# Topic of english presentation

# Cryptology

Presented by :

**LASSOUANI SOFIANE**

December 12, 2016

# Cryptology

**Steganography** **Cryptography** **Cryptanalysis**

# Cryptology

**Steganography** **Cryptography** **Cryptanalysis**

**Traditional** **Modern**

# Steganography

## *Definition*

- Is the art of dissimultion.
- Is the art of hiding messages That no one suspect the existence

# Steganography

## *Definition*

- Is the art of dissimultion.
- Is the art of hiding messages That no one suspect the existence

Invisible inks : This is one of the first technical steganographic processes and certainly one of the best known. The Romans use it to deceive the vigilance of the enemies and to pass messages.

# Steganography

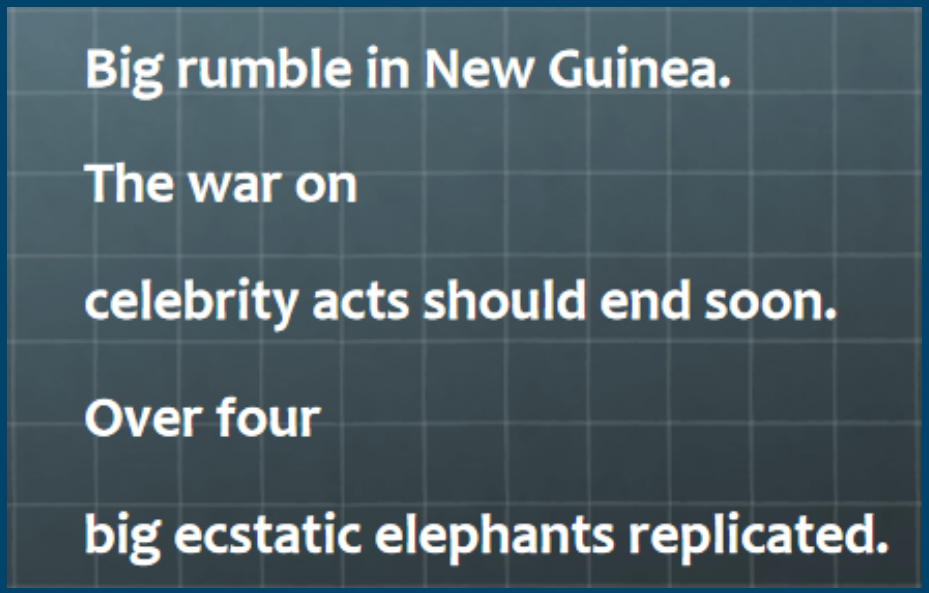
## *Definition*

- Is the art of dissimultion.
- Is the art of hiding messages That no one suspect the existence

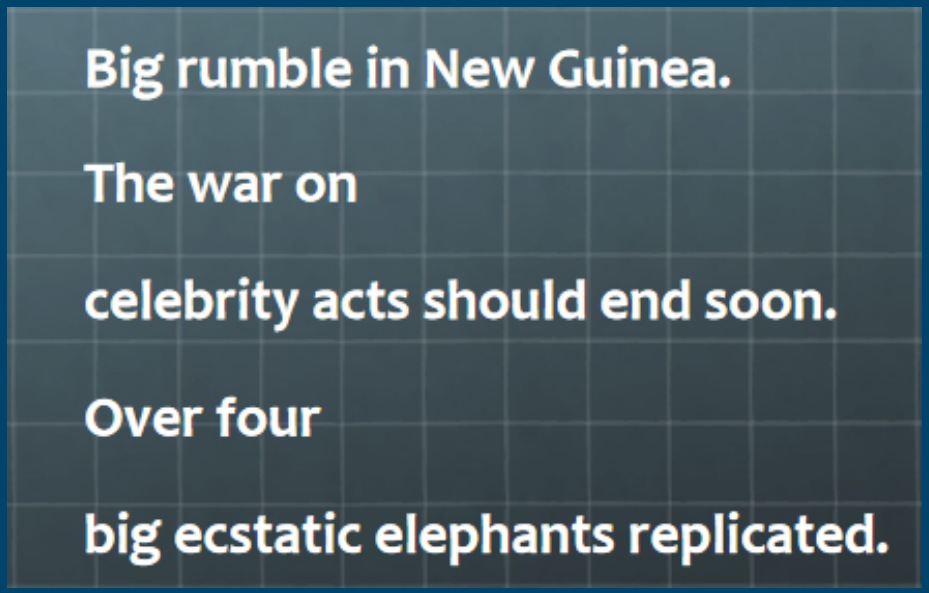
Invisible inks : This is one of the first technical steganographic processes and certainly one of the best known. The Romans use it to deceive the vigilance of the enemies and to pass messages.

