UNIVERSITY OF WATERLOO

Faculty of Mathematics

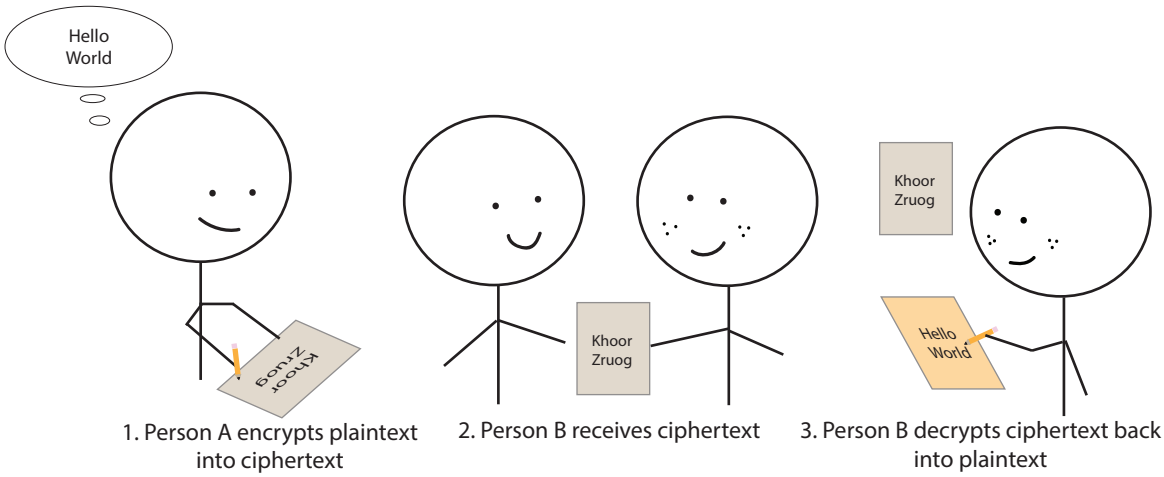
Waterloo, Ontario N2L 3G1

Centre for Education in Mathematics and Computing

Grade 6 Math Circles

November 5/6 2019

Cryptography Solutions



Atbash Cipher

Examples

1. Encrypt "Math Circles" using the Atbash cipher. Nzgs Xrixovh

2. Decrypt "ORLM PRMT" using the Atbash cipher. LION KING

Caesar Cipher

Examples: Encrypt or decrypt the following messages using the shift number given in parentheses:

a) Welcome to Math Circles! (5) Bjqhtrj yt Rfym Hnwhqjx!

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	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	E

b) Ljw hxd anjm cqrb? (9) Can you read this?

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

c) What if I did a Caesar Shift of 26 units on "*Welcome to Math Circles!*"? A Caesar shift of 26 would be shifting by the length of the alphabet. For example I would be shifting A 26 letters to the right. If I did this I would count across the whole alphabet and end up back at A. Thus a shift of 26 letters returns the same plaintext.

Frequency Analysis

What is the shift number of the cipher used? Shift number: 11

Why do you think that Caesar Cipher is considered not as secure as other Cryptography methods?

Frequency analysis can easily decyrpt a message encrypted with Caesar Cipher.

Vigenère Cipher

Example:

Encrypt the message "`ALGEBROS`" **Keyword:** `math`

MLZLNRHZ

keyword	M	A	T	H	M	A	T	H
shift number	12	0	19	7	12	0	19	7
plaintext	A	L	G	E	B	R	O	S
ciphertext	M	L	Z	L	N	R	H	Z

Example:

Decrypt the following message: Hjth xej o dtr ksbs. (`October`)

That was a bad joke.

keyword	O	C	T	O	B	E	R	O	C	T	O	B	E	R	O
shift number	14	2	19	14	1	4	17	14	2	19	14	1	4	17	14
plaintext	T	H	A	T	W	A	S	A	B	A	D	J	O	K	E
ciphertext	H	J	T	H	X	E	J	O	D	T	R	K	S	B	S

Pigpen Cipher

Exercises:

1. **Decrypt** the following messages using Pigpen Cipher:

   (a) 

   I AM RUNNING OUT OF IDEAS

   (b) 

   IT ALWAYS SEEMS IMPOSSIBLE UNTIL IT IS DONE

   (c) What is big, red and eats rocks? 

   BIG RED ROCK EATER

2. **Encrypt** the following messages using Pigpen Cipher:

   (a) We must hide this message!

   (b) Math is kinda cool eh?

Columnar Transposition

Examples Encrypt or decrypt the following messages given the keyword in parentheses:

a) encryption is fun (`friend`) psz rnz etf con yiz niu

F	R	I	E	N	D
E	N	C	R	Y	P
T	I	O	N	I	S
F	U	N	Z	Z	Z

First we fill out our chart. Fill in extra spaces with the letter Z.

D	E	F	I	N	R
P	R	E	C	Y	N
S	N	T	O	I	I
Z	Z	F	N	Z	U

Alphabetize the keyword and bring the columns along for the ride.

