UNIVERSITY OF WATERLOO

Faculty of Mathematics
Waterloo, Ontario N2L 3G1

Centre for Education in
Mathematics and Computing

Grade 6 Math Circles

November 11/12, 2014

Cryptography

Quick Warm-up

Find the quotient and the remainder of the following:

1. $20 \div 4$
2. $33 \div 11$
3. $102 \div 25$
4. $3 \div 7$
5. $8 \div 8$
6. $17 \div 5$
7. $31 \div 7$
8. $99 \div 31$

Quick Into to Modulus

Above we see several examples where we are to find the quotient and remainder. Remember the quotient is the whole number part of the division and the remainder is what is left. So in $23 \div 4$ we have a quotient of 5 since 4 goes into 23 five times, and a remainder of 3 because $23 - (4 \times 5) = 3$.

Finding the **Modulo** of a number is just like finding the remainder.

$$23 \ (mod\ 4) \equiv 3$$

The $\equiv$ sign here means that 23 $(mod\ 4)$ and 3 are **congruent** to each other. In other words when divided by 4 in this case, 23 and 3 have the same remainder.

Reduce the following

1. 6 $(mod\ 4)$
2. 9 $(mod\ 11)$
3. 256 $(mod\ 5)$
4. 25 $(mod\ 5)$
5. 32 $(mod\ 1)$
6. 28 $(mod\ 3)$

7. $-2 \ (mod\ 6)$
8. $-14 \ (mod\ 3)$
9. $-10 \ (mod\ 5)$
10. $-100 \ (mod\ 8)$

Cryptography

Terminology:

Encrypt/encode Translate message from known language to a coded message

Decrypt/decode Translate message from coded to known language.

Cipher Tool used to encrypt/decrypt a message.

Caesar Cipher

The Caesar Cipher is an encryption method that was used many many years ago by Julius Caesar. The Cipher is simple. two people who want to send a message agree on a number, lets say 4, and shift every letter over by that many. Using a shift of 4 we would get the following:

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
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	D

Mathematically we can see this shift as modular arithmetics. If we assign every letter in the alphabet a number from 0-25, where A=0, B=2, ..., Z=25 we can then apply the shift:

$$coded = original + K \ (mod\ 26)$$

Looking at this we can see how we encrypted the message above. To decrypt the message we simply perform the opposite, that is shift every letter to the left instead of the right.

$$original = coded - K \ (mod\ 26)$$

Examples: Encode or decode the following using a the number in parenthesis as the shift number.

1. How are you today? (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

2. Wow, math is actually useful (2)

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

3. Qbun ncgy cm cn? (20)

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

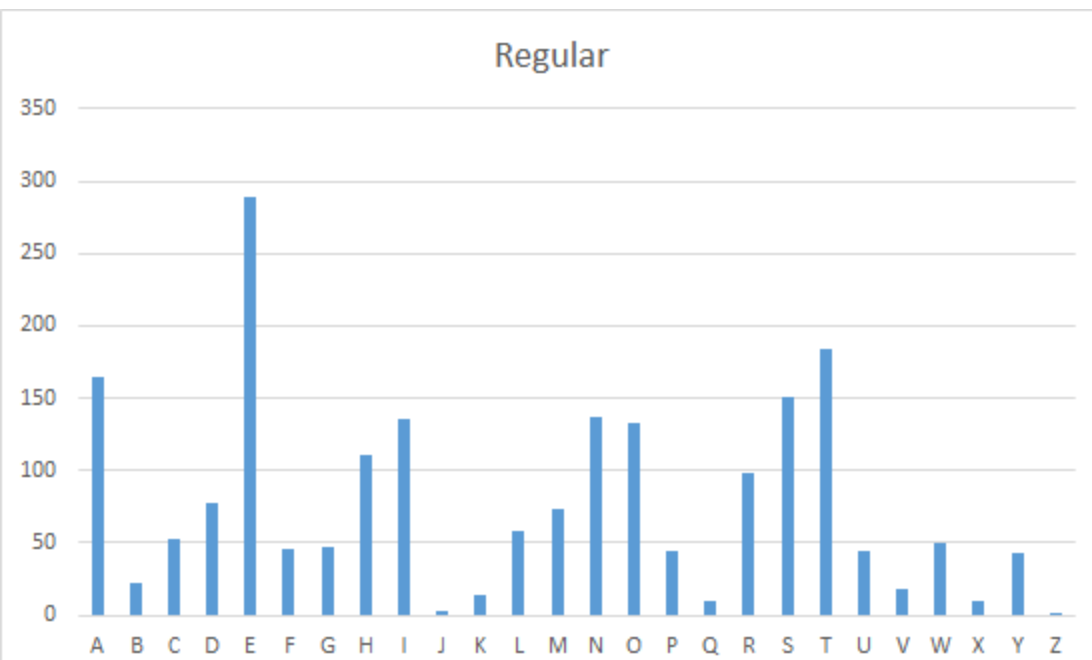
4. Y ted'j adem (16)

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

This cipher was used by military for hundreds of years after Caesars time to pass along strategic messages. However now it is seen as ineffective cipher and can be easily broken using frequency analysis.