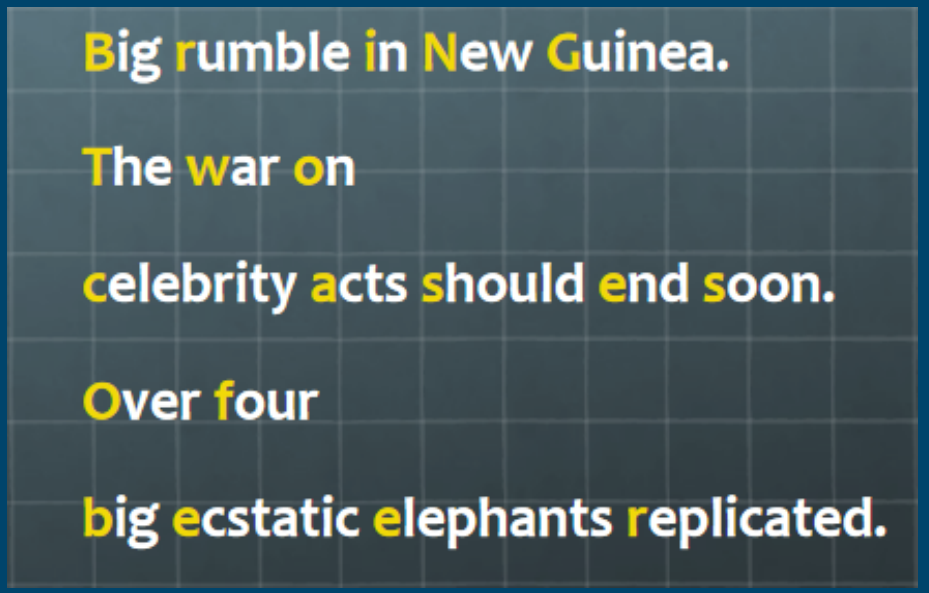
- hide an message in other
- hide an image in other
- hide a text in image