Read off the columns to get your encrypted message.

b) Why didn't the quarter roll down the hill with the nickel?

butmcs aidetx eshoex cearnx (`dime`) because it had more cents

D	E	I	M
B	A	E	C
U	I	S	E
T	D	H	A
M	E	O	R
C	T	E	N
S	Z	Z	Z

Alphabetical Order

D	I	M	E
B	E	C	A
U	S	E	I
T	H	A	D
M	O	R	E
C	E	N	T
S	Z	Z	Z

Spell out word

First we write our table with our keyword in numerical order and write out the ciphertext words down each column. Then we organize the table with our keyword spelled out at the top and bring each column along for the ride. Read out the rows to find the hidden message!

Problem Set:

1. What makes a Cipher good or bad?

   The quality of a cipher is determined by how easy it is to decode messages hidden by the cipher. A cipher that is easy to decode is called weak or bad while one that is hard to decode is considered strong or good.

2. Which is a stronger cipher between the Caesar Cipher and the Vigenère Cipher? Why? The Vigenère Cipher would be considered stronger than the Caesar Cipher. We saw how we could use frequency analysis to help find the shift number done by the Caesar Cipher. Also once the shift of one letter is discovered, the rest can easily be found as the whole message is shifted by the same amount. The Vigenère Cipher shifts every letter of the message by different amounts based on the keyword. This makes it much harder to decode the message.

3. Encrypt or decrypt the following messages using the Columnar Transposition cipher given the keyword in parentheses.

   a) windy day (kite)

      dy id wy na

   b) Always fresh, always Tim Hortons! (drink)

      ashyhn wrltrx ysamox aewitx lfasos

   c) asas ldnx panx ebax pnax (fruit)

      apples and bananas

   d) lce kos aox idi mnk (snack)

      milk and cookies

4. Encrypt or decrypt the following messages using a Caesar cipher given the shift number in parentheses.

   a) Hippopotamus (9)

      Qryyxyxcjvdb

b) I love math jokes! (14)

W zcjs aohv xcysg!

c) Axeeh Phkew (19)

Hello World

d) Zidbhv (21)

Enigma

5. Encrypt or decrypt the following messages using the Vigenère cipher given the keyword in parentheses.

a) Rainbow (colour)

Totbvfy

b) Math rocks! (school)

Ecav fzumz!

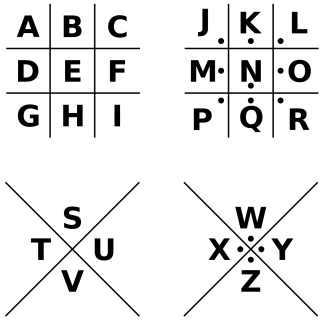
c) Nakfhn hs. Jnwedmrg (Martha)

Batman vs. Superman

d) Rcs yhh y xkwcfw wl ex! (toys)

You got a friend in me!

6. Encrypt or decrypt the following messages using the Pigpen Cipher and the same grid from earlier.

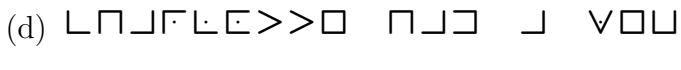


(a) HELLO WORLD!

(b) ISAAC NETWON

(c) 

TOMATOES AND LETTUCE

(d) 

CHARLOTTE HAD A WEB

7. Encrypt or decrypt the following messages using the Atbash Cipher.

   (a) Yellow blue red.

   Bvoold yofv ivw.

   (b) It is cold outside.

   Rg rh xlow lfghrwv.

   (c) Szkkb Yrigswzb!

   Happy Birthday!

   (d) Glilmgl Nzkov Ovzuh

   Toronto Maple Leafs

8. The University of Waterloo is under attack by geese! The leader of the geese rebels sends us an mysterious message and we believe it was encrypted with a Caesar cipher. You are given the frequencies of the letters below.

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
0	0	2	3	1	2	0	4	1	2	0	3	2	0	2	0	4	1	0	1	14	0	2	2	1	0

What is the shift number of the message? Based on the frequency analysis before we saw that E was the most common letter in the English alphabet by far. When looking at the frequencies of each letter in the table above we notice that U occurs by far the most in the encrypted message from the geese. From these two pieces of information we can make a logical assumption that E has been shifted to be U in the hidden message. Counting down the alphabet from E to U is 15. Thus we can say the Caesar cipher was done with a shift of 15.

9. * Police are attempting to identify the name of a doctor. They have found a document with what they believe to be the doctors name on it but it has been encrypted with a Caesar Shift. The encryption of the doctor's name looks as follows:

`NB. TYRX NYO`

Can you identify the name of the doctor?

