CIPHER FUN WHEEL

After Edward Snowden's denunciations on NSA espionages, the word **CRYPTOGRAPHY** has been widely spoken in popular communication platforms.

Even if you do not know what it means, you certainly use it and need it more than you can imagine!

When you use social networks, send messages through Whatsapp, Telegram, purchase online, or make bank transactions, cryptography is a necessary thing for your safety, but more than this, **encryption is the only way to protect our privacy!**

SO... WHAT IS CRYPTOGRAPHY?!?!

Cryptography is the use of techniques that transform text or data into an information that can't be understood, where only the sender and the receiver are able to understand it, or, in other words, **encrypt** and **decipher** it. To achieve this, several techniques are used. There's even a history of cryptography that started way before you could possibly imagine it!

Since 2000 B.C., peoples from Egypt and Mesopotamia already used encryption as a secure messaging. The main purposes are for military secrets,

political and, religious but there are many other reasons, where only the sender and recipient should access the content.

Techniques has been modified and improved over time, so the transmission and reception of messages can be more secure.

The purpose of encryption is not to hide the existence of the message, but to hide its meaning.

Another very useful technique is the **steganography**, which is the art of concealing a message. The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples of steganography in "The Histories of Herodotus".

A good example of this technique was during and after World War II. Espionage agents used photographically produced microdots to send information back and forth. Microdots were typically teeny-weeny, approximately less than the size of the period produced by a typewriter. WWII microdots needed to be embedded in the paper and covered with an adhesive. This was reflective and thus detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards.

The advantage of steganography over cryptography alone is that the secret message does not attract attention to itself as an object of close examination.

Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be under surveillance

Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

THE BETTER PART IS, YOU CAN DO BOTH, CRYPTOGRAPHY AND STEGANOGRAPHY AT THE SAME TIME TO KEEP YOUR MESSAGE MORE SECURE!

Along with encryption, emerged the decryption or cryptanalysis, the art or process of deciphering coded messages without knowing the key, converting it back into comprehensive information.

A parallel would be every time an antibiotic is created, the bacteria become more powerful. A parallel to understand how it works would be every time an antibiotic is created, the bacteria become more powerful, and so on. The same happens with cryptography and cryptanalysis.

A marvelous example is, again, during the World War II, when the world seemed to be falling in the hands of the Axis (Nazi's regime allies), Alan Turing along with the Bletchley Park women and men, achieved to break the German cryptography made by the Enigma Machine, supposedly indecipherable, and thus help win the WWII.

The history of codes and ciphers is the history of centuries of battles between code makers and cryptanalysts trying to create and discover the enigmatic messages.

NOW THAT YOU HAVE A BRIEF BACKGROUND, LET'S GO TO THE FUN PART!

You're a spy in a foreigner land, far far far away from home and the enemies are trying to reach you to find out your secrets. You need to send a message back to your country requesting help.

Choose two or three friends to play with (you can play with more people too!). One is the spy, other is the allied and another one, is the enemy.

The spy will write a ciphered message to send to the allied, which will decipher it. The enemy will attempt to read the message, trying some combinations.

We'll send an encrypted and hidden message for your allies using the Cipher Fun Wheel and to be more fun, we'll hide the message using a steganography technique.

Some **VERY IMPORTANT** things you **MUST** know before start:

1# Sender and receiver must know the key code in order to encrypt and read the message.
2# For this, both sender and receiver must have the exactly same Cipher Fun Wheel (or any other cipher method).

3# Finally, it is `crucial` to keep in secret the key code and which encryption technique was used, so that no spies will discover (remember Fox Mulder from X-Files and trust no one)!

HOW DOES IT WORK?

In cryptography, the regular alphabet characters are called the plaintext, and the substitute characters are called the cipher text. This is the "key" to unlock the coded message.

The cipher wheel is a mechanical aid for doing a substitution code. Our Cipher Fun Wheel is an encryption system using 5 rotatable concentric discs with numbers, symbols and letters codes. Each disc rotates independently from each other. When you turn the discs, they align in relation to each other, and this makes an unique key code.

The first disc is the regular alphabet; the other 4 attached wheels are the substitute alphabet. You decide on how to make the substitution by rotating the discs to match one regular character to substitute with special characters.