# Hide an message

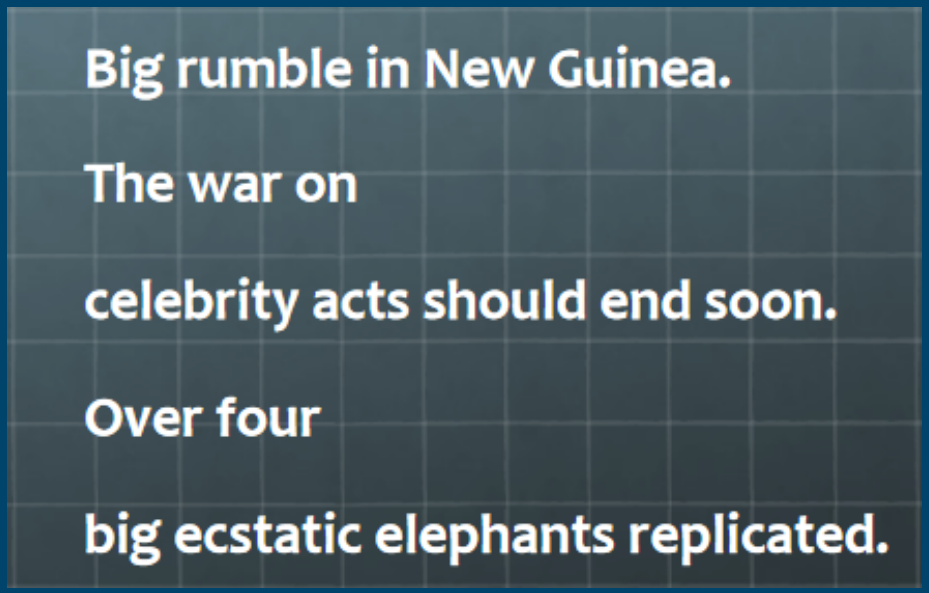


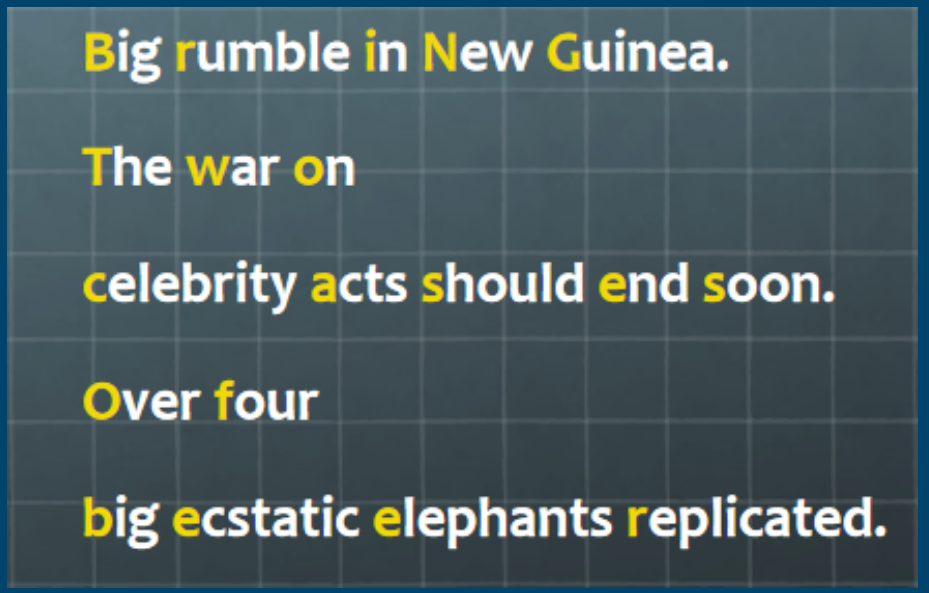
# Hide an message



# Hide an message



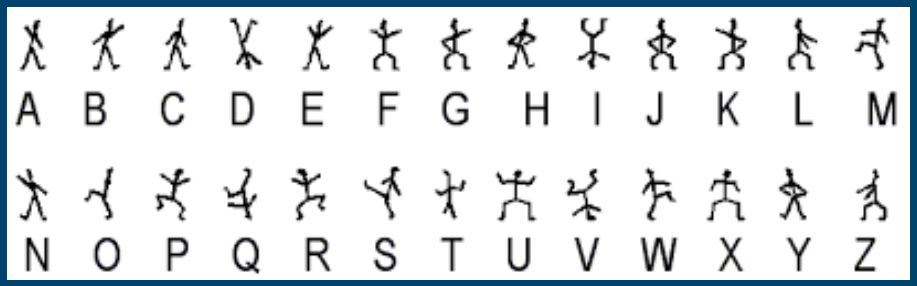

Bring two cases of beer

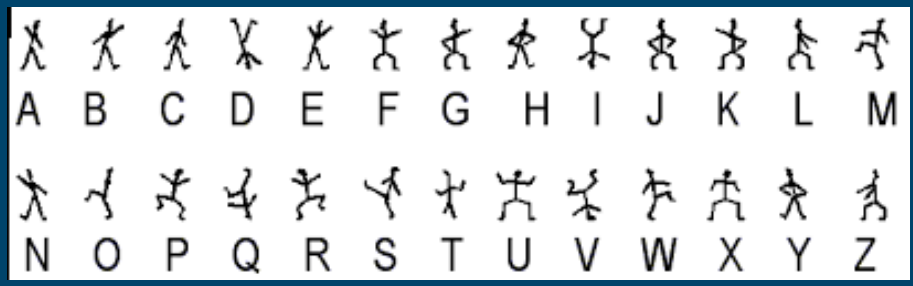
# Hide an image

The Least Significant Beat (LSB) method, or low-order bit method.

