UNIVERSITY OF
WATERLOO
Faculty of Mathematics
Waterloo, Ontario N2L 3G1

Grade 6 Math Circles

November 19/20, 2013

History of Cryptography

Introduction

Cryptography (or cryptology) is the study of writing or reading secret messages or codes. The words comes from the Greek $\kappa\rho\upsilon\tau o\varsigma$ ("hidden, secret"), $\gamma\rho\alpha\phi\omega$ ("writing"), and $\lambda o\gamma\iota\alpha$ ("study of"). Before we begin, it's important to look at some terminology.

The original message or information a sender wishes to share with a specific person is called the *plaintext*. It is very easy to read and must be somehow hidden from enemies.

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

By encrypting plaintext (using methods like the ones covered in this lesson), you create *ciphertext*. Ciphertext looks like gibberish and is very hard to read. A *cipher* is a method of transforming a message to conceal its meaning.

Decryption is the opposite of encryption – it is the process of turning ciphertext back into the readable plaintext.

Substitution Cipher

The earliest 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.

Examples

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

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

Examples

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.

Examples

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
ciphertext	W	X	Y	Z	S	Q	U	A	R	E	B	C	D

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

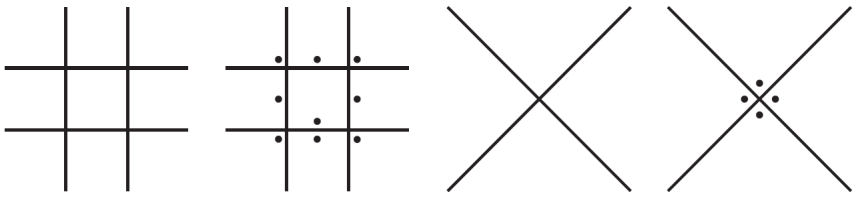
3. Decrypt "QRFZRFU FSDG" using the mixed alphabet cipher from part 1.

   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:

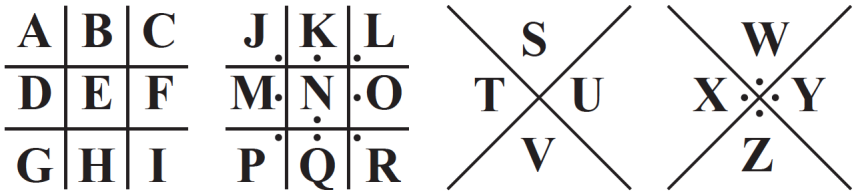
   FINDING NEMO

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.



Examples



1. 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:

2. Decrypt the following using the key above.

The first symbol, ⊓, represents the letter "H" in the first image of the key.
The second symbol, ⊏, represents the letter "O" in the second image of the key.
Continuing this, you will find that the plaintext is:

HOT CHOCOLATE PLEASE

Transposition Cipher

In transposition ciphers the order of the letters in the plaintext is changed according to a regular system or algorithm.

Route Cipher

Route ciphers are transposition ciphers that begin by first writing the plaintext on a grid. Then the letters are read off in a pattern given by a key.

Example

Encrypt "We are having a surprise party for Mom later" using a route cipher.

Begin by writing out the plaintext into a grid. In this case, I have written the message vertically, starting in the top left corner.

W	A	S	S	Y	M
E	V	U	E	F	L
A	I	R	P	O	A
R	N	P	A	R	T
E	G	R	R	M	E
H	A	I	T	O	R

The key would specify a direction that the route should follow when writing out the ciphertext. In this case, let's spiral inward, clockwise, starting from the bottom right.

The ciphertext would be:

ROTIAHERAEWASSYMLATEMRRGNIVUEFORAPRP

Columnar Transposition

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

Example

Encrypt "We are having a surprise party for Mom later" using a columnar transposition with the keyword CANDY.

Both the width of the rows and the order of the columns are defined by the keyword. For example, the word CANDY is 5 letters long (so every row will have 5 letters in it), and the order of the columns is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "2 1 4 3 5"

2	1	4	3	5
W	E	A	R	E
H	A	V	I	N
G	A	S	U	R
P	R	I	S	E
P	A	R	T	Y
F	O	R	M	O
M	L	A	T	E
R	Q	T	U	N

Note that I added 4 random letters (QTUN) at the end of the message in order to have a perfect rectangle with no empty spaces. These extra letters are called "nulls" and the receiver of the message should know that they have no meaning.

To produce the ciphertext just read off the columns in numerical order.

The ciphertext would be:

EAARAOLQ WHGPPFMR RIUSTMTU AVSIRRAT ENREYOEN

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.

