UNIVERSITY OF
WATERLOO

Faculty of Mathematics
Waterloo, Ontario N2L 3G1

Centre for Education in
Mathematics and Computing

Grade 7 and 8 Math Circles

March 19th/20th/21st

Crytography

Introduction

Before we begin, it's important to look at some terminology that is important to what we will be learning about.

Plaintext: The original message or information a sender wishes to share with a specific person. It is very easy to read and must be somehow hidden from those that are not intended to see it.

Encryption: The process of encoding the plaintext in such a way that only authorized parties can clearly read it.

Ciphertext: The text created by encrypting plaintext. It looks like gibberish and is very hard to read.

Cipher: A method of transforming a message to conceal its meaning.

Decryption: The opposite of encryption. It is the process of turning ciphertext back into the readable plaintext.

Substitution Cipher

The earliest pieces of evidence of cryptography have been found in Mesopotamian, Egyptian, Chinese, and Indian writings, but it was the Hebrew scholars of 600 to 500 BCE that began to use simple substitution ciphers. In a substitution cipher the alphabet is rewritten in some other order to represent the the substitution.

Caesar Ciphers

The Caesar cipher is the simplest and most famous substitution cipher. It was first used by the famous Roman general Julius Caesar, who developed it to protect important military messages.

To produce a Caesar cipher, simply shift the alphabet some units to the right. Julius Caesar's original cipher was created by shifting the alphabet three units to the right, as shown below.

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	X	Y	Z	A	B	C	D	E	F	G	H	I	J

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	K	L	M	N	O	P	Q	R	S	T	U	V	W

When encrypting a message, match every letter in the plaintext with the corresponding ciphertext letter beneath it. When decrypting a message, match every letter in the ciphertext with the corresponding plaintext letter above it.

Exercise:

1. Set up a Caesar cipher with a right shift of 9 units.

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	R	S	T	U	V	W	X	Y	Z	A	B	C	D

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	E	F	G	H	I	J	K	L	M	N	O	P	Q

2. Encrypt "Math Circles" using the Caesar cipher from part 1.

The plaintext letter "M" corresponds to the ciphertext letter "D."
The plaintext letter "A" corresponds to the ciphertext letter "R."
Continuing this way, you will find that the ciphertext is:

DRKY TZITCVJ

3. Decrypt "SLEEP IRSSZK" using the Caesar cipher from part 1.

The ciphertext letter "S" corresponds to the plaintext letter "B."
The ciphertext letter "A" corresponds to the plaintext letter "U."
Continuing this way, you will find that the plaintext is:

BUNNY RABBIT

Atbash

Atbash is a simple substitution cipher that was originally created using the Hebrew alphabet, though it can be made to work with every alphabet.

The Atbash cipher is created by reversing the alphabet. That is, the plaintext letter "A" becomes the ciphertext letter "Z," the plaintext letter "B" becomes the ciphertext letter "Y," and so on.

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

This is more easily represented below:

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

Exercise:

1. Encrypt "Math Circles" using the Atbash cipher. The plaintext letter "M" corresponds to the ciphertext letter "N."

   The plaintext letter "A" corresponds to the ciphertext letter "Z."

   Continuing this, you will find that the ciphertext is:

   NZGS XRIXOVH

2. Encrypt the word "wizard" using the Atbash cipher. The plaintext letter "W" corresponds to the ciphertext letter "D."

   The plaintext letter "I" corresponds to the ciphertext letter "R."

   Continuing this, you will find that the ciphertext is:

   DRAZIW

   It's "wizard" backwards!

3. Decrypt "ORLM PRMT" using the Atbash cipher. The ciphertext letter "O" corresponds to the plaintext letter "L."
   The ciphertext letter "R" corresponds to the plaintext letter "I."
   Continuing this, you will find that the plaintext is:

   LION KING

The Atbash cipher is a very weak cipher because there is only one possible way to arrange the alphabet in reverse order.

Mixed Alphabet

To use the mixed alphabet substitution cipher you need a *keyword* (a word with either no repeating letters, or any repeating letters removed) and a *keyletter*. Starting under the keyletter, write each of the letters of the keyword into the boxes. Next, fill in the remaining boxes with the letters (in alphabetical order) that were not in your keyword.

