



University of Waterloo  
Faculty of Mathematics



Centre for Education in  
Mathematics and Computing

## Grade 7/8 Math Circles

Fall 2012

### *Cryptography*

#### What is cryptography and how does it work?

Cryptography is the practice and study of hiding information. Using a key to encrypt the message, also known as plaintext, the sender gives the receiver the encrypted message, also known as ciphertext. Then, the receiver can use the key to unscramble, or decrypt the ciphertext back to plaintext to read the message.

There are multiple ways of encrypting and decrypting a message. One of the most well known and simplest methods is called Caesar Cipher.

**Caesar Cipher** is the method of encrypting where you: shift the alphabet a given number of places.

**Example 1** If you shift the alphabet 5 places, F becomes A, G becomes B, and so on.

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

**Exercise 1** Decrypt the following message using the Caesar cipher by shifting the alphabet 13 places.

Jr jvyy jva!

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

Plaintext: We will win!

**Exercise 2** Try encrypting the following message by shifting the alphabet 4 places.

Math Circles

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

Ciphertext: Iwpd Yenyhao!

**Keyword Cipher** is where we use another word to encrypt or decrypt a message. We will pick a **keyword** that does not contain any repeating letters (or remove the repeating letters of the word) and a **keyletter**. Starting under the keyletter, write each of the letters into the boxes. Next, fill in the remaining boxes with the letters (in alphabetical order) that were **NOT** in your keyword. Then, encrypt or decrypt using the table.

**Example 2** Using the keyword “campground” and the keyletter “g”, fill in the following table.

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

**Exercise 3** Pick your own keyword (remember to remove repeating letters) and keyletter, then encrypt the following message: I love mangos!

Keyword:

Keyletter:

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

Ciphertext: \_\_\_\_\_ !

**Exercise 4** Using the keyword “lumberjack” and the keyletter “g”, decrypt the following message.

Huy ucrmxxtqg tfy wcjmal!

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

Plaintext: [The holidays are coming!](#)

**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.

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

**Exercise 5** Decrypt the following message using the letter to number cipher.

04 15 14 ' 20      05 01 20      20 15 15      13 21 03 08      03 01 14 04 25!

Plaintext: Don't eat too much candy!

**Exercise 6** Encrypt the following message.

Call me maybe!

Ciphertext: 03 01 12 12    13 05    13 01 25 02 05!

**Word Shift Cipher** is a slightly more complex way to encrypt or decrypt a message. To encrypt, to 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 numerical 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 3** Complete the rest of the encrypted message by continuing to loop the key word “me” through the message and adding the numerical values.

**Encryption:**

T	20
O	15
D	04
A	01
Y	25

M	13
E	05
M	13
E	05
M	13

⇒

$20 + 13 = 33 \rightarrow (33 - 26 = 07)$	G
$15 + 5 = 20$	T
$04 + 13 = 17$	Q
$01 + 05 = 06$	F
$25 + 13 = 38 \rightarrow (38 - 26 = 12)$	L

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

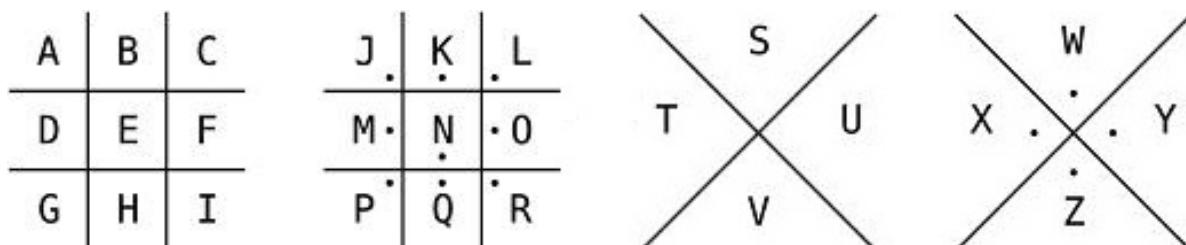
### Decryption:

G	07	M	13		$07 - 13 = -06 \rightarrow (-06 + 26 = 20)$	T
T	20	E	05		$20 - 05 = 10$	O
Q	17	M	13		$17 - 13 = 04$	D
F	06	E	05		$06 - 05 = 01$	A
L	12	M	13		$12 - 13 = -01 \rightarrow (-01 + 26 = 25)$	Y

**Exercise 7** 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					


**Pigpen Cipher** is yet another way that we can encrypt and decrypt a message. With Pigpen cipher, we assign all of the letters to a position in the following grid, so that each of the letters have a symbolic representation based on its location.



