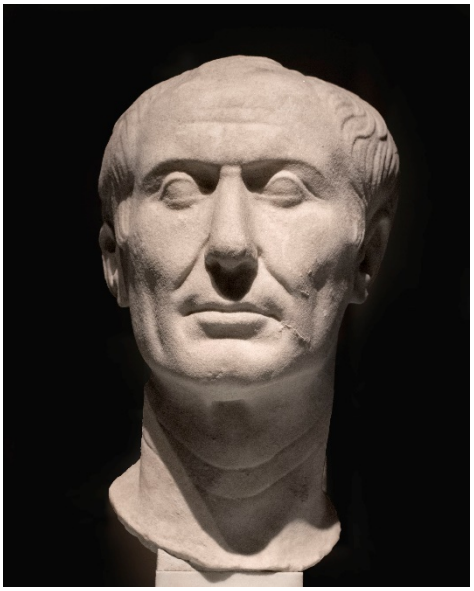
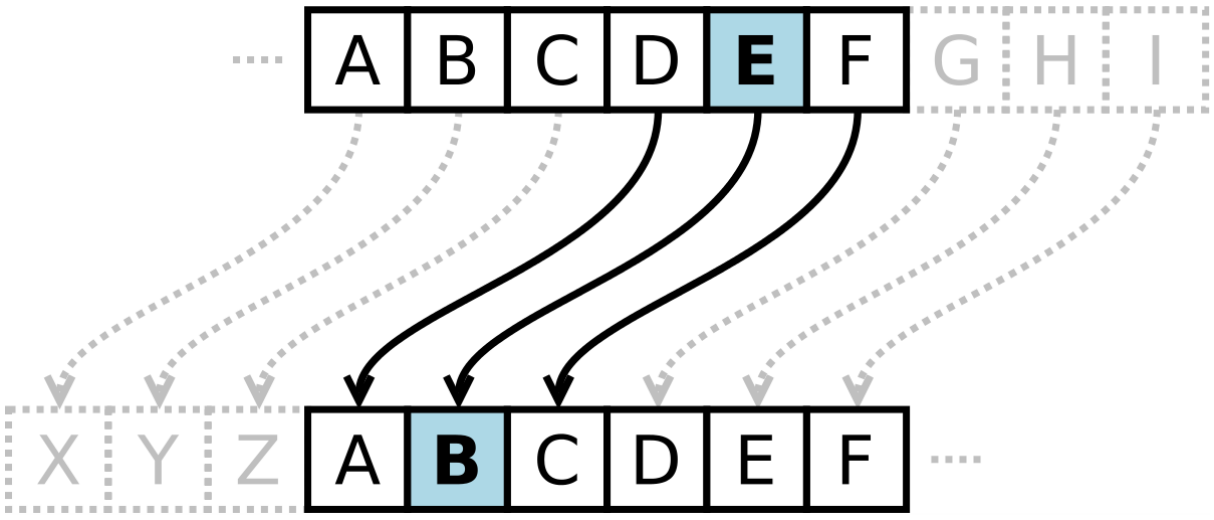
Common and Infamous Codes and Ciphers

Caesar Shift

Named after Julius Caesar, who used it to encode his military messages, the Caesar shift is as simple as a cipher gets. All you do is substitute each letter in the alphabet by shifting it right or left by a specific number of letters. Today, this is seen as one of the simplest forms of code, but it took ancient codebreakers 800 years to learn how to crack it - and nearly another 800 years to come up with anything better.