Example:

Given a keyword **math** and a keyletter **d** your encryption should follow the pattern below. Since the keyword is math and it has no repeating letters, the word math begins at the keyletter, d.

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext				M	A	T	H						

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext													

Then, the remaining letters of the alphabet are filled in following the keyword, skipping the letters in the keyword. In this case, A through Z will be filled in, skipping M, A, T, and H.

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	X	Y	Z	M	A	T	H	B	C	D	E	F	G

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	I	J	K	L	N	O	P	Q	R	S	U	V	W

Exercise:

1. Set up a mixed alphabet cipher using the keyword SQUARE and the keyletter "E."

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

2. Encrypt "Math Circles" using the mixed alphabet cipher from part 1. The plaintext letter "M" corresponds to the ciphertext letter "D."
   The plaintext letter "A" corresponds to the ciphertext letter "W."
   Continuing this, you will find that the ciphertext is:

   DWLA YRJYCSK

3. Decrypt "QRFZRFU FSDG" using the mixed alphabet cipher from part 1. The ciphertext letter "Q" corresponds to the plaintext letter "F."
   The ciphertext letter "R" corresponds to the plaintext letter "I."
   Continuing this, you will find that the plaintext is:

   FINDING NEMO

Letter to Number Cipher

A **letter to number cipher** is where you change each letter into a number using the following table. Make sure to use two digits for all of the letters.

plaintext	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
ciphertext	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Exercise:

1. Decrypt the following message using the letter to number cipher.

   13 01 20 08 ’ 19   20 08 05   02 05 19 20 !

   Plaintext: Math’s the best!

2. Encrypt the following message.

   Heptadecagon

   Ciphertext: 08 05 16 20 01 04 05 03 01 07 15 14

Word Shift Cipher

A **Word Shift Cipher** is a slightly more complex way to encrypt or decrypt a message. To encrypt, choose a key word or phrase, then add the numerical value of each letter to each letter of the message in the order that they appear.

For example, in the tables below, the first two letters are done for you.

First, we find the numical value for “t” is 20; adding the numerical value for “m,” which is 13, gives 33. Then, to make sure that we have a number in the range of 1 to 26, we add (or subtract) 26 until we get a number in that range. So in this case, we take 33 and subtract 26 to get 7, which gives the letter “g.” The numerical value for “o” is 15; adding the numerical value for “e,” which is 5, gives 20, which gives the letter “t.”

Exercise: Complete the rest of the encrypted message by continuing to loop the keyword "me" through the message and adding the numerical values.

Encryption:

T	20	M	13		$20 + 13 = 33 \to (33 - 26 = 07)$	G
O	15	E	05		$15 + 5 = 20$	T
D		M		$\Longrightarrow$		
A		E				
Y		M				

T	20	M	13		$20 + 13 = 33 \to (33 - 26 = 07)$	G
O	15	E	05		$15 + 5 = 20$	T
D	04	M	13	$\Longrightarrow$	$04 + 13 = 17$	Q
A	01	E	05		$01 + 05 = 06$	F
Y	25	M	13		$25 + 13 = 38 \to (38 - 26 = 12)$	L

Now, if we want to decrypt the message, we subtract the numerical values of the keyword letters instead of adding.

Decryption:

G	07	M	13		$07 - 13 = -06 \to (-06 + 26 = 20)$	T
T	20	E	05		$20 - 05 = 15$	O
		M		$\Longrightarrow$		
		E				
		M				

G	07	M	13		$07 - 13 = -06 \to (-06 + 26 = 20)$	T
T	20	E	05		$20 - 05 = 15$	O
Q	17	M	13	$\Longrightarrow$	$17 - 13 = 04$	D
F	06	E	05		$06 - 05 = 01$	A
L	12	M	13		$12 - 13 = -01 \to (-01 + 26 = 25)$	Y

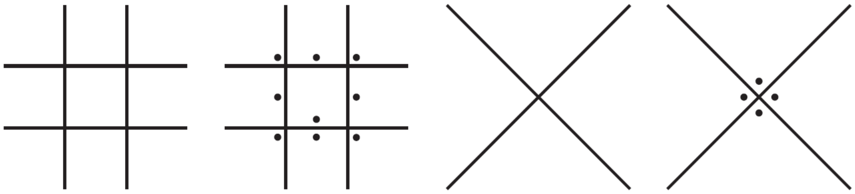
Exercise: Encrypt the following message by looping one of your own keywords through the message and adding the numerical values.