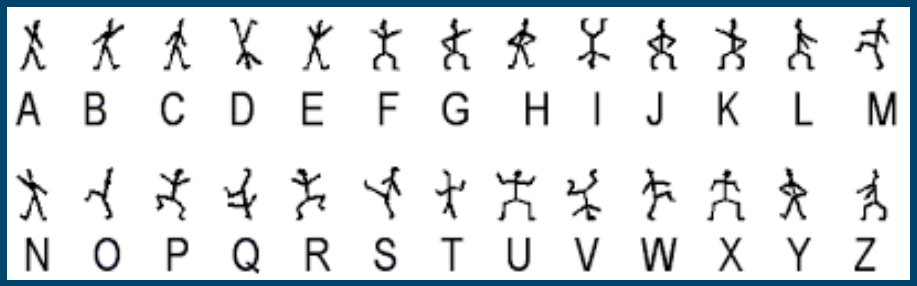
This method consists to modify the least significant bit of the pixels coding the image. An image is a table made up of a set of pixels. For each pixel, the color is coded with three bytes: one for red, one for green, one for blue.

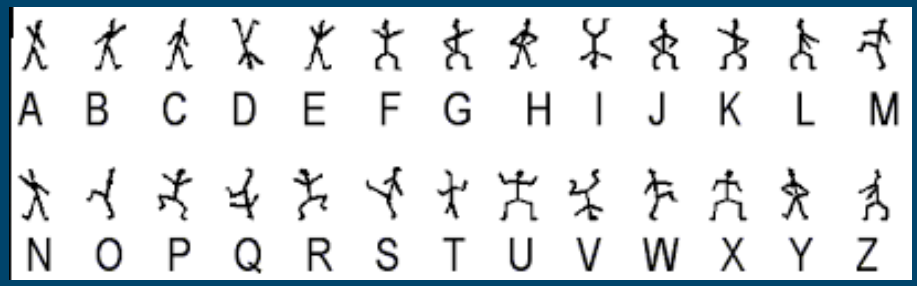
# Hide a text


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

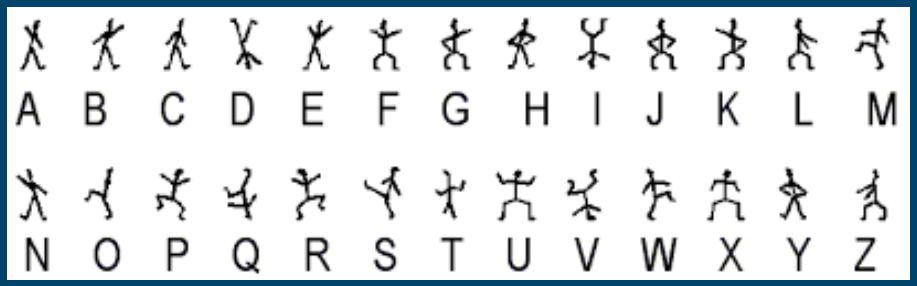
# Hide a text

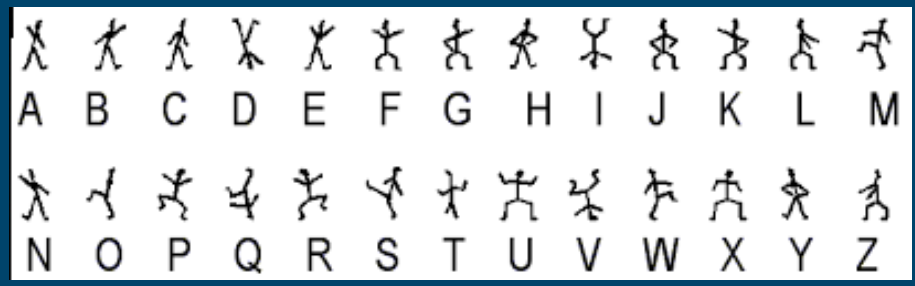



LASSOUANI Sofiane student in master engineering software

# Hide a text




LASSOUANI Sofiane student in master engineering software

https://www.depotnumerique.com/outils/steganographie/cacher-du-texte.php

# cryptography

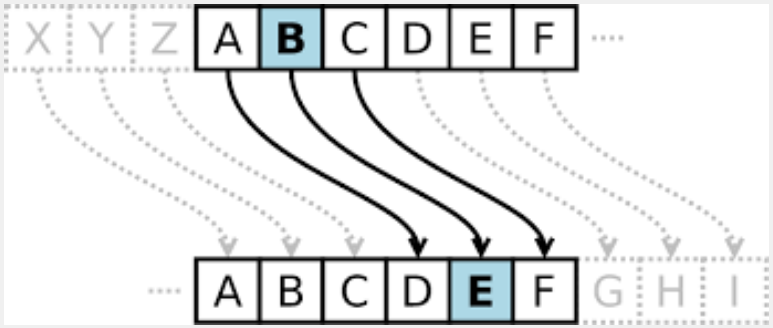
Cryptography is a technique of protecting messages.

- Traditional
  - Substitution
    - Monoalphabetic
    - Polyalphabetic
  - Transpostion
- Modern

# Monoalphabetic

## Cesar.

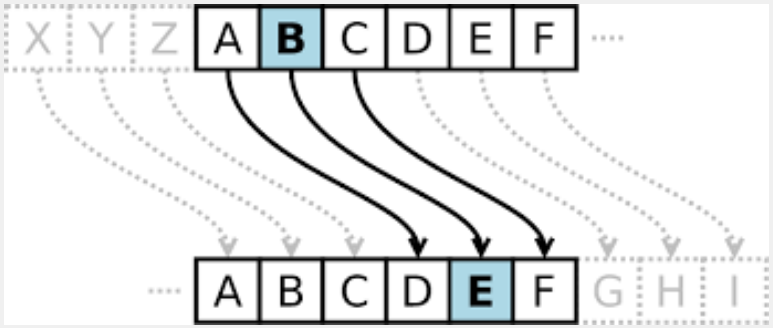
it is a very simple type of encryption used by julius cesar. it is to shift the letters of the alphabet on the right.



# Monoalphabetic

## Cesar.

it is a very simple type of encryption used by julius cesar. it is to shift the letters of the alphabet on the right.