**Example 8** Decrypt the following messages using the Pigpen Key above.

בְּרַאשׁוֹת

Plaintext: trapezoid

# תְּמִימָנָה וְעַמְמָדָה

Plaintext: knowledge is power

## Problem Set

1. What do you call a sleeping bull? F GETTIWDJZ  
**(Keyword Cipher, Keyword: “sleep”, Keyletter: “s”)**
  2. When is a door not a door? DOLU PA’Z HQHY!  
**(Caesar Cipher, Key: 19)**
  3. Crack the following **Caesar cipher** given that it’s a shift of 8.

ESLZWESLAUK AK LZW EMKAU GX JWSKGF.

4. What did zero say to eight? 14 09 03 05 02 05 12 20!  
**(Letter to Number Cipher)**
  5. What is a prehistoric monster called when it sleeps? Z CHMNRMNQD!  
**(Caesar Cipher, Key 1)**
  6. Crack the following **keyword** cipher using the keyword “epsilon” and the keyletter “k”

YY YG YB ILC AYWXG TL ILC TL YC : YY YC YB ILC CADU TL ILC BMJ YC.

Marcus Aurelius

7. What do you call a cat drinking lemonade? N DCFBFHDD!  
**(Keyword Cipher, Keyword: “ostrich”, Keyletter: “j”)**

8. What do you call a dead parrot? N QITLHIV  
**(Word Shift Cipher, Keyword: “math”)**

9. Crack the following **letter to number cipher**

20 15 02 05 15 18 14 15 20 20 15 02 05 , 20 08 01 20 09 19 20  
08 05 17 21 05 19 20 09 15 14 !

10. What do seconds, minutes and months have that hours, days and years do not have?

20 08 05 12 05 20 20 05 18 14

**(Letter to Number Cipher)**

11. How do you get kleenex to dance? KPO V GDOOGZ WJJBT DIOJ DO

**(Caesar Cipher, Key 5)**

12. Crack the following **keyword** cipher given the keyword “delta” and the keyletter “a”

LQYOSNCQDOFY GR BUM DMT RN GR KDSF

13. What do you call a cow with no legs? IMJQFZ XCCH

**(Keyword Cipher, Keyword: “Chicago”, Keyletter: “e”)**

14. What did the skeleton ask for when he went into the coffee shop?

O QID CT QCTTSS OBR O ACD

**(Caesar Cipher, Key: 12)**

15. Why did the chicken cross the road? QL ASQ QL QBS LQBSO PCIS

**(Keyword Cipher, Keyword: “fish”, Keyletter “c”)**

16. Crack the following **letter to number cipher** to see who said the following quote:

“If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.”

Who said it? (crack the code)

10 15 08 14 22 15 14 14 05 21 13 01 14 14

17. What do you get if you divide the circumference of a jack-o-lantern by its diameter?

VPAVFWT KW

**(Word Shift Cipher, Keyword: “fun”)**

18. What kind of number transforms? WXBQUCA XZQUM!

**(Caesar Cipher, Key: 18)**

19. What do you call a man who spent all summer at the beach? FQOMETF

**(Word Shift Cipher twice, keywords: “summer”, “sun”)**

20. What is the scariest side of a haunted house? YMJ NSXNIJ!  
**(Caesar Cipher, Key: 21)**
21. What do you call a crushed angle? I AMLBJVPTN  
**(Word Shift Cipher, Keyword: “hi”)**
22. The following message has been encrypted twice; once by a **Caesar Cipher** with a shift of 6, and again by a **keyword cipher** using the keyword “Omega” and keyletter “a”. Decrypt to find the original message:

