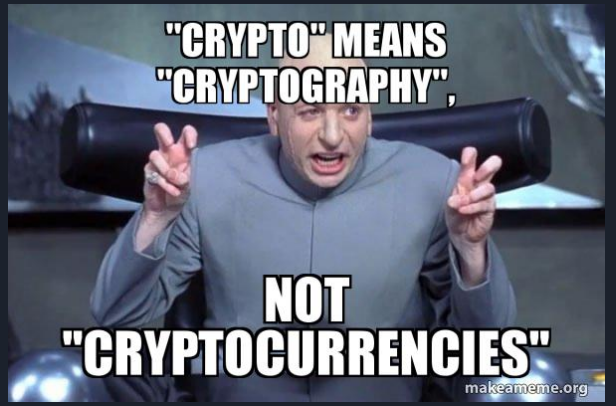
History of cryptography

Cryptography



- **Cryptography**, or cryptology ("hidden, secret") is the practice and study of techniques for secure communication in the presence of adversarial behavior (cryptographic system).
- **Cryptanalysis** ("hidden" and "to analyze") refers to the process of analyzing information systems in order to understand hidden aspects of the systems

- War enables ‘technological’ advances
  - Jules César intensifies
  - Enigma WW2

Cryptography: objectifs

Modern cryptology aims to cover following security needs

- Confidentiality
  - Keep secret information
- Integrity
  - Track modification
- Authentication
  - Who you are
- NonRepudiation
  - The origin of an email, action performed on data

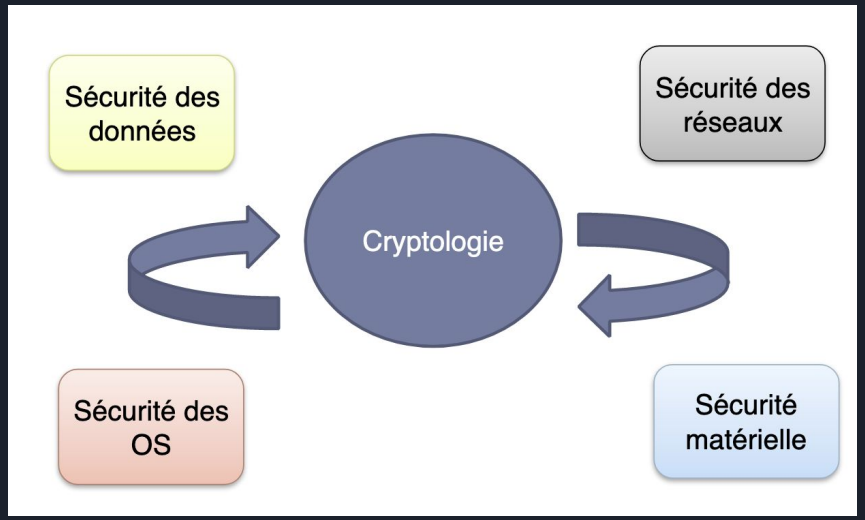
Cryptography: usage

Cryptography is used almost everywhere in our modern world:

- Army
- Banks
- Internet
- Phones
- Your digital ID card
- E-voting system
- Sam . . ng smart fridge

Cryptography: usage

Cryptography is ***essential*** part of IT (Jen ?)



Cryptography: history

Before 20th century cryptography was used only for confidentiality.

The existing means were:

- Steganography (not part of cryptography)
- Cryptography
  - Transposition cipher
    - method of encryption which scrambles the positions of characters (transposition) without changing the characters themselves
  - Substitution cipher
    - method of encrypting in which units of plaintext are replaced with the ciphertext, in a defined manner, with the help of a key

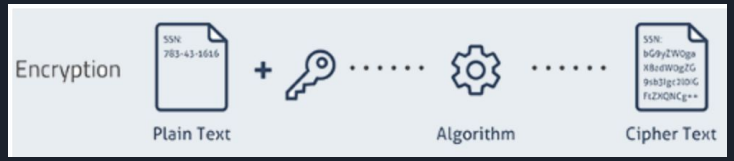
Cryptography != Steganography

Steganography is the practice of concealing a message within another message or a physical object.

