reverse because you are merely switching letters in the message. 19x2 would do the same. If we add one more we get 39. Similarly, 39 can only be divided by 1,3,13, and 39. This would give poor scrambling.

Activity 2:

Unscramble the message :

EREAO ELUOT PXEAH HTTHH TTEII SNIOX NEYVB XGBDE EXTSY OML

There are 48 letters. This gives 1x48, 48x1, 2x24, 24x2, 3x16, 16x3, 4x12, 12x4, 6x8, or 8x6. Assuming the X's are dummy letters, we can assume that the grid is 8x6 as the X's are 6 apart.

E	**L**	**E**	**H**	**I**	**N**	**G**	**T**
R	**U**	**A**	**H**	**S**	**E**	**B**	**S**
E	**O**	**H**	**T**	**N**	**Y**	**D**	**Y**
A	**T**	**H**	**T**	**I**	**V**	**E**	**O**
O	**P**	**T**	**E**	**O**	**B**	**E**	**M**
E	**X**	**T**	**I**	**X**	**X**	**X**	**L**

Elehing truah sebseo htnydy athtiveo opteobem etil
44 letters. This is not the right configuration (switch columns)
The X's likely are added at the end so they need to be moved to the right. Then it becomes trial and error for exactly which column goes where. We know that for the letters at the bottom, E,T, I, L, We can spell Tile or Lite. If we have tile, the top left is EHTE which is not a word. If we have Lite, the top left is THEE. Then we move to the X's. The

top letters are L, I, N, G. If we add these to THEE, we get THE ELING. The next step is finding a word or the start of one. ELING can spell LINGE, INGLE, LINEG, ENGLI, and more. Our second row starts with SHAR, using this we can determine ENGLI is the right option.

T	H	E	E	N	G	L	I
S	H	A	R	E	B	U	S
Y	T	H	E	Y	D	O	N
O	T	H	A	V	E	T	I
M	E	T	O	B	E	P	O
L	I	T	E	X	X	X	X

THE ENGLISH ARE BUSY THEY DO NOT HAVE TIME TO BE POLITE.

One-Time Pads: [14 points]
Read the material in the PDF, and complete Exercises 1, 2, and 3 in the PDF linked below. Include your answers to the exercises and the activities in your submission document.
http://www.cimt.org.uk/resources/codes/codes_u12_text.pdf
Exercise 1: NICE ONE CYRIL : CRMZOENIKVJH,
KEEP BRITAIN TIDY: ZNOKBIRZMMOPREF

Exercise 2: CBIR MEF ENTOL, FFGG ZABNMWO DBYJ

Exercise 3:

A) **19 14 1 16 3 18 1 3 11 12 5 16 15 16 -> SNAPCRACKLEPOP**
B) **19 20 15 16 12 15 15 11 12 9 19 20 5 14 -> STOPLOOKLISTEN**
C) **23 8 15 4 1 18 5 19 23 9 14 19 -> WHODARESWINS**

SBVRZ ZENPV ND (MINUEND)
19 2 22 18 26
26 5 14 16 22
14 4

PJKVA RJGME BWJBH (KEY)
16 10 11 22 1
18 10 7 13 5
2 23

16-19 = -3 +26 = 23 = W
10-2 = 8 = H
11-22 = -11 +26 = 15 = O

22-18 = 4 = D
1 -26 = -25 +26 = 1 = A
18-26 = -8 + 26 = 18 = R
10-5 = 5 = E
7 - 14 = -7 +26 = 19 = S
13 - 16 = -3 +26 = 23 = W
5 - 22 = -17 +26 = 9 = I
2 - 14 = -12 +26 = 14 = N
23 - 4 = 19 = S
WHO DARES WINS