UNIVERSITY OF WATERLOO

Faculty of Mathematics
Waterloo, Ontario N2L 3G1

Centre for Education in
Mathematics and Computing

Grade 6 Math Circles

October 4 & 5, 2016

Cryptography

Introduction to Cryptography

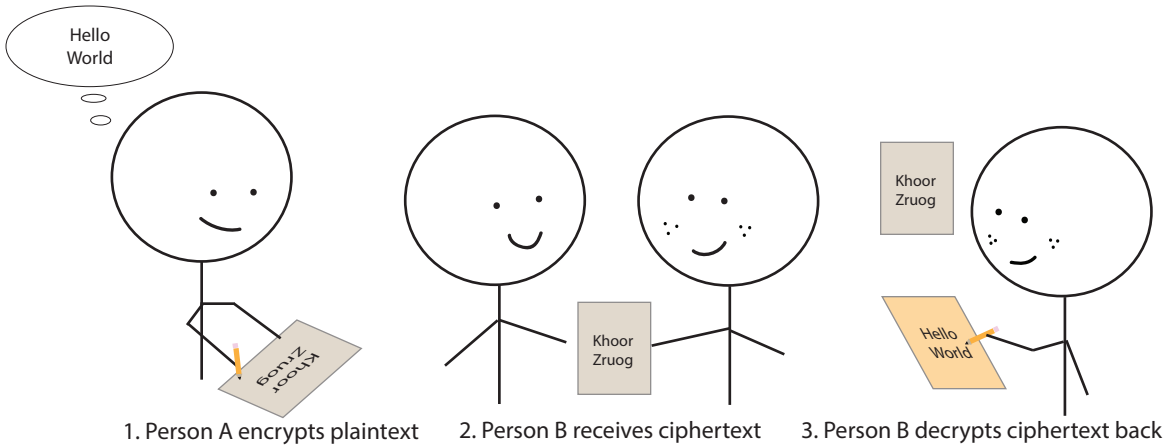
Cryptography is the study of hidden writing or reading and writing secret messages or codes. The word cryptography comes from the Greek word *kryptos* ($\kappa\rho\upsilon\tau\varsigma$) meaning hidden and *graphein* ($\gamma\rho\alpha\phi\omega$) meaning writing. Before we get any further, let's learn 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 message of the plaintext that was encrypted using a *cipher* (the method of performing encryption)

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

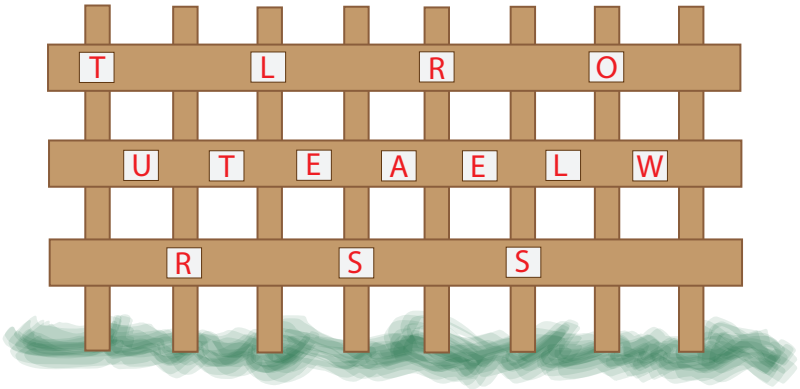


1. Person A encrypts plaintext into ciphertext
2. Person B receives ciphertext
3. Person B decrypts ciphertext back into plaintext

Rail Fence Cipher

Let's warm up with an easy cipher. With the **rail fence cipher**, we will be transposing, or changing the position of the letters in a message. To transpose a message, we need a key number and we will need to write each letter of the message up and down the rail fence. Here is an example of how the cipher works:

Suppose the message is `TURTLES ARE SLOW` and our key number is 3. Now imagine a rail fence with 3 rails.



By reading off the rows of the rail fence, the resulting ciphertext is `TLRO UTEAELW RSS`. We can also use a grid to help encrypt plaintext as shown below.