Examples

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 "W".
   The ciphertext number 33 corresponds to the plaintext letter "N".
   Continuing this, you will find that the plaintext is:

   UNIVERSITY OF WATERLOO

The area of cryptography made little progress after the development of these transposition ciphers. Because of this, we are jumping forward in time, to the First World War.

ADFGX

The ADFGX cipher was used during the German Army during the First World War. It is a *product cipher*, as it combines more than one encryption technique (a Polybius Square and a columnar transposition), making it more secure. As a matter of fact, the Germans believed it was unbreakable.

The ADFGX cipher begins with a modified Polybius Square:

	A	**D**	**F**	**G**	**X**
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	j	c	u	x
X	m	r	e	w	y

A columnar transposition is then applied after the plaintext is represented by the coordinates of the ADFGX grid.

Example

Encrypt the message "Attack at sunset" using the ADFGX cipher.

Each letter in the message must be converted to the coordinates in the ADFGX square above that it is associated with. Read the coordinate along the left side and then along the top.

a	t	t	a	c	k	a	t	s	u	n	s	e	t
⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
AF	AD	AD	AF	GF	DX	AF	AD	FG	GG	FX	FG	XF	AD

Next, these coordinates are subject to a columnar transposition. Write the coordinates in rows under a transposition key (in this case, "TRUCK"):

T	R	U	C	K
A	F	A	D	A
D	A	F	G	F
D	X	A	F	A
D	F	G	G	G
F	X	F	G	X
F	A	D		

Next, sort the letters alphabetically in the transposition key (changing TRUCK to CKRTU) and then rearrange the columns beneath the letters along with the letters themselves:

C	K	R	T	U
D	A	F	A	A
G	F	A	D	F
F	A	X	D	A
G	G	F	D	G
G	X	X	F	F
		A	F	D

Finally, the ciphertext is read off in columns:

DGFGG AFAGX FAXFXA ADDDFF AFAGFD

Near the end of World War I, the Germans modified the ADFGX cipher into the ADFGVX cipher. By increasing the 5×5 Polybius Square into a 6×6 grid they could finally include all 26 letters in the alphabet and the digits 0 through 9.

World War 1 was a major turning point in the use in cryptography; it marked the last major conflict in which a country failed to encrypt any communication with troops and allies. Russia send unencrypted messages that were very easily translated by Russian-speaking intelligence officers on the German side!

Modern Cryptography

Advancements in technology have made all previous cryptography methods obsolete. Gone are the days of encrypting information with only a pencil a piece of paper – the encryption standards of today are so high that even most supercomputers can't crack the ciphers.

Enigma

The shift to using mechanical cipher machines for encryption happened at the end of the First World War. A German engineer invented Enigma, an incredibly complex "electro-mechanical rotor cipher machine" that went on to be used by the German Army during the Second World War.

Enigma was first "broken" by the Polish Cipher Bureau in 1932 by three very talented mathematicians who worked from information supplied by French military intelligence. In retaliation, the German Army just added more rotors and plugs to Enigma, making it exponentially harder to crack the code again.

The British government created a task force of some of the brightest minds in the United Kingdom to break Enigma and other German cipher machines during World War II. This group of cryptologists (codename: "Ultra") was based at Bletchley Park in England.

It was at Bletchley Park that Alan Turing, the "Father of Computer Science", and a team of cryptographers eventually did break Enigma.

Also at Bletchley Park was a man named Bill Tutte. Tutte did not work on Enigma. Instead, he spent his time cracking the Lorenz cipher on a machine called "FISH". Tutte's deciphering of FISH is considered one of the greatest intellectual feats of World War II.

Bletchley Park kept their triumphs secret so that they could continue to intercept German messages. It is said that WWII ended two years sooner because of Ultra.

After the war, Bill Tutte moved to Canada, where he went on to become a professor of Mathematics at the University of Toronto in 1948. In 1962, Tutte accepted a position here at the University of Waterloo, where he would spend the rest of his career.

Computers & Electronics

The development of computers after the Second World War has made vastly more complex ciphers possible.

Modern encryption uses algorithms with keys to encrypt and decrypt information. The public key system, for example, uses two keys. The first, the private key, is two very large prime numbers. The second, the public key, is the product of these two prime numbers. The public key is readily available to anyone, but only the sender and receiver possess the private key, thus keeping their communications secret.

Public key encryption has daily uses, such as online shopping and sending emails.

Because prime factorization of such large numbers is impossible, the only way for someone to try to break the public key system is by brute force, where the attacker tries every possible key until they find the right numbers. This is nearly impossible for even the most powerful supercomputers. This is getting easier though, with advancements in *quantum computing*. Quantum computers are so fast that public key encryption will soon be rendered useless.