Je suis très émue de vous dire que j'ai bien compris, l'autre jour, que vous avez toujours une envie folle de me faire danser. Je garde un souvenir de votre baiser et je voudrais que ce soit là une preuve que je puisse être aimée par vous.[...]

Cryptography: definitions

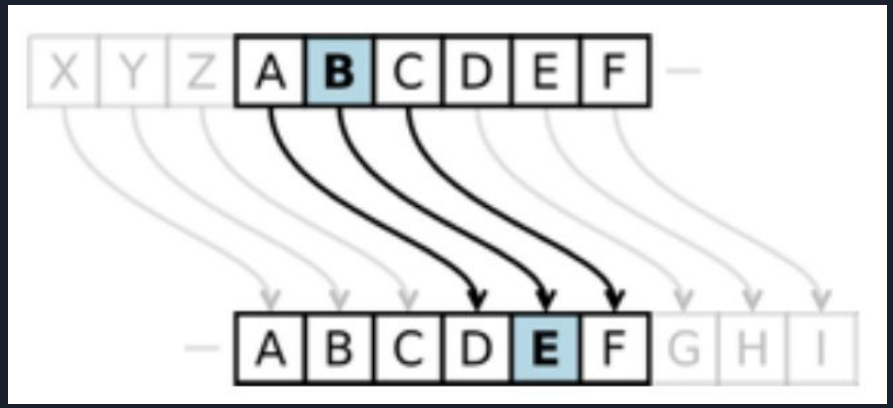
- Plaintext
  - Original message before any modifications
- Key
  - Information used to encrypt and decrypt the message
- Encryption
  - Process transforming plaintext text into ciphertext (unrecognizable form)
  - E ek (M) = C
- Decryption
  - Process converting ciphertext into plaintext (readable and understood by a human or a computer)
  - D dk (C) = M



Cryptography: Substitution cipher

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique.

Each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.



Cryptography: Substitution cipher

Lets encrypt the word CRYPTOGRAPHY with the key 3

Plain text and encrypted alphabet would be:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

And then we replace:

CRYPTOGRAPHIE ---> FUBSWRJUDSKLH

Problem ?

Cryptography: Substitution cipher

What if we assign each letter randomly ?