T				L				R				O	
	U		T		E		A		E		L		W
		R				S				S			

Let's decrypt the following message on the grid below with a key number of 4:

`HR AAET RSFS EA`

H						R					
	A				A		E				T
		R		S				F		S	
			E						A		

Hares are fast

Decrypt the rail fence cipher by starting with the first set of letters. Write the first letter H, then count 4 squares down the grid diagonally and 4 squares up the grid diagonally. Write the next letter R. Start again with the next set of letters. Write the first letter A, then count 3 squares down diagonally and 3 squares up diagonally. Write the next letter A. Repeat this

pattern for the rest of the ciphertext. Was it difficult to decrypt the rail fence cipher? No. But it is time consuming. The rail fence cipher by itself is not very strong.

Examples Encrypt or decrypt the following messages given a key number in parentheses:

a) the sky is blue (4) ti hyse ekbu sl

b) when pigs fly (6) wy hl ef ns pg

c) roae admxml nep (3) random example

d) can rrpu yghf poys ti (5) cryptography is fun

Columnar Transposition

Similar to the rail fence cipher, the **columnar transposition** cipher changes the position of the letters of 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 <u>not</u> 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`

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. Once the table is complete, rewrite the table with the columns labels spelling out the keyword as shown in the table on the right. Finally, read the rows of the table to find the plaintext!

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

Plaintext: `MATH IS EVERYWHERE`

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

a) encryption is fun (`friend`) psx rnx etf con yix niu

b) Why didn't the quarter roll down the hill with the nickel?
butmcs aidetx eshoex cearnx (`dime`) because it had more cents

Caesar Cipher

The simplest and most well known 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.

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

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

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
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?

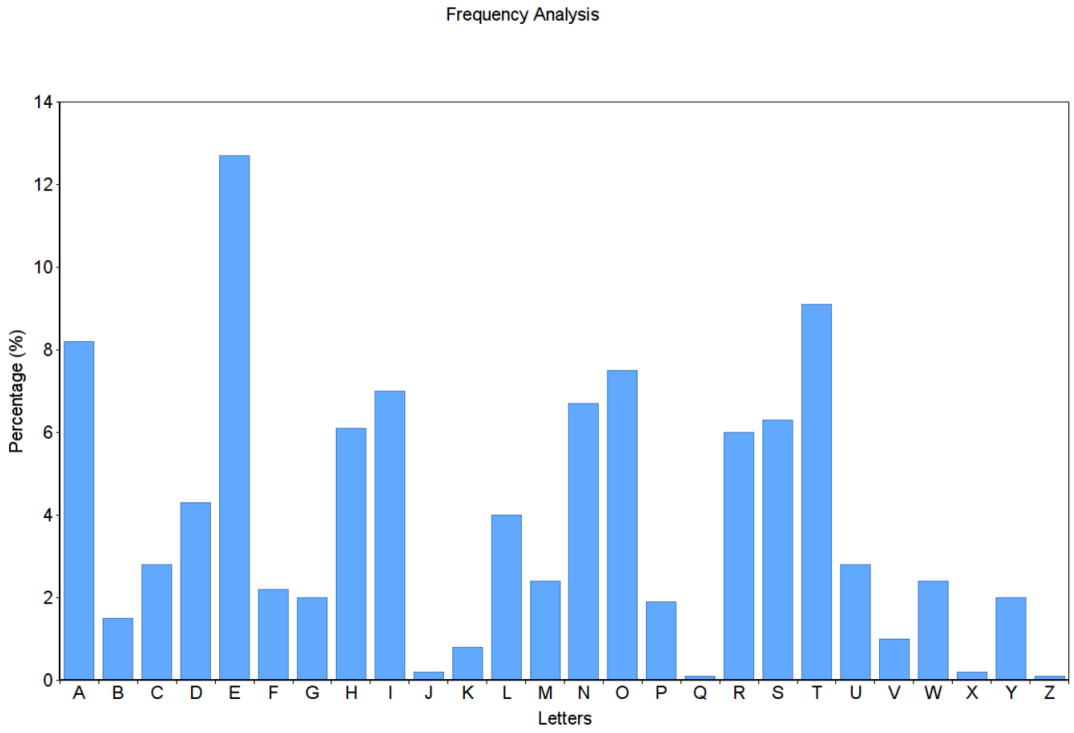
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

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?