## Exemple

MY PRESENTATION IS ABOUT CRYPTOLOGY

QC TVIWIRXEXMSR MW EFSYX GVCTXSPSKC

# Polyalphabetic

## Vigener.

To encrypt with Vigenere :

- Make correspondence letters to a number

  A=0, B=1, ..., Z=25

- Choose a key

# Polyalphabetic

## Vigener.

To encrypt with Vigenere :

- Make correspondence letters to a number
  A=0, B=1, ..., Z=25
- Choose a key

## Exemple

Text : MY PRESENTAT**I**O**O**N IS AB**O**UT CRYPT**O**L**O**GY

Key : MU SICMUSICMUSI CM USICM USICMUSICM

(M+M)=(12+12)mod26=24 is Y,..., (Y+M)=(24+12)mod26=20 is U

The result is : YU JZGEYFBC**I**C**C**F KE UT**W**WF WRIRF**C**D**W**IK

# Transposition

## Another example

| M | Y | P | R | E | S |
|---|---|---|---|---|---|
| E | N | T | A | T | I |
| O | N | I | S | A | B |
| O | U | T | C | R | Y |
| P | T | O | L | O | G |
| Y | Z | Z | Z | Z | Z |

The text is :MY PRESENTATION IS ABOUT CRYPTOLOGY

The result is : MEOOPYYNNUTZPTI-TOZRASCLZETAROZSIBYGZ

# Transposition

## Another example

| M | Y | P | R | E | S |
|---|---|---|---|---|---|
| E | N | T | A | T | I |
| O | N | I | S | A | B |
| O | U | T | C | R | Y |
| P | T | O | L | O | G |
| Y | Z | Z | Z | Z | Z |

