UNIVERSITY OF WATERLOO

Faculty of Mathematics
Waterloo, Ontario N2L 3G1

Centre for Education in
Mathematics and Computing

Grade 7/8 Math Circles

Winter 2015 - March 24/25

Cryptography

What is Cryptography?

Cryptography is the study of protecting, coding, storing and transmitting information and messages so that only those who are intended to may read it. In other words, it is the study of secret messages and codes.

Encryption is the conversion of messages to the secret code, called **ciphertext**. In order to read the information normally, one must **decrypt** the ciphertext, converting it back into **plaintext**.

Today, we will look at some different types of cryptography that are used.

Caesar Cipher

The first ciphertext that we will look at is **Caesar Cipher**. This ciphertext was used by Julius Caesar so that his messages could not be read by his enemies if intercepted.

The cipher is used by shifting the alphabet. We use a number which will be the amount we shift the alphabet to get the ciphertext. The following is an example of a shift of 5:

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

Notice how each letter in the ciphertext is moved over 5 letters from the plaintext.

So, the word "MATHEMATICS" in ciphertext would appear as "HVOCZHVODXN".

Decrypt the message "NUWJ HKRAO YDKYKHWPA" using Caesar Cipher with a shift of 4.

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

Encrypt the message "SACHIN PLAYS QUIDDITCH" using Caesar Cipher with a shift of 3.

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

Keyword Cipher

The **Keyword Cipher** is similar to the Caesar Cipher, but a bit more complex. Here is the process:

1. Pick a word with no repeating letters (if it does have repeating letters, ignore the repeated letters). This is your **keyword**.
2. Pick a key letter, which can be any letter of the alphabet.
3. Start at the key letter, and alphabetically replace each letter with each letter of the keyword.
4. Replace the rest of the alphabet with the letters not in the keyword.

For example, let's consider the keyword "ORANGE" and the key letter "P."
Then the shift is as follows:

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

The word "SCARLET" is now "NKIAWMG".
Decrypt the message "GOX JXQGOXB CF IXBL NCEW" with the keyword "DOCUMENTARY" and the key letter "G".

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

Encrypt the message "MATH CIRCLES" using the keyword "RUNNING" and the key letter "Z".

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

Letter to Number Cipher

The **Letter to Number Cipher** allows for each letter to be represented by a number. Typically, we use the following numbers to represent each letter:

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

So, the message "WHERE'S WALDO" would be written as "2308051805'19 2301120415".
It is important to assign a 2-digit number to each letter, so that we do not get confused.
We can also use a Caesar shift or a Keyword shift with a Letter to Number Cipher. First, assign the numbers, then shift the numbers.
For example, a Letter to Number Cipher with a Caesar Cipher shift of 6 would look like the following:

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

So the message "HAPPY BIRTHDAY" would be written as "0221101019 2203121402242119".
Decrypt the message "16011919 1305 200805 02011212" using the Letter to Number Cipher.

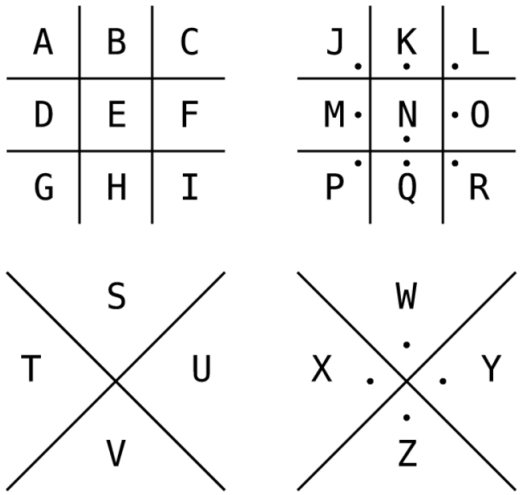
Encrypt the message "SHOOT THE PUCK" using the Letter to Number Cipher combined with a Keyword cipher, with keyword "TULIP" and key letter "W".

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

Pigpen Cipher

So far we have looked at ciphers that use direct substitution of letters for different letters or numbers. Now, we will take a look at the **Pigpen Cipher**, which replaces letters with symbols.