Frequency Analysis (Quickly explained)

Up until this point of the document if we were to count up all the characters used and plot the number of times they appear we would get:



Do you notice any thing? If you were to take any document in English and do the same thing you would get a similar looking graph. This is because some letter in the English language are used more often the others. Notably R,S,T,L,N,E. This is how the Caesar Cipher was broken. You you take letters from a Caesar Cipher the most frequent letter is likely supposed to be the letter "E". From here the shift is likely the distance between E and the new most frequent letter.

More Ciphers

We will now look at more ciphers that are increasingly more difficult to break.

Atbash

An other simple cipher is the atbash cipher. The atbash cipher encodes the alphabet by inverting it giving A=Z B=Y,..., Z=A.

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
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

- To encode a message we replace letters from the first row with letters from the second.
- To decode a message we replace letters from the second row with letters from the first.

Examples

- **Encode** the following with the atbash cipher

  Encryption is fun.

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

- **Decode** the following using atbash cipher

  Dszg grnv rh rg?

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

<u>Further thinking:</u> What would a plot of the frequencies look like if the atbash cipher was used?

Keyword Cipher

The keyword cipher requires 2 pieces of information for the encryption and decryption. A keyword with no repeated letters (if there is a repeated letter just remove the second occurrence of it) and a starting letter known as the key letter. Once you have these two keys, you replace the key letter with the first letter of the keyword and the next letter with the second letter of the keyword, and so on. Then you replace the remaining letter alphabetically in the remaining spaces. For example:

Using the keyword **PARENTS** and the key letter **H**

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

Once we have our coded Alphabet encoding and decoding is the same as atbash:

- To encode a message we replace letters from the first row with letters from the second.
- To decode a message we replace letters from the second row with letters from the first.

This cipher is better but it still exhibits some of the letter frequency patterns as before.

Examples

- **Encode** the following using keyword spider and key letter f.

  This might take a while.

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

- **Decode** the following using keyword spider and key letter f.

  D vb v bvklzj xfyzj

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

<u>Further thinking:</u> What would a plot of the frequencies look like if the keyword cipher was used?

Word Shift

Remember, the problem with the ciphers so far was that they did not hide the frequencies of letters. This lead to code breakers being able to figure out the shift based on the new frequencies. So, if we can "hide" the frequencies such that they seem more uniform it will be harder to crack.

The word shift cipher does just this. This cipher requires a keyword for the example we will use the word "alien". The steps to the cipher are:

1. Convert the letters of you keyword into numbers. A=0, B=1,... , Z=25.
2. Write the letters/numbers of your keyword under the letters of the message you want to encode.
3. Convert each letter using the shift: $coded = original + k \ (mod\ 26)$

Example with keyword alien First we find the numbers associated with the word alien:

A	L	I	E	N
0	11	8	4	13

Next we want to encode the message "Aliens are coming":

A	l	i	e	n	s		a	r	e		c	o	m	i	n	g
0	11	8	4	13	0		11	8	4		13	0	11	8	4	13

A few shifts:

$A + 0 \ (mod\ 26) = 0 \ (mod\ 26) = 0$ -> A

$L + 11 \ (mod\ 26) = 22 \ (mod\ 26) = 22$ -> W

...

$n + 4 \ (mod\ 26) = 17 \ (mod\ 26) = 11$ -> R

$g + 13 \ (mod\ 26) = 19 \ (mod\ 26) = 19$ -> T

With this encoded alphabet, we could encrypt the message "Aliens are coming" as:

To decode a word shift we use the same steps, however the formula used is now $original = coded - k \ (mod\ 26)$

For example if we were to decode the message "Blbqnn zz Whppzqnn?" using keyword alien again, we would get:

B	l	b	q	n	n		z	z		W	h	p	p	z	q	n	n
0	11	8	4	13	0		11	8		4	13	0	11	8	4	13	0

$B - 0 \ (mod\ 26) = 1 \ (mod\ 26) = 1$ -> B

$L - 11 \ (mod\ 26) = 0 \ (mod\ 26) = 0$ -> a

...