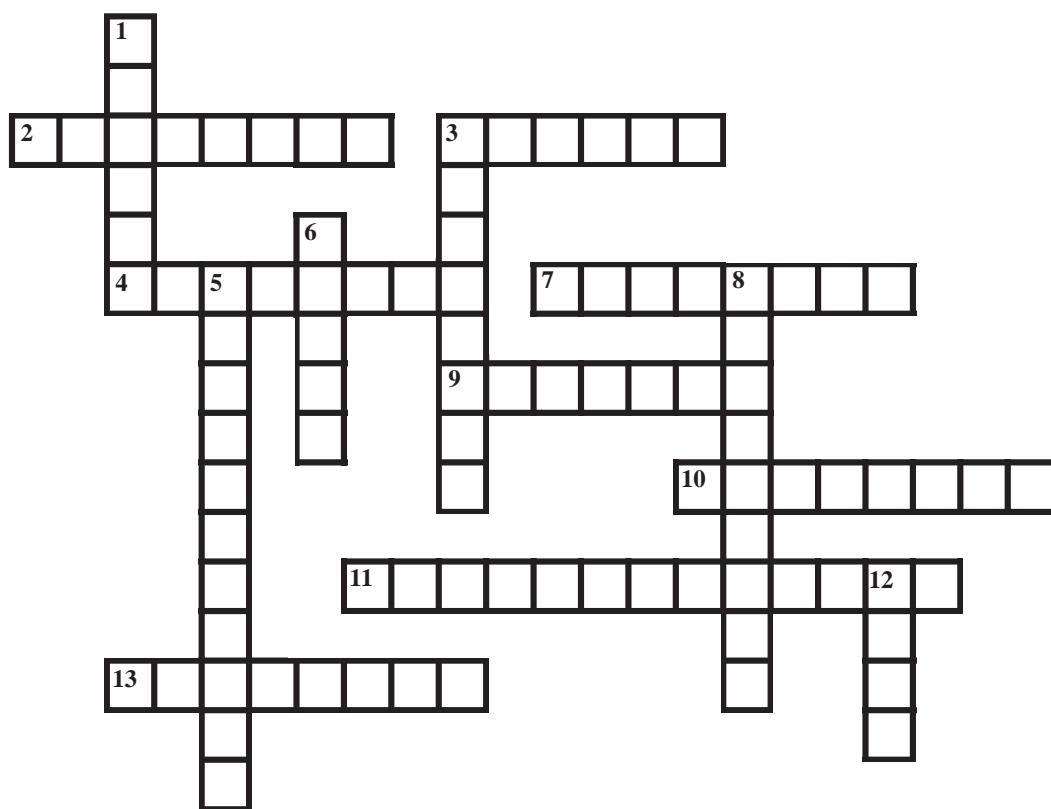
YDYJOS UDX HYJKEKLYDWY WFDINYJ UBB LMEDOK.

Benjamin Franklin

## Cryptic Crossword

Complete the crossword below using the given cipher. For the pigpen ciphers use the key below. Note: Word Shift and Keyword are different methods of encrypting and decrypting.

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



### Across

- 2. dlckzgcp
- 3. ㄱ>ㄱ ㄱ<ㄱ
- 4. hgfwswqc
- 7. ijzsrxrf
- 9. ㄴㅓㄴㅂㅂㄴ
- 10. jhrphwub
- 11. hignngxdwvech
- 13. nlcuhafy

### Down

- 1. otopej
  - 3. ㄱㄱㅂㅂK ㄱLㄱ
  - 5. jscuuucwecum
  - 6. ㄴㅓ ㄴㅓ ㄴㅓ
  - 8. fdmbqlaup
  - 12. fwjf
- Word shift key: “secure”  
Pigpen  
Word shift key: “tans”  
Pigpen  
Caesar key: 14  
Caesar key: 21