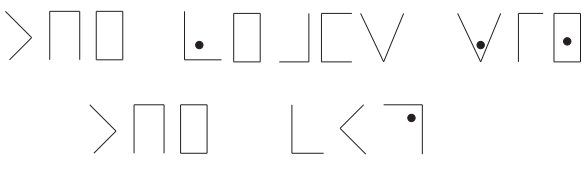
There are different symbols, grids and shapes that we can use when identifying letters within the Pigpen Cipher, but the most common is as follows:



We take the individual parts of these grids to form letters. For example, here is the code "MATH ROCKS":

Encrypt the message "CROSBY GETS THE GOAL"

Decrypt the following message:



Word Shift Cipher

The **Word Shift Cipher** is a more complex code, similar to the Letter to Number Cipher. We will again take the letter-number representation as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	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

Here is the process of the Word Shift Cipher:

1. Encrypt your message from the table above

2. Pick a keyword, and encrypt it from the table above. Repeat the word as much as needed to fill the length of the message

3. Add the numbers from the two encryptions. If this number is greater than 26, take the number and subtract 26 from it. The resulting message is your encrypted message.

To decrypt the message, subtract the repeating keyword from the ciphertext. If the number is negative, add 26.

For example, let's consider the message "GET THE COOKIES" with the keyword "SANTA".

GET THE COOKIES :	7	5	20	20	8	5	3	15	15	11	9	5	19
SANTA:	19	1	14	20	1	19	1	14	20	1	19	1	14
Encryption:	26	6	34	40	9	24	4	29	35	12	28	6	34
Simplified encryption:	26	6	8	14	9	24	4	3	9	12	2	6	8
Ciphertext:	Z	F	H	N	I	X	D	C	I	L	B	F	H

Encrypt the message "IS IT SUMMER YET" using the keyword "SUN".

Decrypt the message "V M S H M O T S H U Q S U K A" using the keyword "BEACH".

Modulus

When dividing two numbers, we are often left with a remainder. Rather than writing out a whole bunch of decimals, the **modulo operation** was created to show the remainder of one number with respect to another.

For example, we can say that $3 \equiv 23 \pmod 5$, which means that 23 has remainder of 3 when divided by 5. The sign $\equiv$ means that 3 (mod 5) and 23 are **congruent**.

Reduce the following in terms of modulo:

a) 18 (mod 4)

b) 25 (mod 3)

c) 42 (mod 6)

d) -75 (mod 7)

Ciphers and Modulus

We can use the modulo operation to make certain ciphers easier to find. Let's look at the Caesar Cipher again:

A different way to encrypt this message would be to convert every letter of the alphabet to a number, beginning with A = 0, B = 1,..., Z = 25. So we have:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then we have that the encrypted message is:

Encrypted = (Original letter + Shift) (mod 26)

So if we consider the example "ABRACADABRA" with a shift of 6, we do the following:

A = 00 : (0 + 6) (mod 26) = 6 (mod 26) = G

B = 01 : (1 + 6) (mod 26) = 7 (mod 26) = H

R = 17 : (17 + 6) (mod 26) = 23 (mod 26) = X

A = 00 : G

C = 02 : (2 + 6) (mod 26) = 8 (mod 26) = I

A = 00 : G

D = 03 : (3 + 6) (mod 26) = 9 (mod 26) = J

A = 00 : G

B = 01 : H

R = 17 : X

A = 00 : G

So we have “GHXGIGJGHXG”

To decrypt a message using modulus and the Caesar Cipher, we have:

Decrypted = (Original letter - Shift) (mod 26)

Decrypt the message “VSULQJ LV KHUH” using the Caesar Cipher, modulus, and a shift of 23.