M	
A	
T	
H	
R	
O	
C	
K	
S	

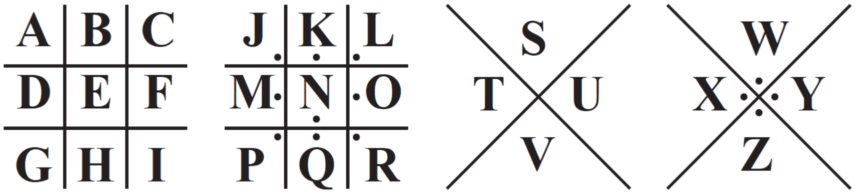
$\Longrightarrow$

Pigpen Cipher

In the Pigpen cipher, we assign all of the letters to a position in the following grid so that each letter has a symbolic representation based on its location.



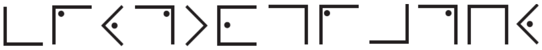
Exercise:



Encrypt the word "cryptography" using the key above.

The letter "C" is found in the upper right corner of the first image in the key, and can be represented by the symbol └. The letter "R" is found in the lower right corner of the second image in the key, and can be represented by the symbol ┌.

Continuing this, you will find that the ciphertext is:



Polybius Square

Developed by the Ancient Greek historian and scholar Polybius, the Polybius Square is another transposition cipher. This cipher utilises a grid and coordinates, representing every letter in the plaintext by a number pair in the ciphertext.

	1	**2**	**3**	**4**	**5**
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Note that the letters “i” and “j” share a cell in the grid.

Exercise:

1. Encrypt “Math Circles” using the Polybius Square. The plaintext letter “M” corresponds to the ciphertext number 32.

   The plaintext letter “A” corresponds to the ciphertext number 11.

   Continuing this, you will find that the ciphertext is:

   32114423 13244213311543

2. Decrypt “45332451154243244454 3421 5211441542313434” using the Polybius Square.

   The ciphertext number 45 corresponds to the plaintext letter “U.”

   The ciphertext number 33 corresponds to the plaintext letter “N.”

   Continuing this, you will find that the plaintext is:

   UNIVERSITY OF WATERLOO

Additional Ciphers

Chaining Cipher

This encryption method combines the concepts of word shift and blocks (splitting your message into groups of a specific size). First, we pick a keyword. Then, the number of letters in that word becomes the key number.

Keyword: FUN Key number: 3

Replace any spaces in the plaintext with a symbol (e.g. a space becomes &).
Split the chain of letters into groups the size of the key number. If you do not have enough letters to fill the last group, fill it in with spaces.

Encrypt MATH CIRCLES

MATH&CIRCLES

MAT H&C IRC LES

Assign every letter its corresponding number. Treat spaces as 27.

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	01	02	03	04	05	06	07	08	09	10	11	12	13

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	14	15	16	17	18	19	20	21	22	23	24	25	26

Plaintext	M	A	T	H	&	C	I	R	C	L	E	S
Plaintext Numbers	13	1	20	8	27	3	9	18	3	12	5	19
Cipher Numbers	6	21	14	19	22	7	27	22	10	9	13	13
Ciphertext Numbers	19	22	7	27	22	10	9	13	13	21	18	5
Ciphertext	S	V	G	&	V	J	I	M	M	U	R	E

The numbers are added down the columns to determine the ciphertext. The Cipher Numbers for the first block are the numbers corresponding to the keyword. Every other block uses the numbers from the previous ciphertext. The numbers chain over, hence the name ”chaining cipher”!

Remember, if you get a number that is larger than 27, you must subtract 27 to get a number corresponding to a letter or space.