$n - 13 \ (mod\ 26) = 0 \ (mod\ 26) = 0$ -> a

$n - 0 \ (mod\ 26) = 13 \ (mod\ 26) = 13$ -> n

After all the substitutions are made we get: _____

Frequencies using various keywords

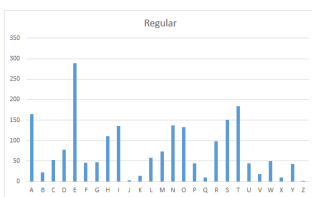


Figure 1: Regular Frequencies

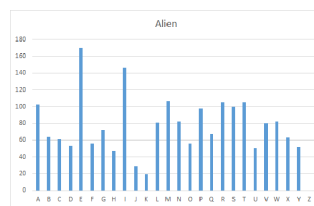


Figure 2: Alien

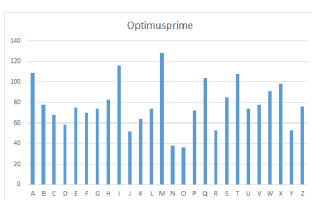


Figure 3: Optimus Prime

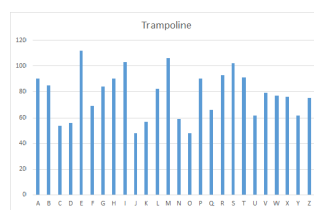


Figure 4: Trampoline

PROBLEMS

1. Reduce the following:

   (a) 4 (mod 4)

   (b) 7 (mod 2)

   (c) 124 (mod 5)

   (d) 37 (mod 10)

   (e) -5 (mod 7)

   (f) -12 (mod 8)

   (g) 0 (mod 6)

   (h) -20 (mod 26)

2. What happens when you encrypt a message using a Caesar cipher and a shift of 26?

3. Decode the following messages using a Caesar cipher, where the shift used the encode it is in parentheses.

   (a) Jshwduynts (5)

   (b) Upz Tupsz (1)

   (c) Jxqe fp qeb ybpq (23)

   (d) Y byau jkhjbui (16)

4. Decode the following messages that have been encoded with Atbash:

   (a) slow gsv kslmv

   (b) hold wldm

   (c) ivevihv

5. Using the keyword **TRAMPOLINE** and the key letter **A** decode: "Rtm anhipk"

6. * Using the keyword **CANADA** and the key letter **M** decode: "Fgenau oar tess"

7. What make a cipher bad? Are the Ciphers from question 5 and 6 bad?

8. Using the keyword **WATERLOO** and the key letter **F** decode: "Vzij kcemzhiejq"

9. Using the keyword **BATMAN** and the word shift cipher decrypt : "J lhhe cjzsm"

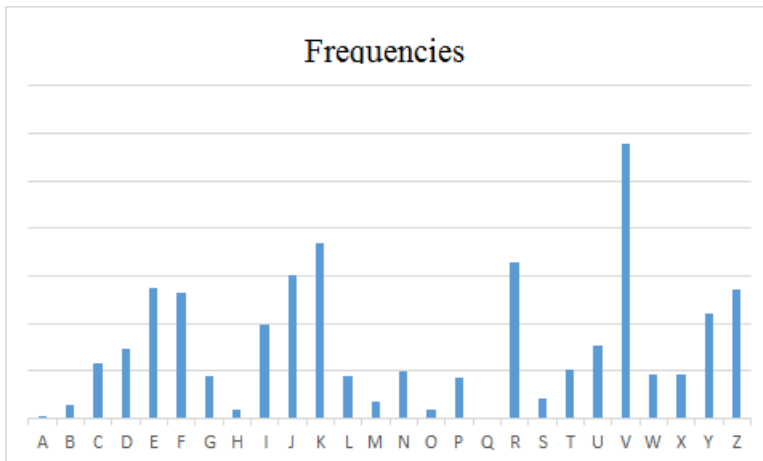
10. Using keyword **PIKACHU** and the word shift cipher decode: "Ewueovh"

11. You intercept a coded message and count the letter frequencies in the message and get:

A	B	C	D	E	F	G	H	J	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
38	12	6	13	1	6	1	38	5	9	18	52	7	9	23	32	0	2	15	10	35	31	6	0	23	29

You think it was encrypted using a Caesar cipher. What is the most likely shift used in the encryption? (explain why you think this is the most likely shift)

12. You think that a message has been encrypted using a Caesar cipher. You count the frequencies and plot them to get:



What is the most likely shift?

The next questions show that you can increase the strength of an encrypted message by combining multiple ciphers.

13. ** The following message was encrypted using Atbash, then a Caesar cipher of 3: "Kinyl kyalyj"

14. ** The following was encrypted using a word shift(keyword = dog), then Atbash. "Vhbd gcohgt"

15. *** The following was encrypted using a Caesar cipher with a shift of 5, then a Caesar cipher with a shift of 6, then a word shift(keyword = cat) then a keyword cipher with keyword **Trampoline** and key letter **D**: "Nwv bzo hjgbsdn chxd"