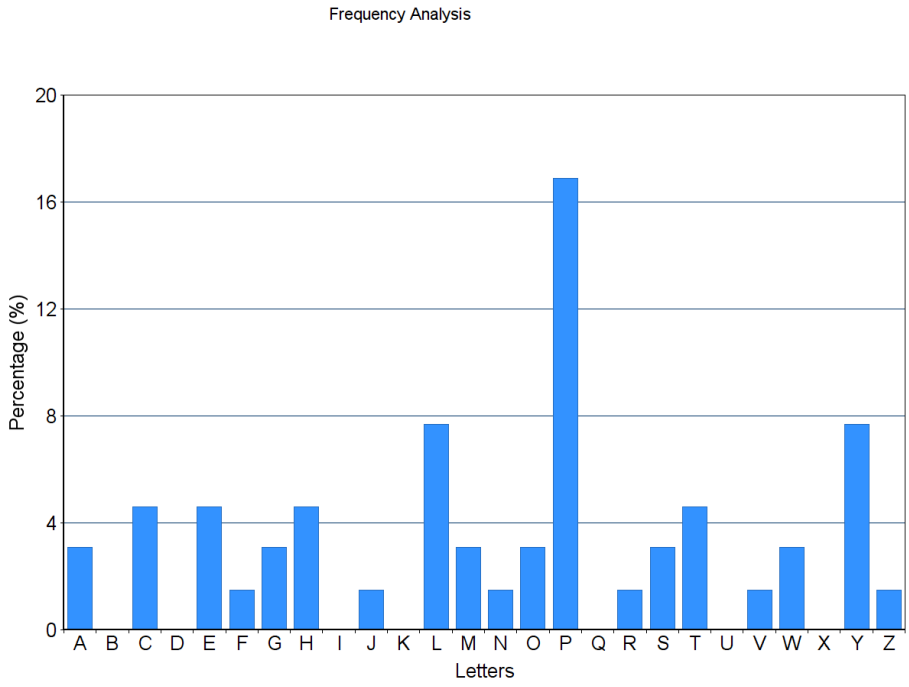
The most commonly used letter of the English alphabet is the letter E. Following the letter E, other commonly used letters include T, A, O, I, N and more!

Fun fact! Written in 1939, Ernest Vincent Wright's *Gadsby* is a 50 000 - word novel that never uses the letter E! (Except for in the prologue and in his name).

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? 11

Using frequency analysis, it is not very difficult to break the Caesar cipher and so it is not an effective cipher to use if you want to encrypt a secret message. The next cipher does use the Caesar Cipher but is more difficult to break.

Vigenère Cipher

Contrary to popular belief, the **Vigenère Cipher** was invented by Giovan Battista Bellaso in 1553. The cipher was misattributed to Blaise de Vigenère in the 16th century. How does it work? 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). Then translate each letter of the keyword into its corresponding number. Each corresponding number is the shift number we will use to encrypt 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	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

Tofieou fcqnacfgw kg ueesfet

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. For example, the keyword letter `C` corresponds to a shift number of 2. With a Caesar cipher of shift 2, the plaintext letter `R` is becomes `T`.

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 to replace the ciphertext letter with plaintext letters (similar to the Caesar cipher).

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
ciphertext	T	O	F	I	E	O	U	M	U	O	S	E	N	W	Q	H	T	C	P	I
plaintext	R	A	C	E	C	A	R	I	S	A	P	A	L	I	N	D	R	O	M	E

Racecar is a palindrome

Fun fact! Although the Vigenère cipher is not difficult to understand, it took roughly 300 years for the cipher to be decrypted by Friedrich Kasiski in 1863!

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

a) What do you call friends who love math? *Mlzlnrhz* (`math`) Algebros

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

b) 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

The Enigma Machine

Some time in the 1920s, a German engineer developed the Enigma machine - an electro-mechanical rotor cipher machine that was eventually used by the Germans during World War II. Although their secret messages were believed to be impossible to decrypt, three very talented Polish mathematicians were able to decrypt the German military messages. However, the Germans increased the security of their Enigma machines making it even more difficult for the Allies to decrypt. This lead to the British government creating a team comprised of some of the brightest minds in the United Kingdom to break Enigma and other German cipher machines. This team (code name: "Ultra") was based at Bletchley Park, England. It was there in Bletchley Park where Alan Turing, the "Father of Computer Science", and a team of cryptographers broke Enigma. It is said that because of Ultra, WWII ended two whole years sooner.

