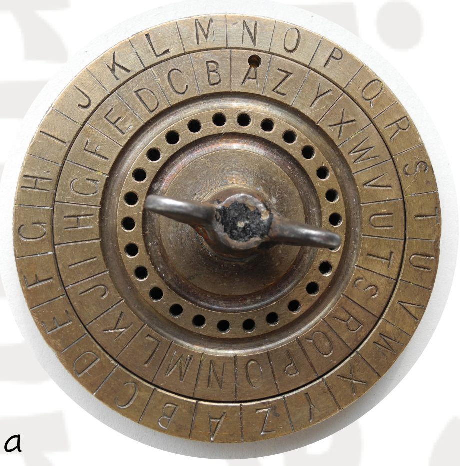
Cryptology

Cryptology is the science of making and breaking secure codes. It is the practice and study of techniques for secure communication.

Until modern times, cryptography referred almost exclusively to **ENCRYPTION,** which is the process of converting ordinary information (called **plaintext**) into **cipher text. DECRYPTION** is the reverse, in other words, moving from the cipher text back to plaintext.

PART I: Caesar Cipher

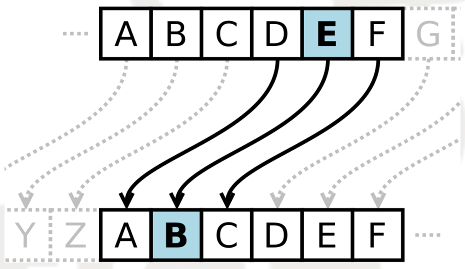


A **CIPHER** is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by an **ALGORITHM** and in each instance by a "**KEY**". The key is a secret and usually a short string of characters, which is needed to decrypt the cipher text

ALPHABET SHIFT CIPHERS are believed to have been used by **Julius Caesar** over 2000 years ago.

The **Caesar Cipher,** also known as a shift cipher, is one of the oldest and simplest forms of encrypting a message. It is a type of ***substitution cipher*** where each letter in the original message is replaced with a letter corresponding to a certain number of letters shifted up or down in the alphabet.

In this way, a message that initially was quite readable, ends up as a cipher text.
For example, here's the Caesar Cipher encryption of a full message, using a left shift of 3.