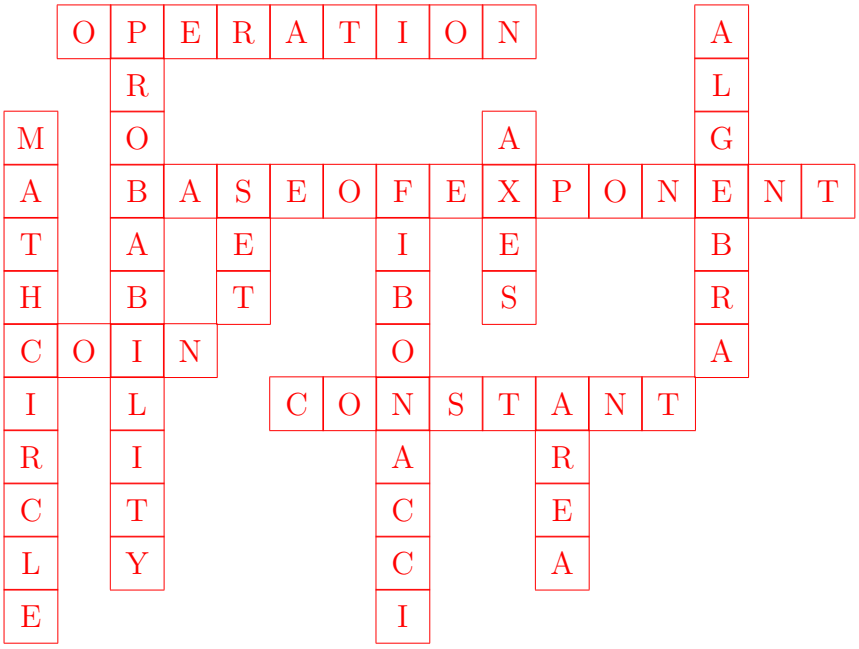
Dr. John Doe

Explanation: This is more of a trick question. The trick in this question is to realize that the two letters before the period in the doctor's name are "DR" as the title for a doctor. Using this information we know that "N" has been shifted to "D" and "B" has been shifted to "R". Counting between these letters we see that there has been a Caesar shift of 14 to decrypt the name of the doctor. Using a Caesar shift of 14 to decode the entire name we get Dr. John Doe.

Caesar Shift of 14:

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

10. Crossword Puzzle



11. The message `CDAEE IGFLZ STORZ AAHVI EOTSS` has been encrypted using a Columnar Transposition with the keyword `Match`. What is the message? `ACE IS A DOG THAT LOVES TREES`

12. Decode the message `Iwt fjxrz qgdlc udm yjbeh dktg iwt apon sdv.` That has been encoded with two Caesar shifts. The first shift is 5 and the second is 10. `The quick brown fox jumps over the lazy dog.` **This is the same as one Caesar shift of 15.**

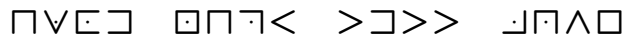
13. *The message `Adojzd tr c bnppkkl` has been encrypted twice. First with an Atbash cipher and then a Vigenère cipher with the keyword Deck. Find the original message.
    After decoding Vigenère cipher: `Xzmzwz rh z xlfmgib`
    Original message after decoding Atbash Cipher: `Canada is a country`

14. *The following ciphertext was encrypted first by a Columnar Transposition cipher (keyword `cloud`), then by the Vigenère cipher (keyword `float`). Decrypt the ciphertext.

    `xeok xxlb eflp qexk cgsn`

    After decrypting Vigenère cipher Cipher with keyword `float`: `stak esan emge ceef rssu`
    Original message after decrypting Columnar Transposition cipher: `Secret messages are fun`

15. ** The following ciphertext was encrypted first by a Columnar Transposition cipher (keyword `zone`) and then a Atbash cipher. A Caesar Cipher of shift of 8 is applied third. Finally a pigpen cipher is applied last with the same key as before.



After decrypting Pigpen Cipher: `HWOD NHPU TDTT JQVE`

After decrypting Caesar Cipher with shift of 8: `ZOGV FZHM LVLL BINW` After decrypting Atbash Cipher: `ALTE UASN OEOO YRMD` Original message after decrypting Columnar Transposition cipher with keyword `zone`: `YOU ARE ALMOST DONE`

16. *** One-Time Pad Encryption

    For this cipher, you need to translate letters into numbers and numbers into letters as we did in the Vigenère cipher.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

    Given a random key, to encrypt your plaintext you must do the following:

    1. Align your plaintext and key in a table such that each plaintext letter is paired up with key letter.
    2. Translate your plaintext and key into numbers.
    3. Add each pair of numbers together.
    4. If the sum is more than 25, subtract 25.
    5. Translate each number back into a letter. This is your ciphertext!

    a) Encrypt the following plaintext given the random key:

    `THIS IS A SECRET` (random key `LPFTSJZHFEIMA`)

    `DWNLABZZJGZQT`

    b) Challenge! Decrypt the following ciphertext given the random key:

    `ZPOHXIGTMJIZOKXF` (random key: `HLMQTPYBFFNVOZTC`)

    `SECRET IS REVEALED`