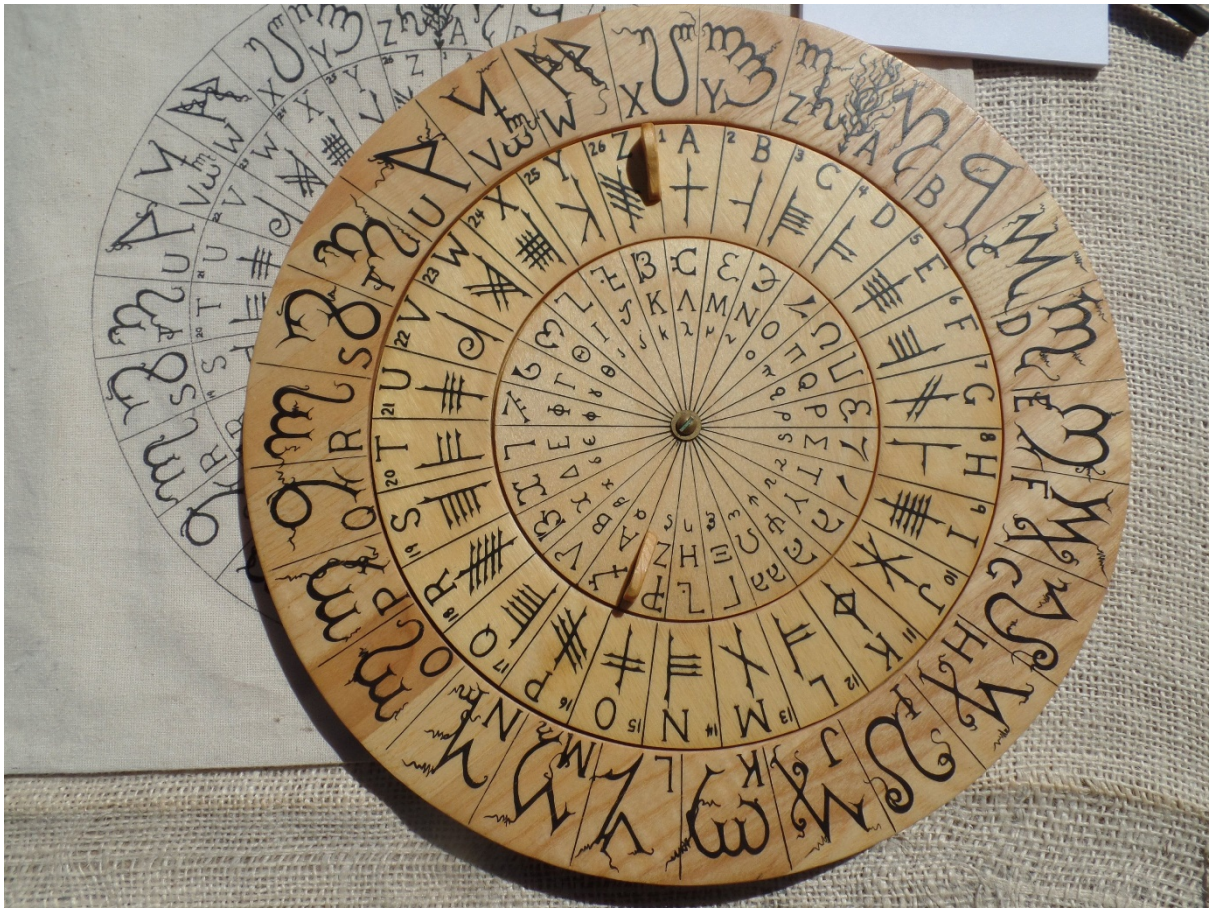
(https://en.wikipedia.org/wiki/Julius_Caesar)



(https://en.wikipedia.org/wiki/Caesar_cipher)

Alberti's Disk

Sometimes called a formula disk. In 1467, architect Leon Battista Alberti described a curious device. It was a disk made up of two concentric rings: the outer ring engraved with a standard alphabet (stabilis), and the inner ring, engraved with the same alphabet but written out of order (mobilis). By rotating the inner ring and matching letters across the disk, a message could be enciphered, one letter at a time, in a fiendishly complex way.

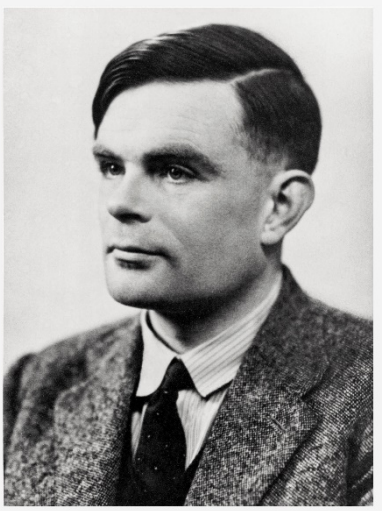


(https://www.pinterest.co.uk/pin/360288038932959096/)

Thanks to the internet, you no longer need to own a physical Alberti's Disk to encode/decode messages yourself.