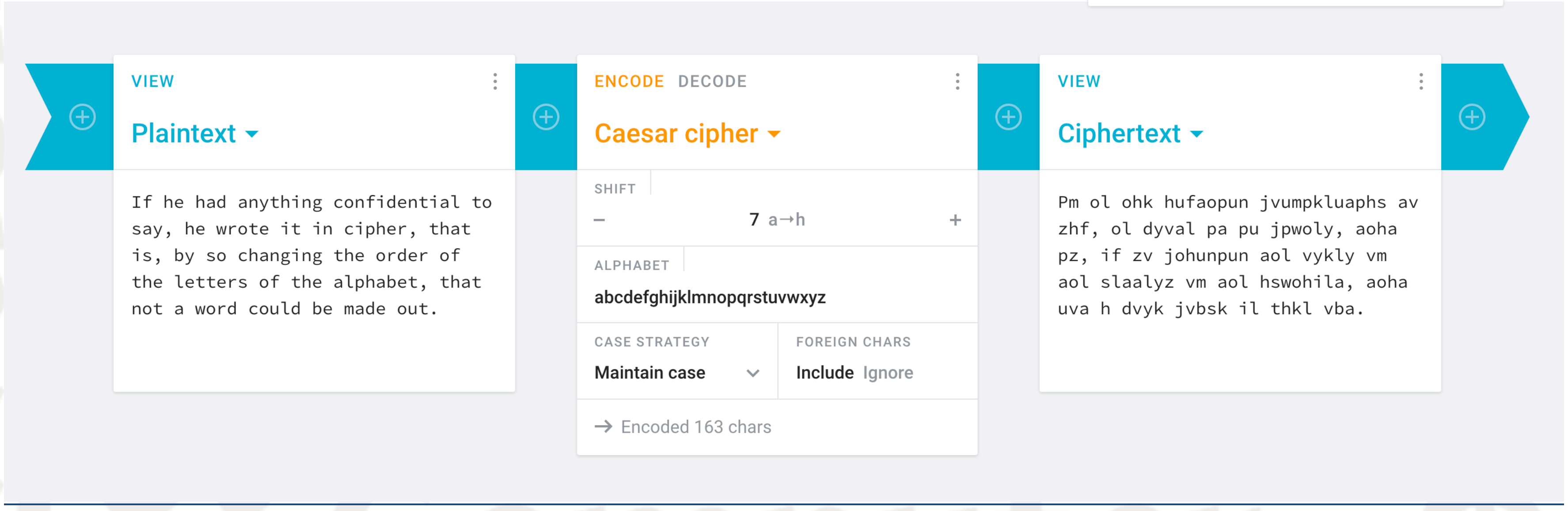


The Caesar Cipher can be expressed in a more mathematical form as follows:

$E_n(x) = (x+ n) \bmod 26$

In plain terms, this means that the encryption of a letter x is equal to a shift of x +n , where n is the number of letters shifted. The result of the process is then taken under modulo division, essentially meaning that if a letter is shifted past the end of the alphabet, it wraps around to the beginning.

1) **Use the webpage below the practice your decoding skills**
