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

Introduction to Cryptography

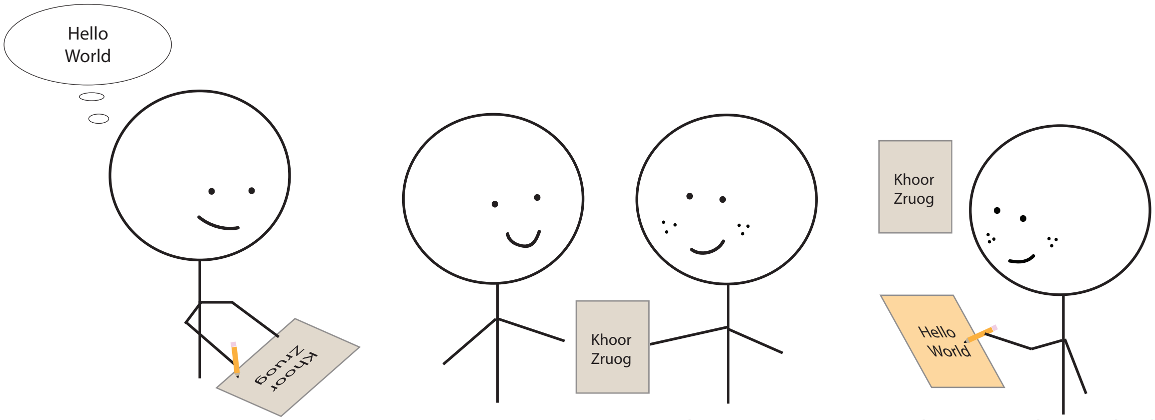
Cryptography is the study of hidden writing or reading and writing secret messages or codes. The word cryptography comes from the Greek word *kryptos* ($\kappa\rho\upsilon\tau\varsigma$) meaning hidden and *graphein* ($\gamma\rho\alpha\phi\omega$) meaning writing. Before we get any further, let's learn some terminology:

Plaintext: The original message or information the sender wants to encode or hide

Encryption: The process of encrypting plaintext such that only authorized parties, such as the sender and receiver, can read it

Ciphertext: The encrypted plaintext that was encrypted using a *cipher* (the method of performing encryption)

Decryption: The process of decoding ciphertext back into its original plaintext



1. Person A encrypts plaintext into ciphertext
2. Person B receives ciphertext
3. Person B decrypts ciphertext back into plaintext

Atbash Cipher

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.

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:

$$\begin{array}{ccccccccccccc} A & B & C & D & E & F & G & H & I & J & K & L & M \\ \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow \\ Z & Y & X & W & V & U & T & S & R & Q & P & O & N \end{array}$$

Examples

1. Encrypt “Math Circles” using the Atbash cipher.

2. Decrypt “ORLM PRMT” using the Atbash cipher.

Caesar Cipher

The most famous cipher is the **Caesar Cipher** and it is named after, as you may have guessed, Julius Caesar. What did he use this cipher for? To communicate with his army! It would not turn out so well if Caesar's enemies were able to intercept and read his messages. Caesar was able to encrypt his messages by shifting over every letter of the alphabet by 3 units. Using a shift of 3 letters, here is the cipher that Caesar used:

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	D	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

Now suppose Caesar wants to send the following message:

```
CAESAR SALAD IS NAMED AFTER ME AS WELL
```

Using the cipher shown earlier, Caesar's encrypted message is:

```
FDHVDU VDODG LV QDPH DIWHU PH DV ZHOO
```

To decrypt the encrypted message, we replace letters from the ciphertext row with letters from the plaintext row. We can also use the Caesar shift with **different shift numbers.**

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

a) Welcome to Math Circles! (5)

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																									

b) Ljw hxd anjm cqrb? (9)