It will then be up to *you* to develop the next great encryption algorithm to be used in the future.

Problem Set

1. How do you get a kleenex to dance? KPO V GDOOGZ WJJBT DIOJ DO
   (Caesar Cipher; 5)

2. What kind of numbers transform? LKGRNFH KIRNV
   (Atbash)

3. What do you call a dead parrot? K BZWHQZY
   (Mixed Alphabet. Keyword: BIRD; Keyletter: "P")

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

5. The following ciphertext was encrypted using a Route cipher. I wrote the plaintext into a grid, vertically, with 6 columns and 4 rows, then I spiralled inward, counter-clockwise, starting from the lower left corner. What is the plaintext?

   MWOTRSELCHFEOONEEKAICMER

6. The following ciphertext was encrypted using a columnar transposition with the keyword FLAKE. What is the plaintext?

   NSNQL EOTIT WRMOC TCGUY IIIOK

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

   231125453311 321144114411

8. The following ciphertext was encrypted using the ADFGX cipher with the keyword EARTH. What is the plaintext?

GFFAGAD ADDFFDG AADGXGG XGAFAFA FGDGDAF

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

43422322312412 3145 532412252231442455254312

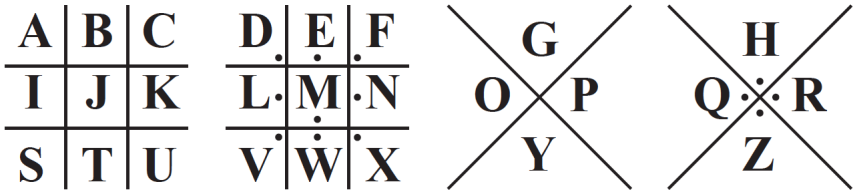
10. * The following ciphertext was first encrypted using a mixed alphabet cipher with a keyword PARTY and keyletter "B", then it was further encrypted with a Route cipher (I wrote vertically in a grid with 5 columns and 4 rows, then I spiralled inward, clockwise, starting from the upper left corner). What is the plaintext?

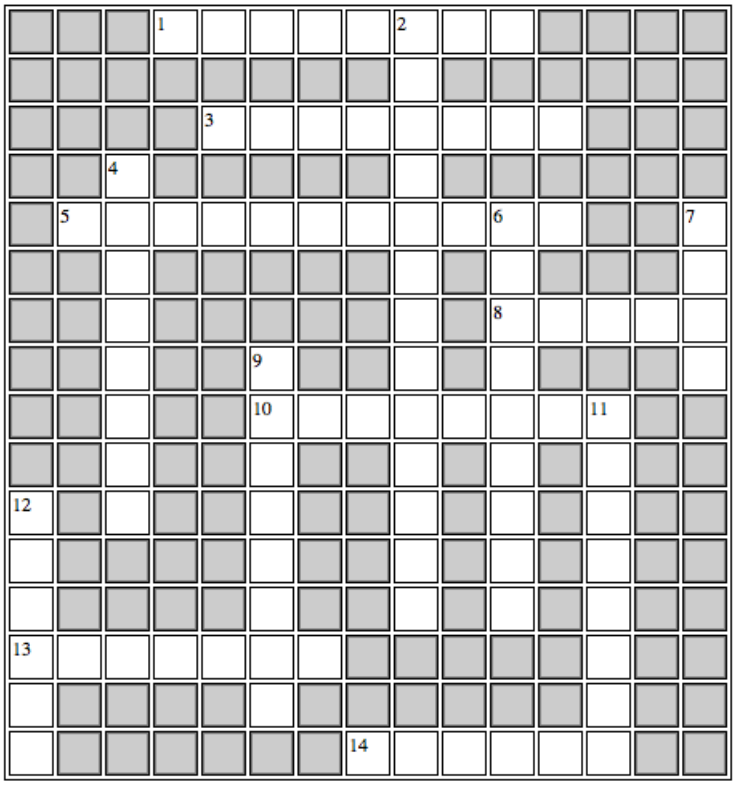
OJZMHDIBJZRCTCGWTAND

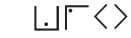
11. ** The following ciphertext was first encrypted using a Caesar cipher with a shift of 3, then it was further encrypted with Atbash, and finally encrypted again using the ADFGX cipher with the keyword WATER. What is the plaintext?

DDXGGGGGGX FGGADGXFDD GGDXDFGFXD FXXGGDXAXF
GGDFXFFFGX

12. 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