The text is :MY PRESENTATION IS ABOUT CRYPTOLOGY

The result is : MEOOPYYNNUTZPTI-TOZRASCLZETAROZSIBYGZ

- Key= 21543

The result is : YNNUTZMEOOPYSI-BYGZETAROZPTITOZ

# Cryptanalyse

## Definition

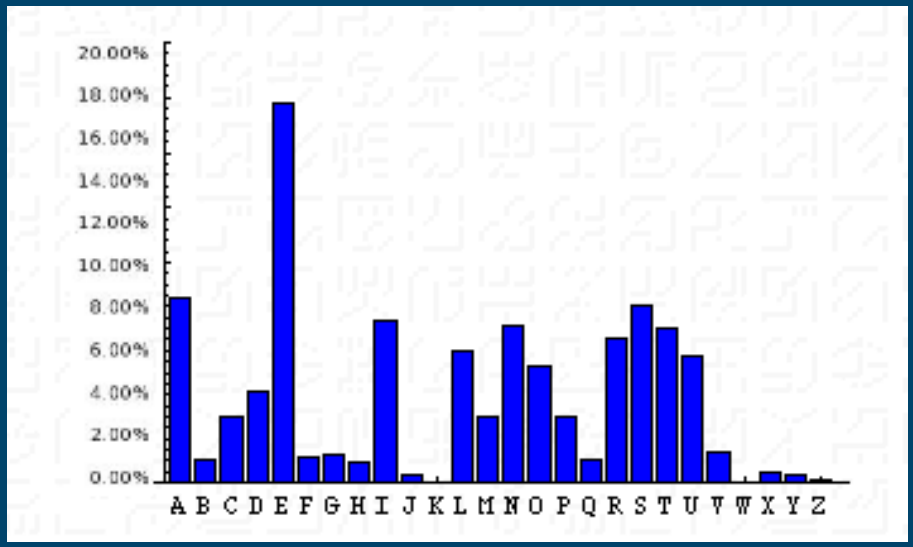
Cryptanalysis is the science of trying to know the encrypted message without having the encryption key

## Frequency analysis

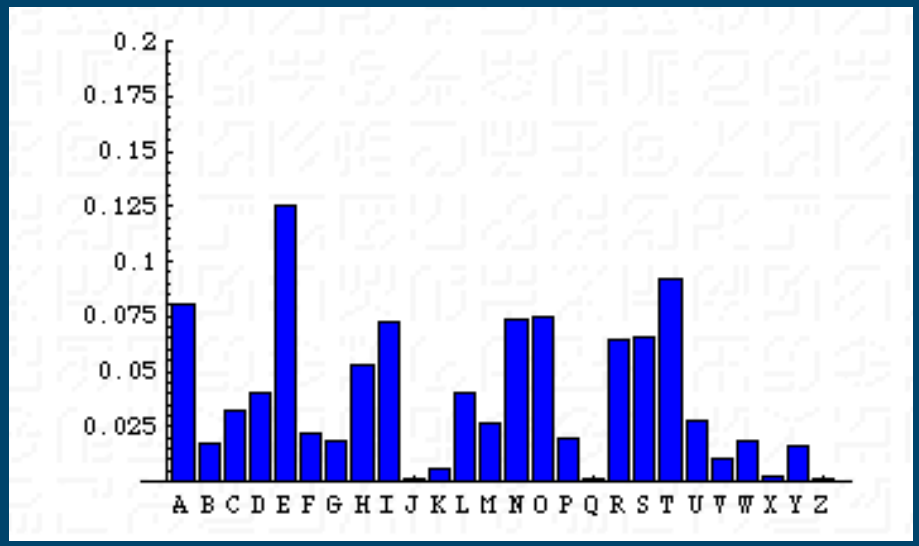
It examines the frequency of letters used in an encrypted message

## Exemple

The frequency analysis is based on the fact that, in every language , some letters or letter combinations appear with some frequency . For example, in French , e is the most common letter , followed by a and s . Conversely, w is little used.