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																									

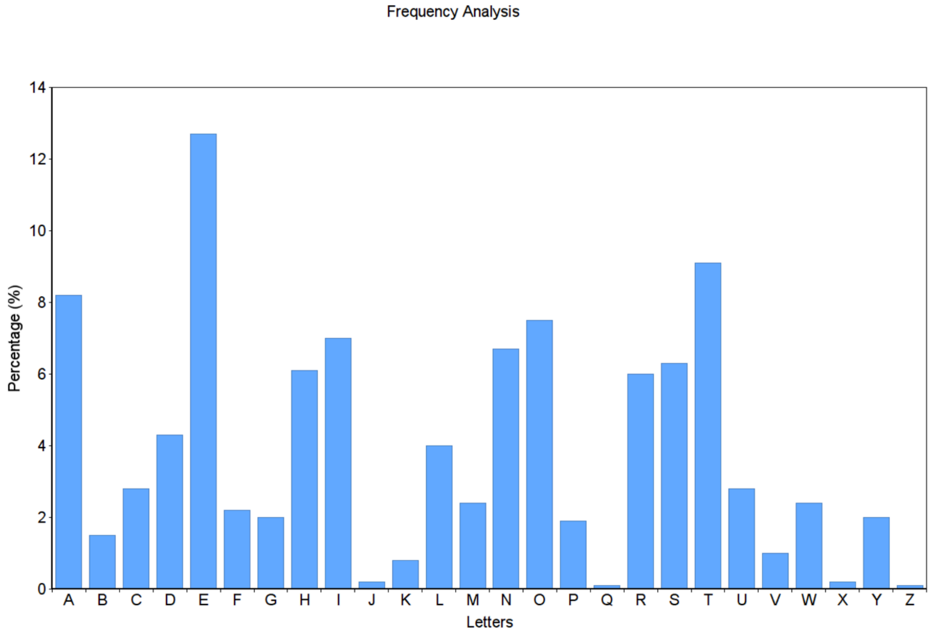
c) What if I did a Caesar Shift of 26 units on "*Welcome to Math Circles!*"?

Frequency Analysis

What happens if we do not know the shift number? The encryption needs to be broken but how can we do it? Is it even possible?

The answer is yes! To break the encryption, we can use something called **frequency analysis** (the study of the frequency of letters or groups of letters in a ciphertext). Since we are dealing with letters, **frequency** is the number of times a letter occurs. In the Caesar cipher, we can count the frequency of each letter and calculate it as a percentage.

Check it out! Below is a frequency graph that shows the average frequency of each letter in the English alphabet. What do you notice?

