HISTORY OF CRYPTOGRAPHY

 Version : 0.0.4 Update : 23/03/2022

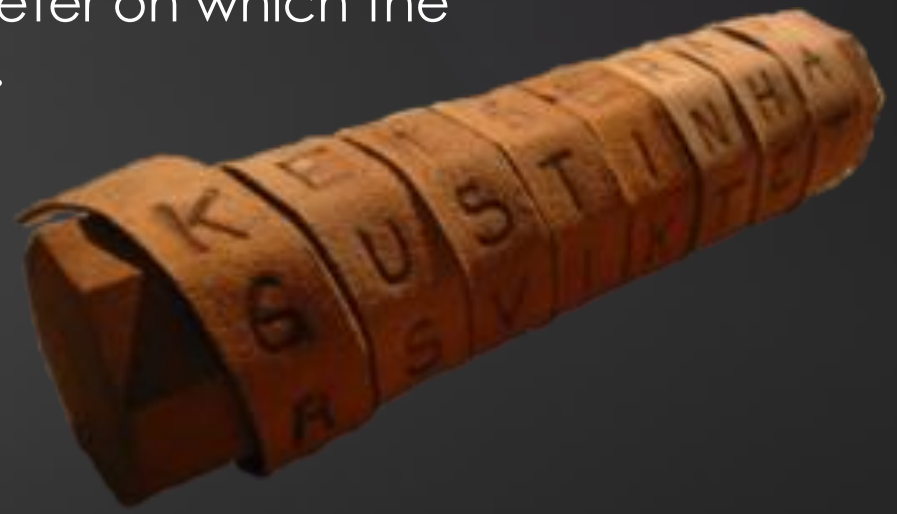
History

- Cryptography appeared in antiquity with **Scytale** (transposition).
- **Caesar cipher** with letters shift (monoalphabetic substitution).
- **Vigenère cipher** with letters shift (polyalphabetic substitution).

- **Enigma machine** created by the Germans (substitution and transposition).

Scytale

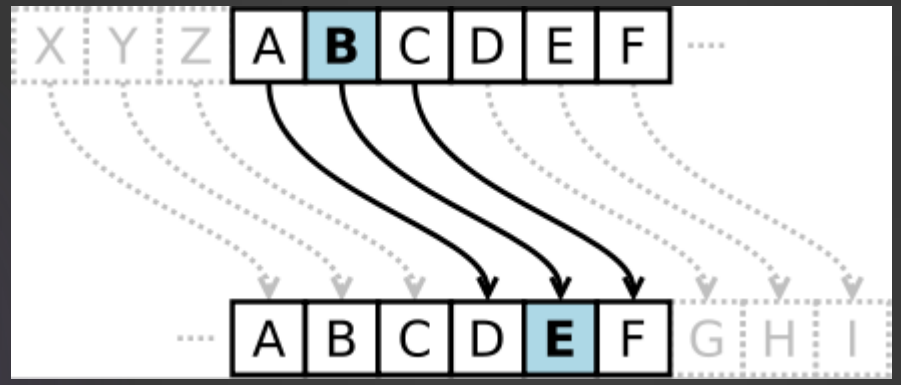
- It's a baton used to perform a transposition cipher.
- It consist of a cylinder with a strip of parchment wound around it on which is written a message.
- The recipient uses a baton of the same diameter on which the parchment is wrapped to read the message.



- Exercise:
  - Decrypt "AQPETUASTERUAZLD".

Caesar cipher

- It's a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.



- Exercises:
  - Decrypt "Oh vruw hq hvw mhwh".
  - Encrypt "Veni , vidi , vici".