Key space (number of possible keys) 26! = 400 000 000 000 000 000 000 000 000

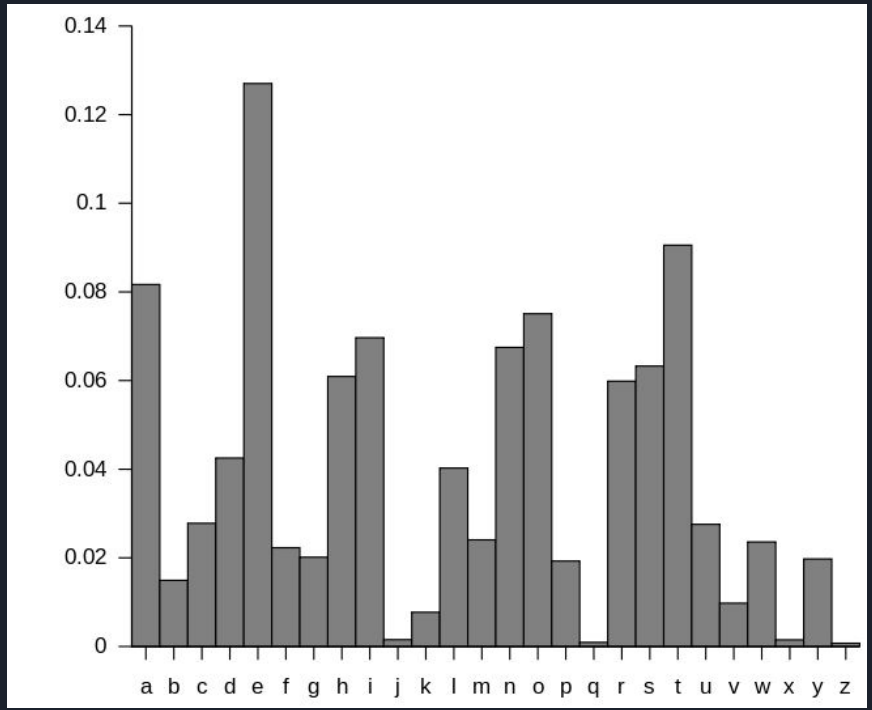
Around 300 years to brute force

~~Problem~~ ? Cryptanalysis

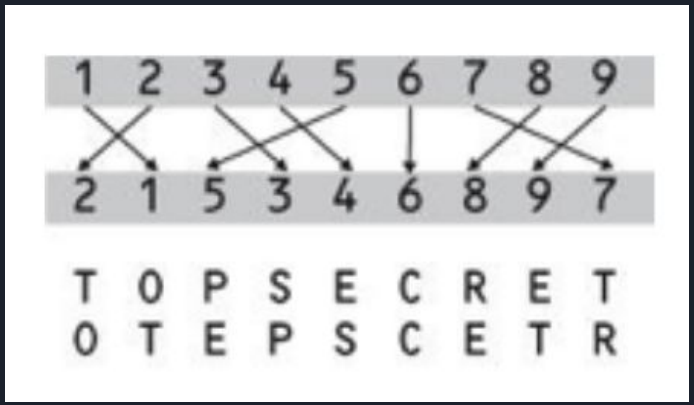
Cryptography: Substitution cipher

Frequency analysis:

In cryptanalysis, frequency analysis (also known as counting letters) is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.



Cryptography: Transposition cipher




```
C I P H E R     Key
1 4 5 3 2 6     Sequence (key letters in alphabetical order)
T H I S I S     Plaintext
W I K I P E
D I A * * *

Ciphertext by column:
  #1 TWD, #2 IP, #3 SI, #4 HII, #5 IKA, #6 SE
Ciphertext in groups of 5 for readability:
  TWDIP SIHII IKASE
```

Cryptography: Monoalphabetic cipher

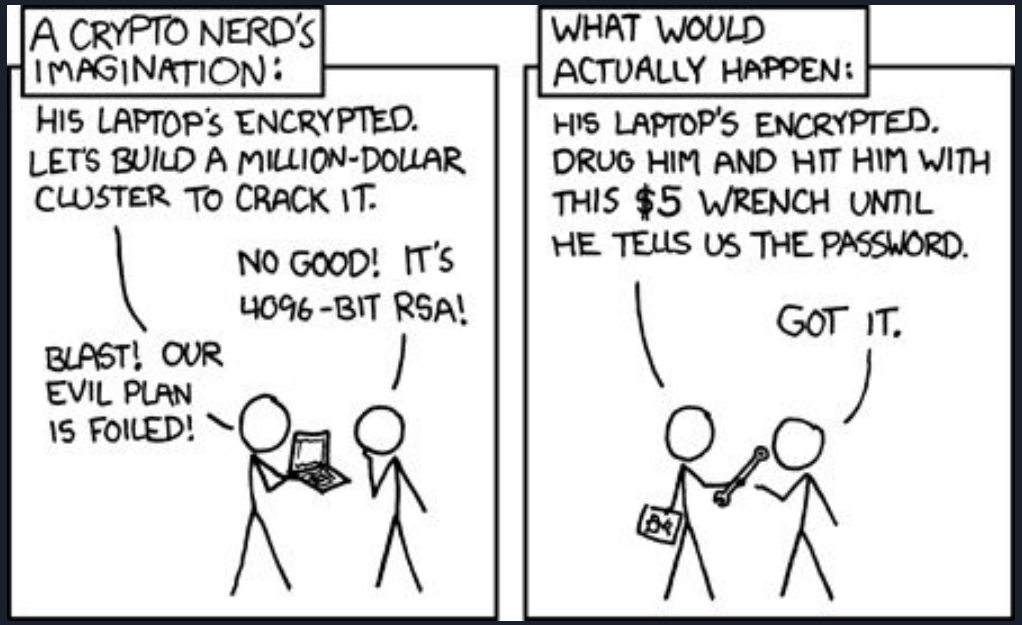
Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if ‘A’ is encrypted as ‘D’, for any number of occurrence in that plaintext, ‘A’ will always get encrypted to ‘D’.

- Used until 16th century

Cryptography: Monoalphabetic cipher

Technological progress is like an axe in the hands of a pathological criminal. (Albert Einstein)

- Enigma WW2


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.