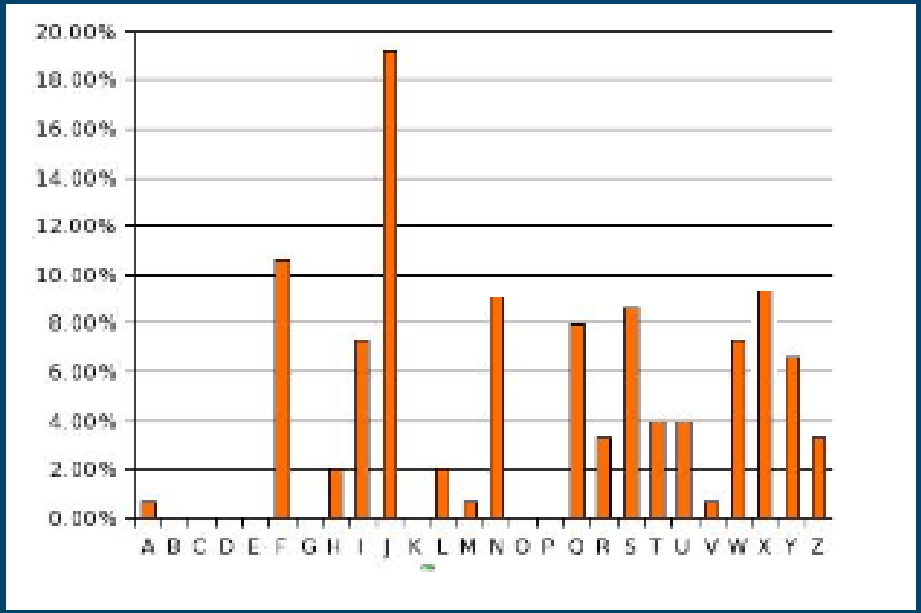


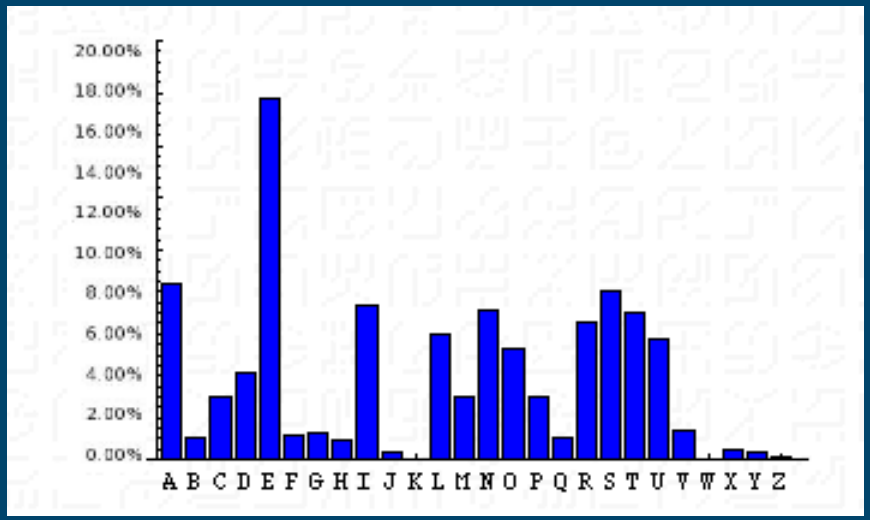

French



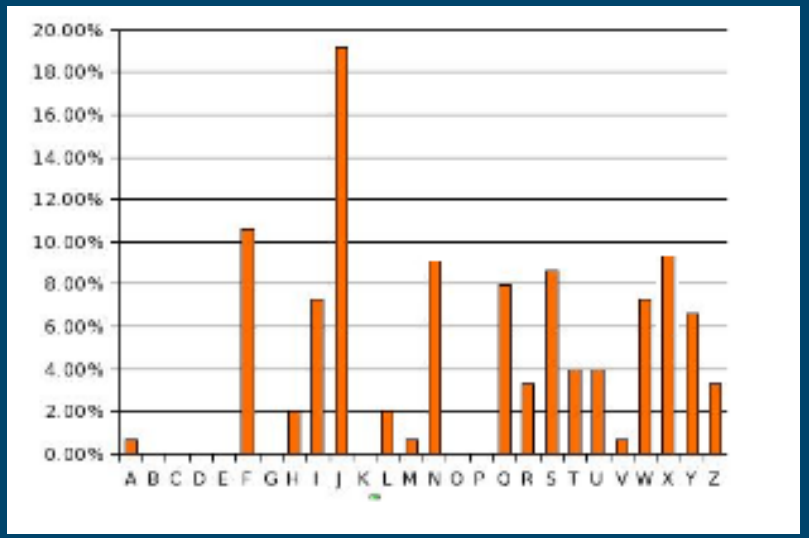

English

AJVFS YQFQT NXJIW JXXJQ JLFWI
NJSIJ QFUTW YJZSM TRRJI JQFHF
RUFLS JXJUW JXJSY JJYIJ RFSIJ