Exercise:

1. Encrypt COMPLEX NUMBER with the keyword two.

C	O	M	P	L	E	X	&	N	U	M	B	E	R	&
3	15	13	16	12	5	24	27	14	21	13	2	5	18	27
20	23	15	23	11	1	12	23	6	9	23	20	3	9	22
23	11	1	12	23	6	9	23	20	3	9	22	8	27	22
W	K	A	L	W	F	I	W	T	C	I	V	H	&	V

Ciphertext: WKALWFIWTCIVH V

2. Decrypt WFBEPNGEEEVGQJHZ with the keyword code.

T	R	Y	&	T	H	E	&	P	R	O	B	L	E	M	S
20	18	25	27	20	8	5	27	16	18	15	2	12	5	13	19
3	15	4	5	23	6	2	5	16	14	7	5	5	5	22	7
23	6	2	5	16	14	7	5	5	5	22	7	17	10	8	26
W	F	B	E	P	N	G	E	E	E	V	G	Q	J	H	Z

Plaintext: TRY THE PROBLEMS

Columnar Transposition

In a columnar transposition cipher, your plaintext is written out in rows with the same amount of letters as a given keyword. Then, the columns are read according to the alphabetical order of the keyword to create the ciphertext.

Plaintext: THERE ARE TWO WEEKS LEFT OF MATH CIRCLES
Keyword: CANDY

C	A	N	D	Y
2	1	4	3	5
T	H	E	R	E
A	R	E	T	W
O	W	E	E	K
S	L	E	F	T
O	F	M	A	T
H	C	I	R	C
L	E	S	Q	T

Ciphertext: HRWLFCE TAOSOHL RTEFARQ EEEEMIS EWKTTCT

The notice that in this example there were not enough letters to fill in the last row. In this case random letters are selected to fill in the remaining spaces. These letters are called “nulls”. They should be select such that once decrypted it is clear that they do not add meaning to the message.

Additionally, spaces are ignored when encrypting a message using columnar transposition. It is up to the person doing the decryption to determine where the spaces belong.

Exercise:

1. Decrypt AEPN RCMA PIIT TSRL CIOT with keyword learn.

L	E	A	R	N
3	2	1	5	4
P	R	A	C	T
I	C	E	I	S
I	M	P	O	R
T	A	N	T	L

Plaintext: PRACTICE IS IMPORTANT

Problem Set

1. How do you get a tissue to dance? KPO V GDOOGZ WJJBDZ DI DO
   (Caesar Cipher; 5)
   Put a little boogie in it

2. What do mathematicians eat on Thanksgiving? KFNKPRM KR
   (Atbash)
   Pumpkin pi

3. What geometric figure is like a lost parrot? K BZWHQZY
   (Mixed Alphabet. Keyword: BIRD; Keyletter: "P")
   A polygon

4. What do you call a sleeping bull? F GETTIWDJZ
   (Mixed Alphabet. Keyword: SLEEP; Keyletter: "S")
   A bulldozer

5. The following ciphertext was encrypted using the Polybius Square. What is the plaintext?

   231125453311 321144114411

   Hakuna matata

CHALLENGE

6. The following ciphertext was first encrypted using the Atbash cipher, then it was further encrypted with the Polybius Square. What is the plaintext?

   3451552432423244 5554312122 532412252231442455254312

   Decrypted by Polybius Square:
   O V Z I/J M R M T   Z Y L F G   X I/J B K G L T I/J Z K S B

   Decrypted by Atbash Cipher:
   Learning About Cryptography

7. The following ciphertext was first encrypted using a Caesar cipher with a shift of 3, then it was further encrypted with Atbash, and finally encrypted again using a letter to number cipher with keyword equal. What is the plaintext? (pay attention to which numbers you are subtracting in which order)