https://cryptii.com/pipes/caesar-cipher



VIEW
Plaintext

If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out.

ENCODE DECODE
Caesar cipher

SHIFT
– 7 a→h +

ALPHABET
abcdefghijklmnopqrstuvwxyz

CASE STRATEGY
Maintain case

FOREIGN CHARS
Include Ignore

→ Encoded 163 chars

VIEW
Ciphertext

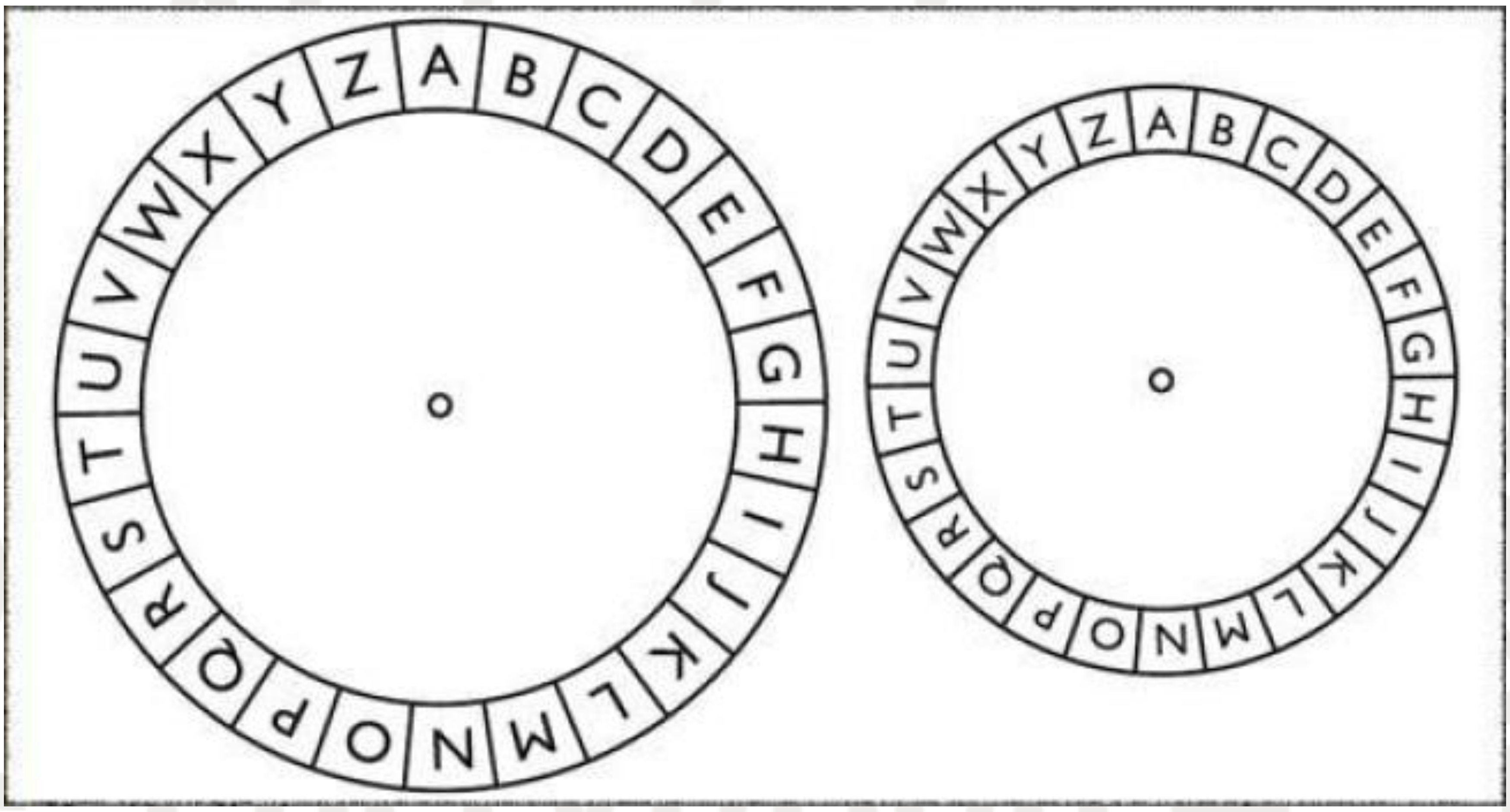
Pm ol ohk hufaopun jvumpkluaphs av zhf, ol dyval pa pu jpwoly, aoha pz, if zv johunpun aol vykly vm aol slaalyz vm aol hswohila, aoha uva h dvyk jvbsk il thkl vba.