You code your message by looking at each letter in your message (first disc) and writing down the substitute letters (it's your code!) using one of the other 4 discs (choose only one!). The person who gets this ciphered message will decode it by using the key code to match the letters on his cipher wheel, reading the substitute letters and writing the regular alphabet letters.
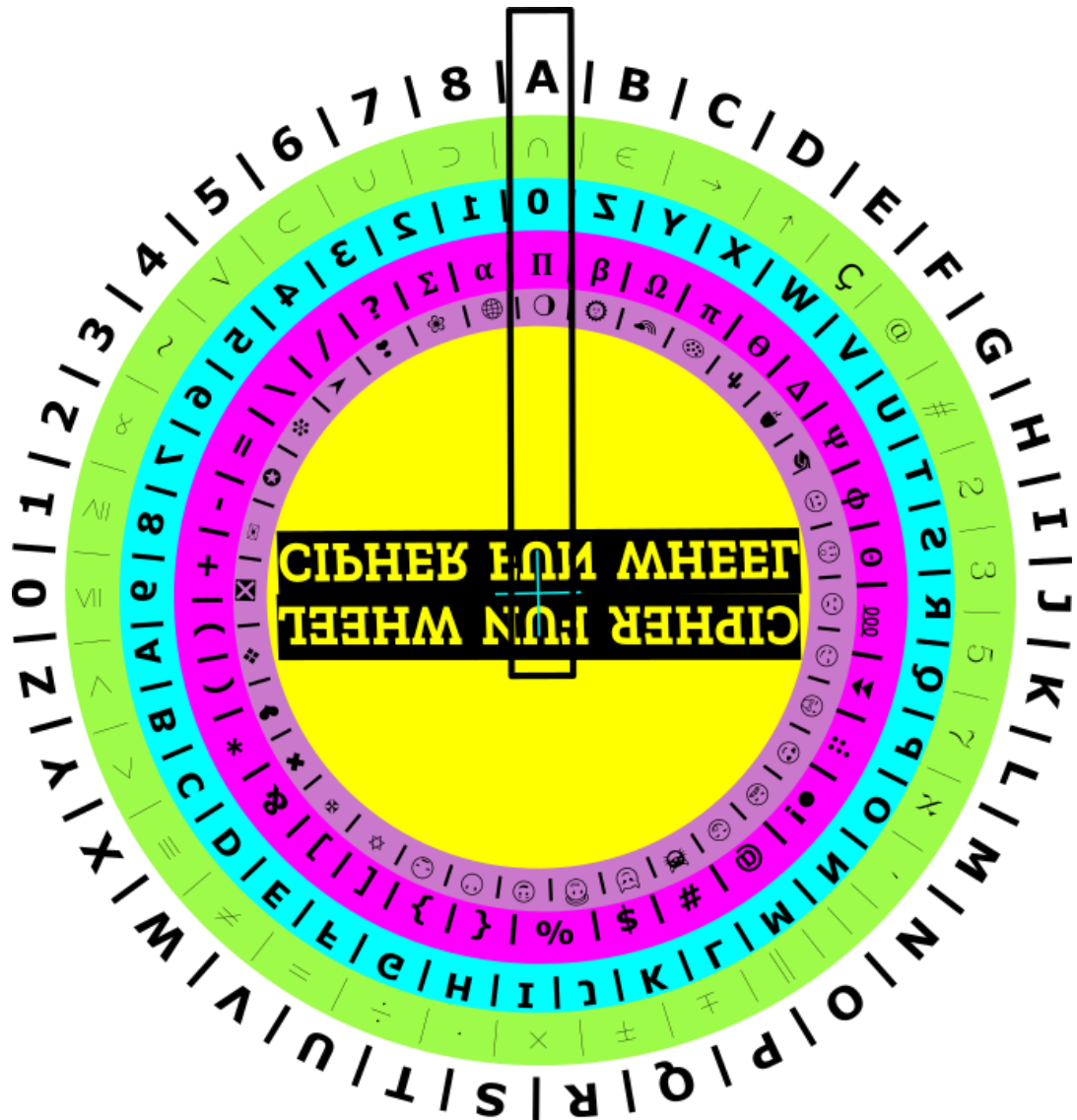
First you must choose a letter/number of the ordered alphabet, usually we start with the letter **A**, then you choose one element of the other wheel (in any disc you want!). With this encryption method, is possible to create over 1.679.616 unique key codes!

Here and now, let's use this example: ∩ 0 𝛑 ◗

So our key code is: A ∩ 0 𝛑 ◗

This is the basis to encrypt and decrypt the message.

Let's start with a simple message: "**HELP ME!**" (note that the wheel does not have punctuation but this will not affect the message).

The receiver must adjust the wheel in this exact position of the key code to be able to decipher the message.

#	🌵	😉	$	😋	W
H	E	L	P	M	E

Now you know what message to send and the key code, let's write it in invisible ink.

You'll need just juice of 1 lemon squeezed in a cup to make your invisible ink. Using a swab as a pen, you will write the encrypted message in a paper sheet. To decipher it, your friend must know the key code and need a source of heat like a lamp, hair dryer, a lighted candle.... But be very careful to don't burn yourself!

Congratulations !!!!

At this moment, you are safe from your enemies. Although, it is never too much take very careful with your communications. We never know who can intercept the messages. Enemies are all around!

Now that you know how to create and read an encrypted message, you can create ciphers that are more elaborate and modify the system.

You can use the **Cipher Wheel Freedom** template for start.