Enigma Machine

This infamous Nazi coding device may have looked like a typewriter, but hidden inside was the most complex cryptographic system of rotors and gears yet devised. The Enigma was a type of enciphering machine used by the German armed forces to send messages securely. Although Polish mathematicians had worked out how to read Enigma messages and had shared this information with the British, the Germans increased its security at the outbreak of war by changing the cipher system daily. This made the task of understanding the code even more difficult. Allied code-breakers - including British genius Alan Turing and his team at Bletchley Park - worked day and night for years, building machines called bombes to crack the Germans' military messages. Their efforts are estimated to have shortened the war by as much as two years, saving millions of lives.



(https://www.newyorker.com/culture/culture-desk/living-in-alan-turings-future)

(https://www.manchester.ac.uk/discover/news/enigma-machine-visits-the-alan-turning-building/)

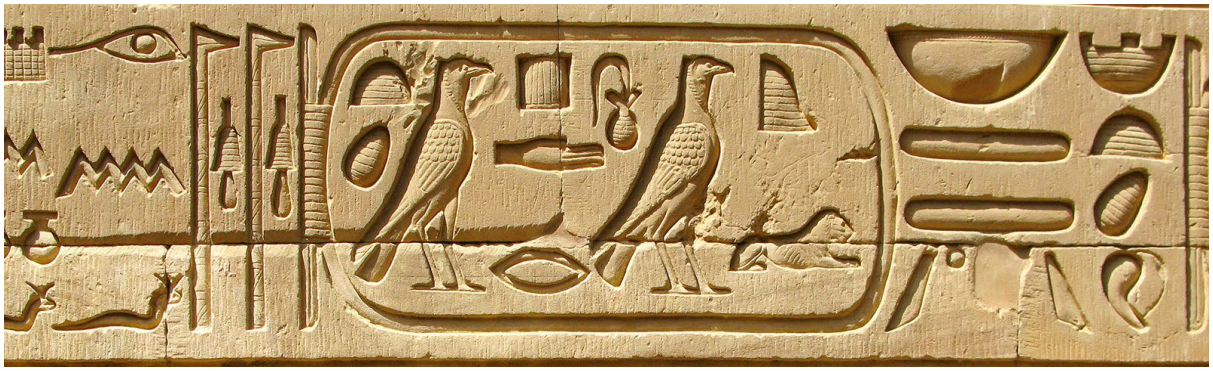
Vigenère Cipher

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

(https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html)

Blaise de Vigenère developed what is now called the Vigenère cipher in 1585. It is an example of a polyalphabetic substitution cipher. A polyalphabetic substitution cipher is similar to a monoalphabetic substitution except that the cipher alphabet is changed periodically while enciphering the message. He used a table known as the Vigenère square, to encipher messages. This 16th-century cipher uses a keyword to generate a series of different Caesar shifts within the same message. Though simple to use, this method of coding resisted all attempts to break it for over 300 years, earning it the nickname “le chiffre indéchiffrable”: the undecipherable cipher. Nowadays, however, they can be broken very easily with the use of online decoders.

Hieroglyphs



(https://www.britannica.com/topic/hieroglyph)

When no one is left who knows how to read a language, it becomes a secret code of its own. That's exactly what happened with the hieroglyphs of ancient Egypt. These beautiful, iconic characters baffled linguists for centuries, until Napoleon's troops discovered the Rosetta Stone, which allowed scholars to match the hieroglyphs with known Greek words, giving us the key to understanding the language and culture of one of the greatest civilizations in history.

(https://blog.britishmuseum.org/everything-you-ever-wanted-to-know-about-the-rosetta-stone/)

Sources

https://www.theguardian.com/childrens-books-site/2015/sep/10/top-10-codes-keys-and-ciphers

https://goto.pachanka.org/crypto/alberti-cipher-disk

https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

https://www.cs.uri.edu/cryptography/classicalvigenere.htm