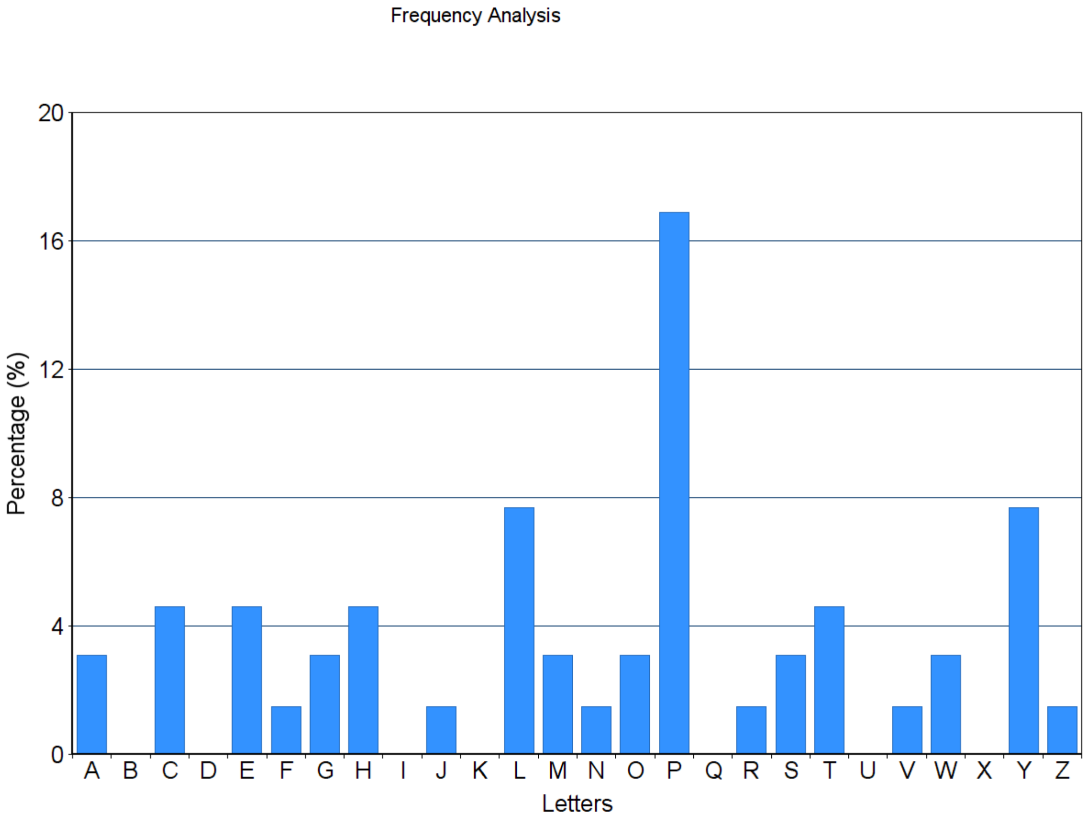


The most commonly used letter of the English alphabet is the letter E. Following the letter E, other commonly used letters include T, A, O, I, N and more!

Now, Caesar has encrypted his message using a different shift number:

```
Mp acpalcpo!  Hp htww leelnv ty esp pgpytyr.  Jzf slgp mppy hlcypo.
```

Below is a frequency graph of Caesar's ciphertext. What do you notice about this graph?



What is the shift number of the cipher used?

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

Vigenère Cipher

The Vigenère Cipher uses a keyword and multiple Caesar ciphers to encrypt a message. For this cipher, we will need to translate the alphabet into numbers:

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

Suppose we use the keyword `CODE` and we want to encrypt the following plaintext:

`RACECAR BACKWARDS IS RACECAR`

To begin, write out the plaintext and keyword on a table (and repeat the keyword until the end of the plaintext).

keyword	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C
shift number																									
plaintext	R	A	C	E	C	A	R	B	A	C	K	W	A	R	D	S	I	S	R	A	C	E	C	A	R
ciphertext																									

We then translate each letter in our keywords into numbers and write them underneath in the shift numbers row. These correspond to the shift numbers you will use to **apply a Caesar shift** to each plaintext letter.

keyword	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C
shift number	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2
plaintext	R	A	C	E	C	A	R	B	A	C	K	W	A	R	D	S	I	S	R	A	C	E	C	A	R
ciphertext																									

We then translate each letter in our letter of our keywords into numbers and write them underneath in the shift numbers row. These correspond to the shift numbers you will use to apply a Caesar shift to each plaintext letter.

For example, starting on the left column our plaintext letter is **R** and our shift number is 2 (from our keyword letter C). Thus to get our ciphertext we apply a Caesar shift of 2 on **R**.

Caesar Shift of 2:

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

We get **T** for our ciphertext letter as shown above. **Note we could also just count 2 letters to the right from R in the alphabet to find our ciphertext letter T.** Our original chart now looks like this:

keyword	**C**	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C
shift number	**2**	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2
plaintext	**R**	A	C	E	C	A	R	B	A	C	K	W	A	R	D	S	I	S	R	A	C	E	C	A	R
ciphertext	**T**																								

The next column of the chart we have the letter A and a shift number of 14. So we apply a Caesar shift of 14 to the letter A.