Extra Activity! Using the links below, you can create a Do-It-Yourself Enigma machine!

How to Use the DIY Enigma Machine:
`http://wiki.franklinheath.co.uk/index.php/Enigma/Paper_Enigma`

DIY Enigma Printouts:
`https://fhcouk.files.wordpress.com/2012/05/pringlesenigma3a4.pdf`

Problem Set Solutions

1. Encrypt or decrypt the following messages using the Rail Fence cipher given the key number in parentheses.
   a) Pancake breakfast (4) pek akaf nabeat crs
   b) University of Waterloo (9) uo nyfo itwo vial estr re
   c) wgl heiue efvom nieyos lsn... (5) When life gives you lemons...
   d) ya ond uoe mm ae kl e! (7) You make lemonade!

2. 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

3. 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

4. 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!

5. Why might a cipher be considered bad? Give an example.
   A cipher is bad when it is easy to decrypt. For example, the Caesar cipher is not a good cipher because the frequency of the letters that occur in the plaintext can give away which letter replaced the letter E, since it is the most common letter in the alphabet, and the shift number can be easily determined.

6. Teacher: Why are you doing multiplication on the floor?
   Student: Fvb avsk tl uva av bzl ahislz! (Caesar, shift number: `7`)
   You told me not to use the tables!

7. How do you make seven an even number? Yuxr rmy f bsy!
   (Vigenère, keyword: `funny`)
   Take the s out!

8. Why can't your nose be 12 inches long?
   Bhlt eteudo cenobo asiwef uta! (Rail Fence, key number: `5`)
   Because then it would be a foot!

9. What did the triangle say to the circle? Uoe rns opl ais yet!
   (Columnar Transposition, keyword: `shape`)
   You are pointless!

10. 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? 16

*11. The following ciphertext was encrypted first by Caesar cipher (shift number `4`), then with a Rail Fence cipher (key number `3`). Decrypt the ciphertext.

    `Xiliiycw lwqxnowvexepeymk iesegpqr`

    These math jokes are actually amusing

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

    `xeok xxlb eflp qexk cgsn`

    Secret messages are fun

*13. Anna and Elsa have chosen a different pairing of letters so that they can communicate in secret using the Vatsyayana cipher. You intercept a message between them. Can you decrypt it?

`Vouc Owhu,`

`Ve bea lugk ke yazwv u hgelqug?  Reqo eg, wok'h ne ugv fwub!`

`Etub, ybo...`

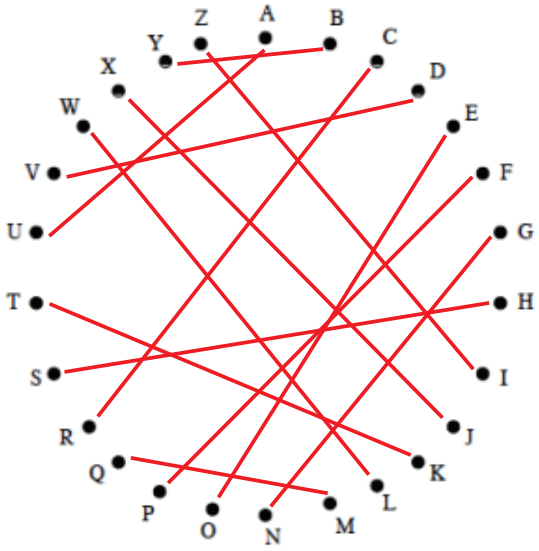
`Wedo, Uggu`

Dear Elsa,

Do you want to build a snowman? Come on, let's go and play!

Okay, bye...

Love, Anna



**14. The following ciphertext was encrypted using a Caesar cipher (shift number `5`), then by a Columnar Transposition cipher (keyword `tiger`), and then a Rail Fence cipher (key number `4`). Decrypt the ciphertext.

`sezzzr ezepaiaecc thsgnndrro esars`

Caesar needs a stronger cipher

***15. The following ciphertext was encrypted using a Rail Fence cipher (key number `3`), then the Vigenère cipher (keyword `cipher`), then a Caesar cipher (shift number `7`), and finally a Columnar Transposition cipher (keyword `plain`). Decrypt the ciphertext.

`otxglay bdpqlny tbcpzig cfugncy cnlcpgx`

There are so many more ciphers to learn!

***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