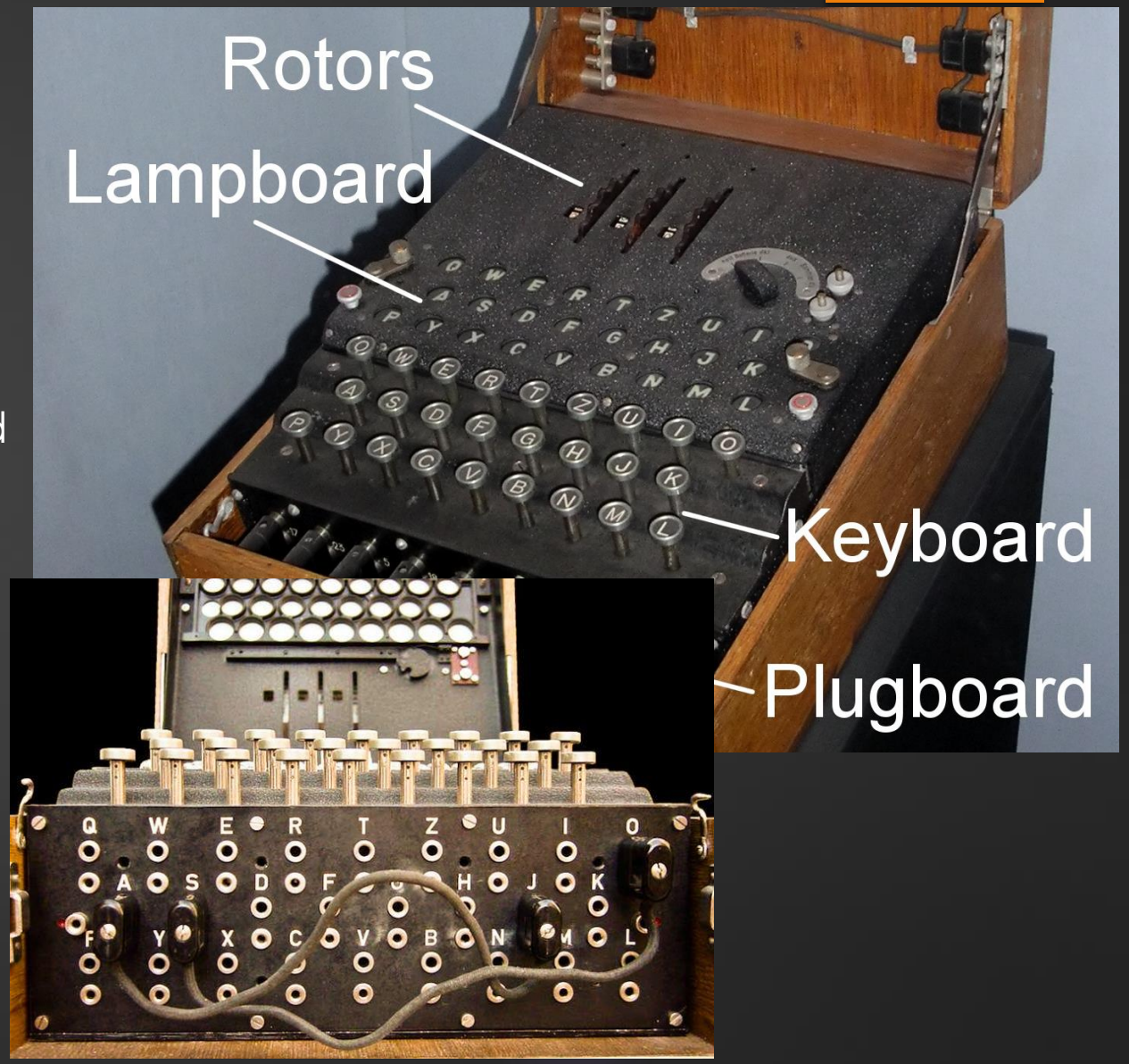
Vigenère cipher

- It has several Caesar ciphers in sequence with different shift values.
- To encrypt and decrypt a table of alphabets must be used.
- The alphabet is written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers.
- Exercises with “CRYPTO” key:
  - Encrypt “CHIFFRE”.
  - Decrypt “XZETGSTV”.

Lettres de la clé \ Lettres en clair	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

Enigma machine

- Used by Nazi during World War 2.
- It was made up of:
  - **Plugboard**: one (or more) letter could be exchanged with another.
    When a key is pressed, the electric current first passes through the exchanged letter cable, before passing through the rotors.
  - 3 **rotors** (with 26 letters) must be chosen (each rotor moves the next like a clock).



INTRODUCTION TO CRYPTOGRAPHY

Concepts

- Hidden a secret for data confidentiality like authentication.
- Non-repudiation (author cannot dispute).
- Data integrity : verify that the information received is the same as the sent. Also called “tamper proof” or “tamper resistant”.

Terms

- **Cleartext / Plaintext** is an unencrypted message.
- **Cyphertext** is an encrypted message.
- **Cipher** is the algorithm used to encrypt and/or decrypt a message.
- **Cryptanalysis** is the art of cracking a cyphertext / an encryption (like mathematiciens who finding weaknesses in cyphers).

Terms : warning in French

- **Cryptologie** c'est la science de la cryptographie.
- **Chiffrement** c'est le procédé de la cryptographie.
- **Déchiffrer** c'est retrouver le message d'origine avec la clé de déchiffrement.
- **Décrypter** c'est retrouver le message d'origine sans la clé de déchiffrement.

- **/!\ Crypter /!** cela signifierait chiffrer un message sans la clé…

Keys

- A **key** is used by the cypher to encrypt message.
- Generally **larger key** are more secure against bruteforce.
- **Encryption can use one or more key**

Story of Alice, Bob and others

- **Alice and Bob:** Generic characters who want to exchange a message or a key.
- **Eve:** An eavesdropper / a passive attacker.

About time

- Cryptographic methods use very large numbers. Table with values allowing to have an element of comparison with other values.

Title	Values
Number of seconds in a day	86 400 seconds
Number of seconds in a year	31,536,000 seconds 3 * 10 ^ 7 seconds
Number of seconds since the creation of the universe (13.7 billion years)	432 * 10 ^ 15 seconds
Number of atoms in the universe	10 ^ 80 atoms

- Now we can say that a message encrypted with the AES-256 algorithm and a machine that can make 100 billion attempts per second, it would take 10 ^ 58 seconds to test all the keys. This necessary computing time is much longer than the age of the universe.