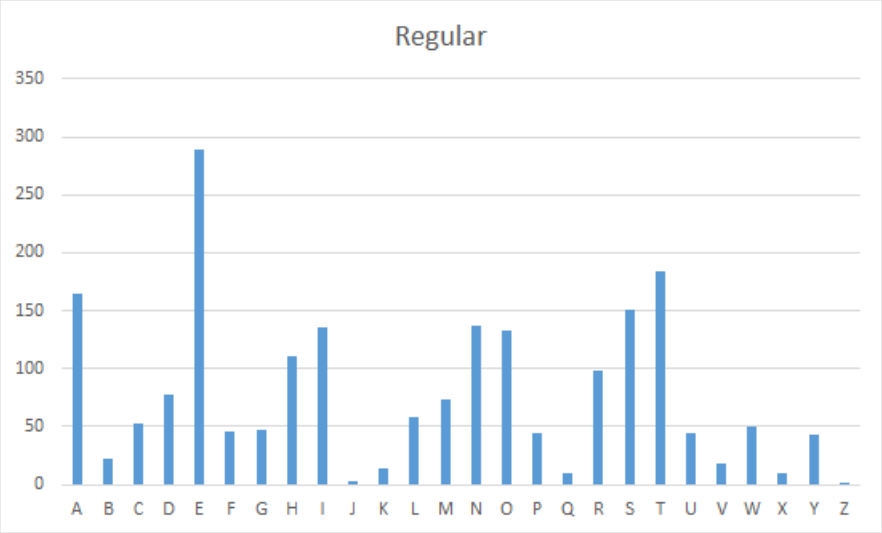
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

The Word Shift Cipher uses modulus without realizing it. When we find the remainder and subtract from 26, we are simply finding a number modulo 26.

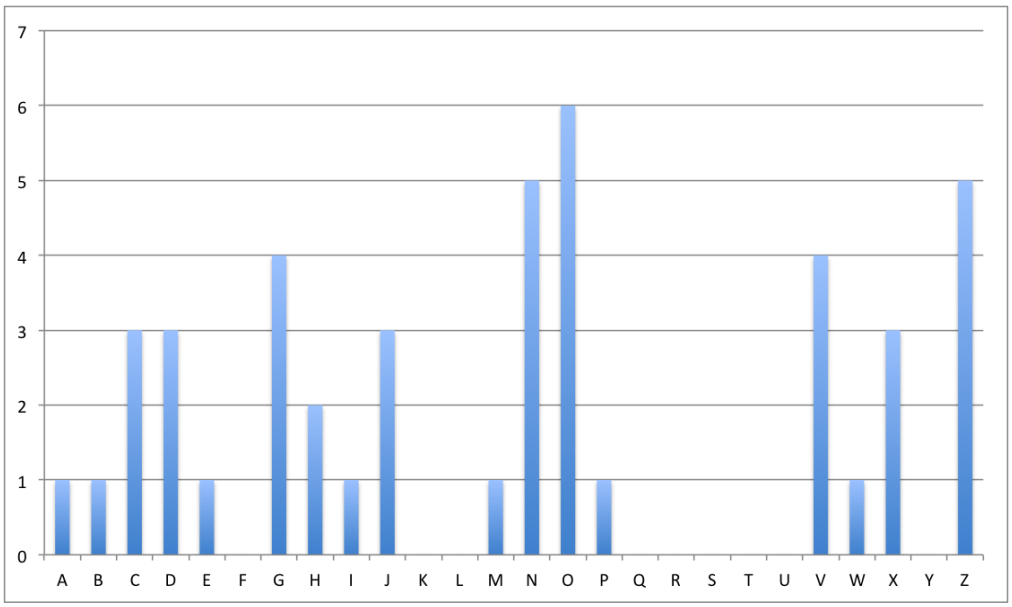
Frequency Analysis

In any phrase in the English language, certain letters are more frequent than others (E, A, S, T, O, for example). This will correspond to certain letters being more frequent in ciphertext as well.

Here is a **frequency analysis** of a regular English text. This shows the number of times each letter appears:



From the example "MATHEMATICS IS THE GREATEST SUBJECT IN ALL OF SCHOOL" with a Caesar Cipher and a shift of 5, we get the ciphertext: "HVOCZHVODXN DN OCZ BMZVOZNO NPWEZXO DI VGG JA NXCJJG", which gives the following frequency analysis:



Although not perfect (since our sample of letters is not large enough), can you figure out which ciphertext letters correspond to which English letters just by comparing the graphs?