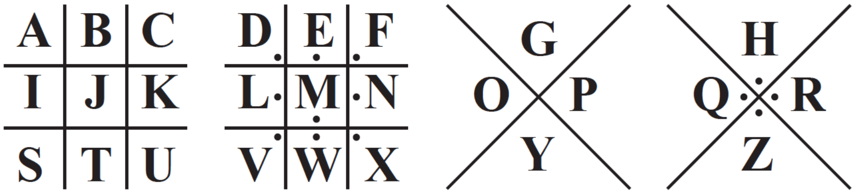
OMPL CZNQK VHJT D SALMZ

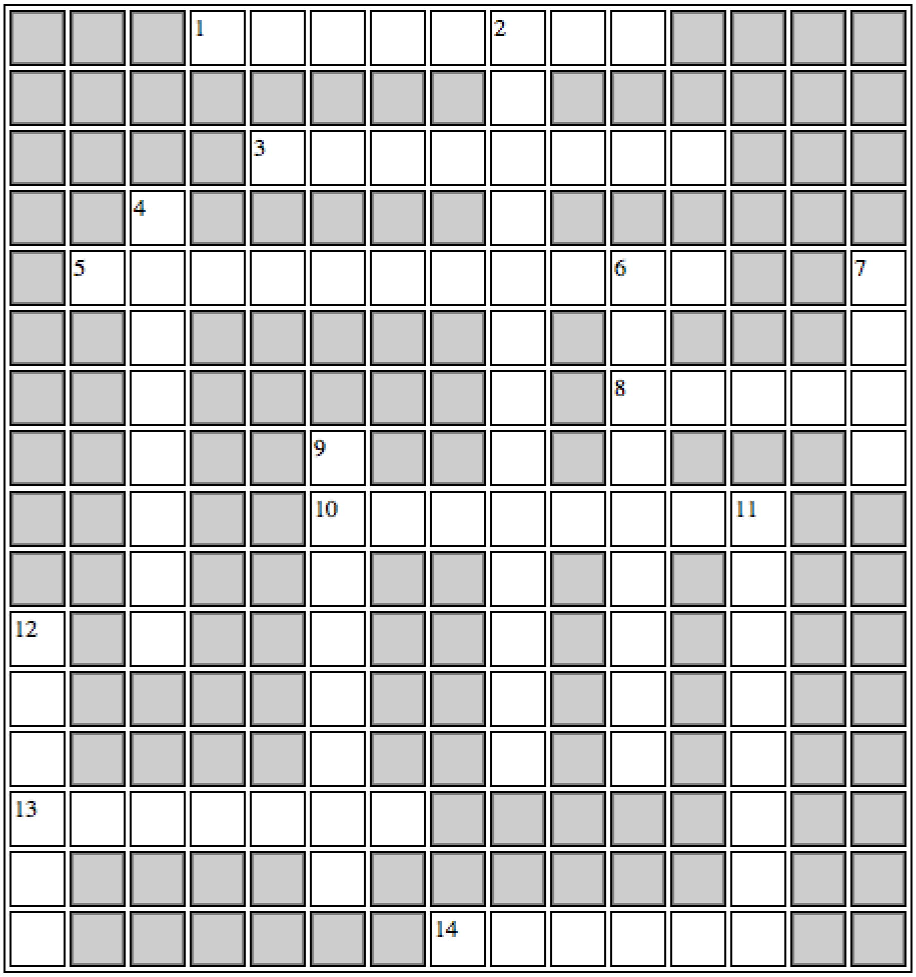
Decrypted by Letter to Number Cipher with Keyword Equal:
JVUK QUWVJ JCSY C GVURY

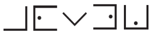
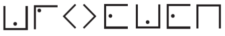
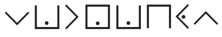
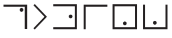
Decrypted by Atbash Cipher:
QEFP JFDEQ QXHB X TEFIB

Decrypted by Caeser Cipher with a Shift of 3:
This might take a while

8. Complete the crossword using the given ciphers. For the pigpen ciphers, use the key below.





	Across			**Down**	
1	NFOGRKOV	Atbash	2	GRIRCCVCFXIRD	Caesar (9)
3	HFYGIZXG	Atbash	4	ZFTWHMCA	Mixed (lumberjack, g)
5	MOLYXYFIFQV	Caesar (3)	6	GIZKVALRW	Atbash
8		Pigpen	7	NERN	Caesar (13)
10		Pigpen	9		Pigpen
13	JWQOKZJ	Mixed (Brazil, o)	11	HEMTUCRY	Mixed (campground, g)
14		Pigpen	12	HJFZIV	Atbash

			1 M	U	L	T	I	2 P	L	E				
								A						
				3 S	U	B	T	R	A	C	T			
		4 F						A						
	5 P	R	O	B	A	B	I	L	I	6 T	Y			7 A
		A						L		R				R
		C						E		8 A	N	G	L	E
		T			9 G			L		P				A
		I			10 E	X	P	O	N	E	N	11 T		
		O			O			G		Z		R		
12 S		N			M			R		O		I		
Q					E			A		I		A		
U					T			M		D		N		
13 A	L	G	E	B	R	A						G		
R					Y							L		
E							14 V	O	L	U	M	E		