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

We get O for our ciphertext letter in this column after using a Caesar cipher with shift number 14.

keyword	**C**	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C
shift number	**2**	**14**	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2
plaintext	**R**	**A**	C	E	C	A	R	B	A	C	K	W	A	R	D	S	I	S	R	A	C	E	C	A	R
ciphertext	**T**	**O**																							

Each letter in the ciphertext is determined by the shift number and the plaintext letter. For each plaintext letter, we apply a Caesar cipher using the corresponding shift number.

keyword	**C**	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C
shift number	**2**	**14**	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2
plaintext	**R**	**A**	C	E	C	A	R	B	A	C	K	W	A	R	D	S	I	S	R	A	C	E	C	A	R
ciphertext	**T**	**O**	F	I	E	O	U	F	C	Q	N	A	C	F	G	W	K	G	U	E	E	S	F	E	T

Our encrypted message is then: `TOFIEOU FCQNACFGW KG UEESFET`

Example:

Encrypt the message “ALGEBROS” **Keyword:** math

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

Decryption

We can decrypt a Vigenère-encrypted ciphertext by using the keyword. Using the same keyword CODE, let’s decrypt the following message:

```
TOFIEOU MU O SENWQHTCPI
```

We can use a table again to find the plaintext. Again, we translate the keyword into numbers to give us the corresponding shift numbers. Then, using the shift number, we can find the cipher and use it to replace the ciphertext letter with plaintext letters.

Note: we are now **decoding** Caesar Shifts. We start with ciphertext and get plaintext.

keyword	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E
shift number	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4
plaintext																				
ciphertext	T	O	F	I	E	O	U	M	U	O	S	E	N	W	Q	H	T	C	P	I

Let’s start with the left column again. We have a ciphertext letter **T** and a shift number 2. We need to Caesar shift our ciphertext by 2 to get back to our plaintext.

Caesar Shift of 2:

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

After a Caesar shift of 2 our ciphertext letter **T** is changed to our plaintext letter **R**. **Note we could also just count 2 letters to the left from T in the alphabet to find our plaintext letter R.** Our original chart now looks like this:

keyword	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E
shift number	**2**	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4
plaintext	**R**																			
ciphertext	**T**	O	F	I	E	O	U	M	U	O	S	E	N	W	Q	H	T	C	P	I

We repeat this to get our whole message in ciphertext.

keyword	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E
shift number	**2**	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4
plaintext	**R**	A	C	E	C	A	R	I	S	A	P	A	L	I	N	D	R	O	M	E
ciphertext	**T**	O	F	I	E	O	U	M	U	O	S	E	N	W	Q	H	T	C	P	I

Racecar is a palindrome

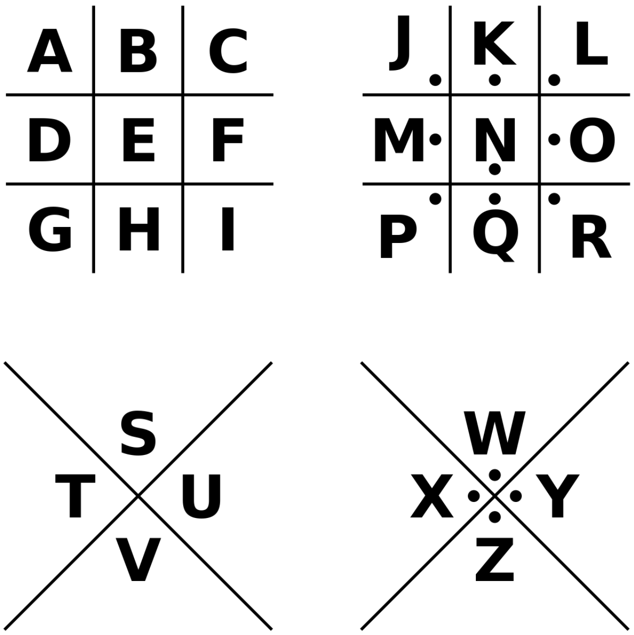
Example:

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

keyword	O	C	T	O	B	E	R	O	C	T	O	B	E	R	O
shift number	14														
plaintext	T														
ciphertext	H	J	T	H	X	E	J	O	D	T	R	K	S	B	S

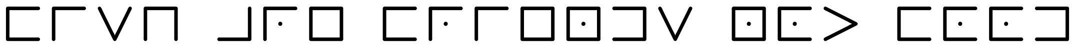
Pigpen Cipher

Up until now all of our ciphers have been done using the scrambling of letters. What about other methods? The pigpen cipher is a famous cipher which exchanges letters for symbols. The cipher can be arranged a variety of ways but usually looks as follows:



Each letter has a symbolic representation based on its location in the grid above. For example A is represented as ┘ and R would be represented as ┌·.