Or https://www.boxentriq.com/code-breaking/caesar-cipher

to learn and practice more about the cipher. This cipher tool support English, French, German, Italian, Portugese, Spanish, Swedish.

2) **Create your cipher by using the template below or use the interactive webpage for the wheel. And respond to the following message!**

TEMPLATE:

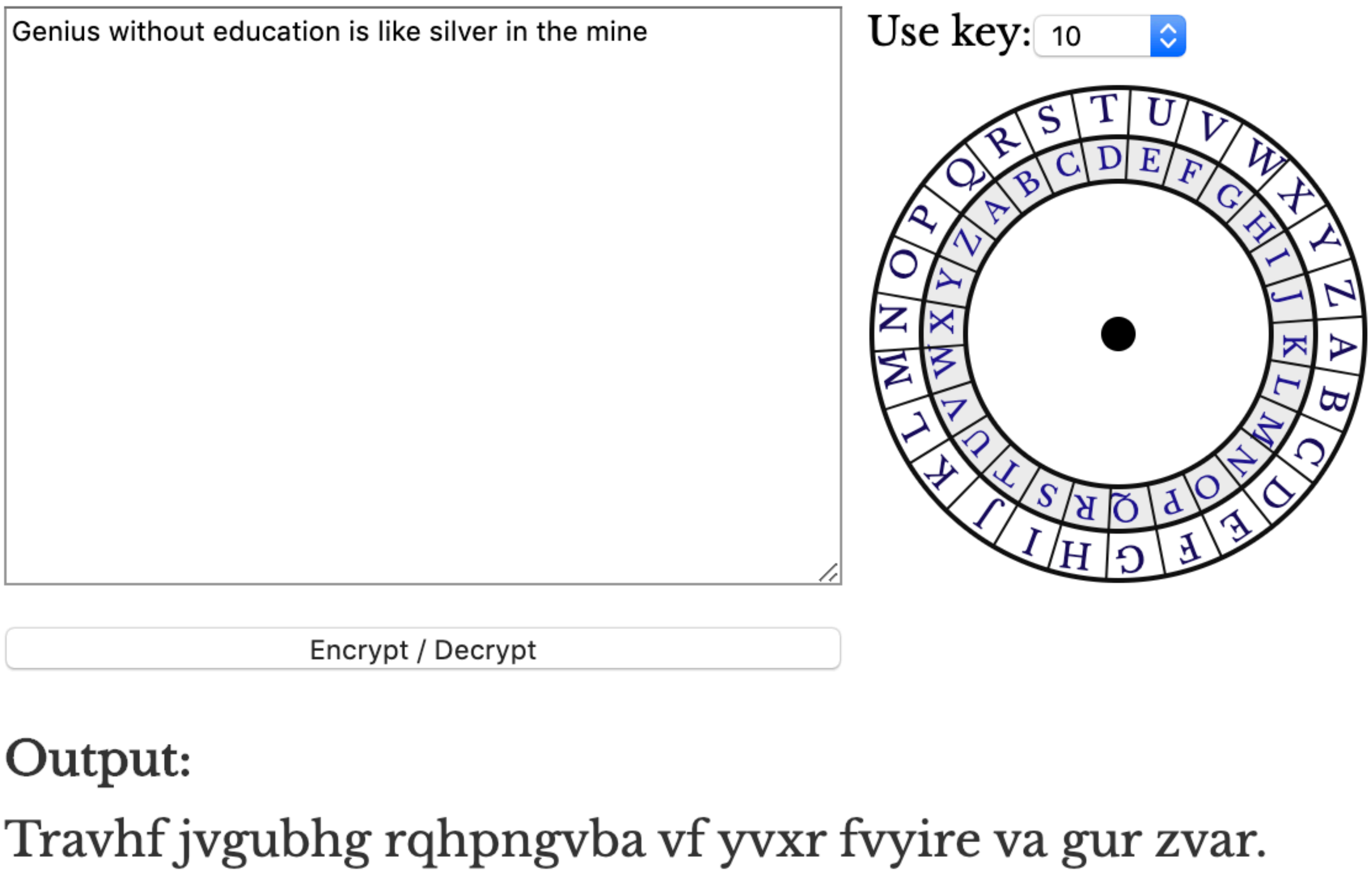

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

This template is taken from https://howtoraiseahappygenius.com/game-cracking-the-code-caesar-cipher-rot-left-1/

Visit the page for a detailed information on the ciphers.

WEBPAGE:

https://www.xarg.org/tools/caesar-cipher/



Genius without education is like silver in the mine

Use key: 10

Output:

Travhf jvgubhg rqhpngvba vf yvxr fvyire va gur zvar.

MISSION: IMPOSSIBLE CRACK THE CODE

"Your mission ,......, should you decide to accept it, is... As usual, should you or any member of your I.M. Force be captured or killed, the secretary will disavow any knowledge of your existence. This tape will self-destruct in five seconds. Good luck, ..."

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

Mr T. sends you this message to decode;

Xtrjynrjx ny nx ymj ujtuqj st tsj hfs nrflnsj fsdymnsl tk bmt it ymj ymnslx st tsj hfs nrflnsj.

Fqfs Yzwnsl

MISSION: IMPOSSIBLE CRACK THE CODE

"Your mission ,......, should you decide to accept it, is... As usual, should you or any member of your I.M. Force be captured or killed, the secretary will disavow any knowledge of your existence. This tape will self-destruct in five seconds. Good luck, ..."

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

Mr T. sends you this message to decode;

Xtrjynrjx ny nx ymj ujtuqj st tsj hfs nrflnsj fsdymnsl tk bmt it ymj ymnslx st tsj hfs nrflnsj.

Fqfs Yzwnsl

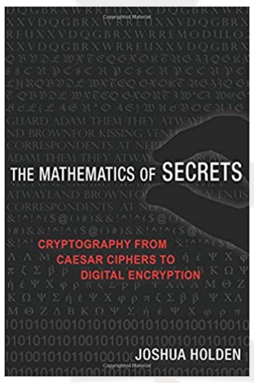
Resources:
https://www.boxentriq.com/code-breaking/caesar-cipher
https://en.wikipedia.org/wiki/Caesar_cipher
https://www.xarg.org/tools/caesar-cipher/

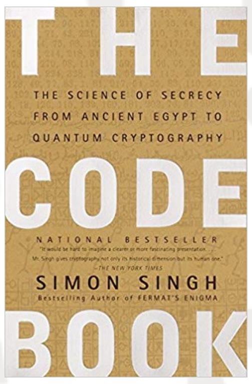
Image Attributions:
https://en.wikipedia.org/wiki/Caesar_cipher

Book Recommendations:

- The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption by Joshuo Holden

- The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography by Simon Singh


THE MATHEMATICS OF SECRETS
CRYPTOGRAPHY FROM CAESAR CIPHERS TO DIGITAL ENCRYPTION
JOSHUA HOLDEN


THE
THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY
CODE
NATIONAL BESTSELLER
SIMON SINGH
Bestselling Author of FERMAT'S ENIGMA
BOOK