Based on the regular frequency analysis and the ciphertext "PK XA KN JKP PK XA, PDWP EO PDA MQAOPEKJ", try to crack the code!

Problems

1. Carol and Nadine are passing notes in class using the Caesar Cipher. Carol is writing in ciphertext and Nadine is writing in plaintext. Decode their messages to find out what they are talking about.
Nadine: "My favourite number is 6, so use that shift in your cipher."
Carol: "IE, quhn ni ai ni nby guff uznyl mwbiif?"
Nadine: "Sure, I need to get some new boots."
Carol: "C domn xih'n quhn ni xi gs bigyqile!"

2. A soccer team is holding a team meeting, but they think that the opposition might be in the room beside theirs. To ensure that their strategy is kept secret, they are using the Keyword Cipher, with keyword "STRIKE" and key letter "D". The coach will write down the game plan in ciphertext, and the players will respond in plaintext. Try to decrypt the coach's messages, and encrypt the players' messages!
Coach: "Itn nkt yxcc qest xfs nktf zlgmm en ef."
Captain: "What about their star forward?"
Coach: "Ctxpt ked rgl gol strtfmt ng nxbt zxlt gr."
Defender: "And I'll let the forwards take care of the goals."

3. Aliens from the planet Rithmatik only know how to communicate using numbers in place of their letters. One day, the aliens decide to take over the Earth and have this message for you:
"2305 03151305 0914 1605010305. 2305 10211920 03011305 061518 200805 0301140425."

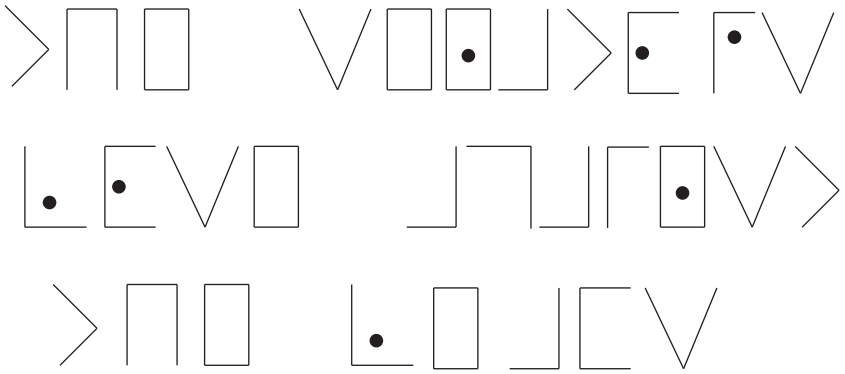
4. You want to reply to the aliens with the message "I DON'T HAVE ANY. PLEASE DON'T EAT ME." What will this message look like?

5. The aliens are getting angry, and when they get angry, they drift farther from English. This time, their message is a mix of the Caesar (shift 8) and Letter to Number Ciphers. The aliens do Letter to Number before Caesar. They say:
"24010623, 201312 1523 06232322 1207 2507 1126070808010625." Decrypt their message."

6. You want to impress the aliens and reply with a mix of Letter to Number and Keyword Ciphers. You want to say "The sugar is this way." How can you say this with a keyword of "apricot" and the key letter "F"?

7. Use the Pigpen Cipher to encrypt the message "The parade is on Tuesday."

8. Decrypt the following message:



9. Use the Word Shift Cipher to find out what the coldest city in Canada is, using the keyword "CANADA": "H V F F O B"

10. Use the Word Shift Cipher to encrypt the message "LET'S GO TO THE YUKON" with the keyword "NUNAVUT".

11. Reduce the following in terms of modulo:
a) 3 (mod 4)
b) 5 (mod 3)
c) 47 (mod 26)
d) -8 (mod 6)

12. Draw a frequency analysis graph for question 1. Are the results as expected?

13. Decrypt the following (Hint: It is a shift):
"Max vhew gxoxk uhmaxkxw fx tgrptr"