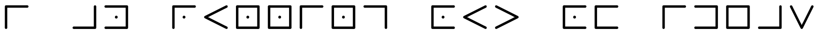
If we wanted to encrypt the message "*FISH ARE FRIENDS NOT FOOD*" it would look like:

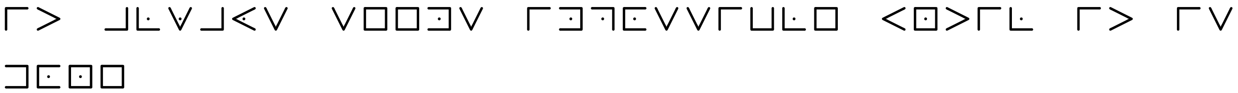


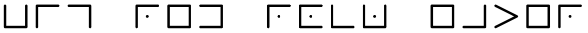
FISH ARE FRIENDS NOT FOOD

Exercises:

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

   (a) 

   (b) 

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

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

   (a) We must hide this message!

   (b) Math is kinda cool eh?

Columnar Transposition

The **columnar transposition** cipher changes the position of the letters in a message. For this cipher, we will need a keyword (preferably a word with no repeating letters). Let's do an example to see how the cipher works.

Suppose that our keyword is `PENCIL` and we want to encrypt the following message:

`MATH IS THE BEST SUBJECT`

The number of letters in our keyword becomes the number of columns we will make.

P	**E**	**N**	**C**	**I**	**L**
M	A	T	H	I	S
T	H	E	B	E	S
T	S	U	B	J	E
C	T	Z	Z	Z	Z

Write your message underneath the columns letter by letter as shown on the left. For extra spaces in the table, fill it with a random letter that is not in your message.

C	**E**	**I**	**L**	**N**	**P**
H	A	I	S	T	M
B	H	E	S	E	T
B	S	J	E	U	T
Z	T	Z	Z	Z	C

Next, to change it up, rearrange your columns by the alphabetical order of your keyword.

To read the resulting ciphertext, read off the columns from left to right. For this example, the resulting ciphertext is `HBBZ AHST IEJZ SSEZ TEUZ MTTC`.

How do we decrypt a columnar transposition cipher? Suppose the keyword is BLUE and we want to decrypt the following ciphertext: MIEH HVWE ASRE TEYR

B	E	L	U
M	H	A	T
I	V	S	E
E	W	R	Y
H	E	E	R

Start with a table and label each column with the letters of our keyword in alphabetical order. Write the first set of letters, MIEH, of the ciphertext under the leftmost column. Write the second set of letter, HVWE, in the next column and so on.

B	L	U	E
M	A	T	H
I	S	E	V
E	R	Y	W
H	E	R	E

Once the table is complete, rewrite the table with the columns labels spelling out the keyword as shown below: Finally, read the rows of the table to find the plaintext!

Plaintext: **MATH IS EVERYWHERE**

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

a) encryption is fun (friend)

b) Why didn't the quarter roll down the hill with the nickel?
butmcs aidetx eshoex cearnx (dime)

Problem Set:

1. What makes a Cipher good or bad?

2. Which is a stronger cipher between the Caesar Cipher and the Vigenère Cipher? Why?

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

   a) windy day (kite)

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

   c) asas ldnx panx ebax pnax (fruit)

   d) lce kos aox idi mnk (snack)

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

   a) Hippopotamus (9)

   b) I love math jokes! (14)

   c) Axeeh Phkew (19)

   d) Zidbhv (21)

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

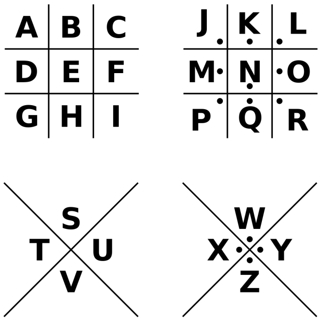
   a) Rainbow (colour)

   b) Math rocks! (school)

   c) Nakfhn hs. Jnwedmrg (Martha)

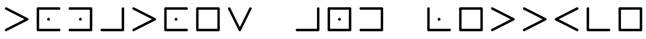
   d) Rcs yhh y xkwcfw wl ex! (toys)

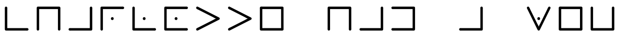
6. Encrypt or decrypt the following messages using the Pigpen Cipher and the same grid from earlier.



   (a) HELLO WORLD!

   (b) ISAAC NETWON

   (c) 

   (d) 

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

   (a) Yellow blue red.

   (b) It is cold outside.

   (c) Szkkb Yrigswzb!

   (d) Glilmgl Nzkov Ovzuh

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

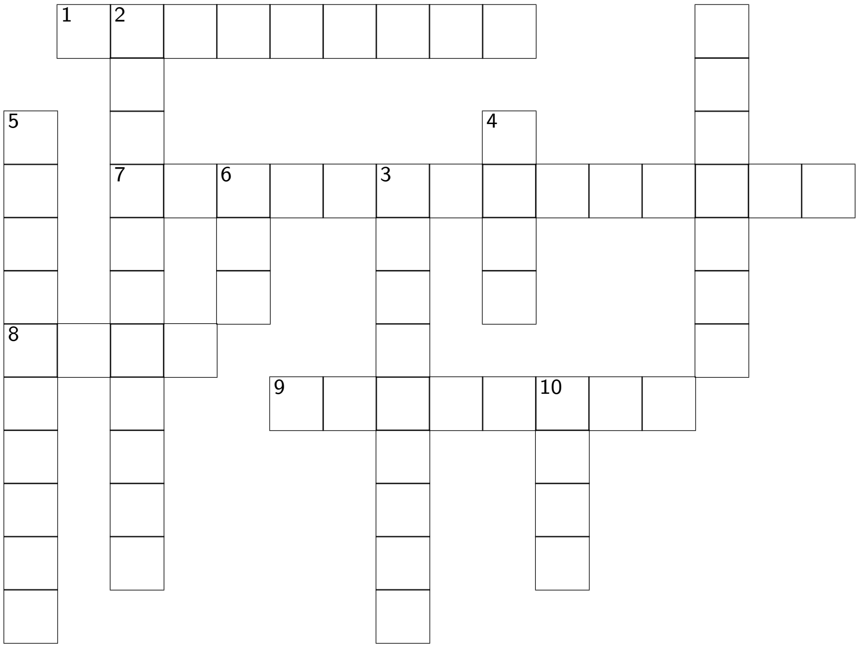
   What is the shift number of the message?

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?

10. Crossword Puzzle



Across

1 TACWLRNZL, Vigenère (fly)

7 YZHVLUVCKLMVMG, Atbash

8 BNHM, Caeser Shift (25)

9 FCTVHGQH, Vigenère (dog)

Down

2 KILYZYRORGB, Atbash

3 MPIVUUHJP, Caeser Shift (7)

4 ┘⋗□∨, Pigpen Cipher

5 ZNGU PVEPYRF, Caeser Shift (13)

6 ∨□>, Pigpen Cipher

10 ZIVZ, Atbash

11. The message `CDAEE IGFLZ STORZ AAHVI EOTSS` has been encrypted using a Columnar Transposition with the keyword `Match`. What is the message?

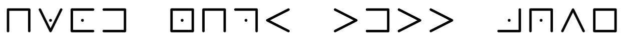
12. Decode the message `Iwt fjxrz qgdlc udm yjbeh dktg iwt apon sdv.` That has been encoded with two Caesar shifts. The first shift is 5 and the second is 10.

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.

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`

15. ** The following ciphertext was encrypted first by a Columnar Transposition cipher 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.



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`)

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

`ZPOHXIGTMJIZOKXF` (random key: `HLMQTPYBFFNVOZTC`)