FJSYW JWIFS XQFQT NRFNX
QJLFW INJSI NYVZJ UTZWQ
NSXYF SYNQS JUJZY UFXQZ
NFHHT WIJWQ JSYWJ J

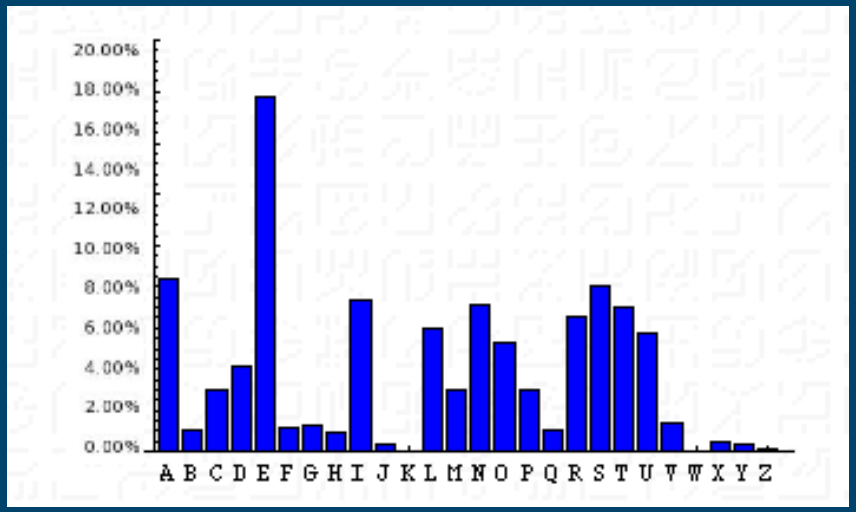


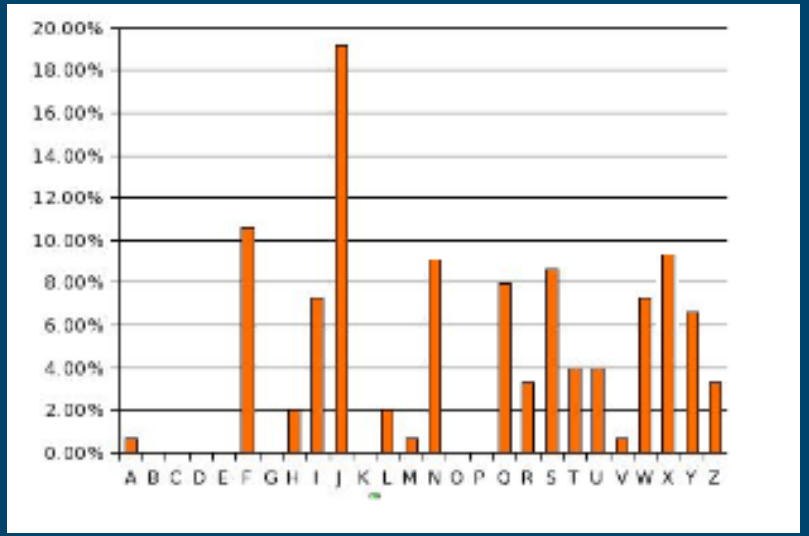



Frensh




Message




.E.... .. ... .E ..E..E .E

.....E. .E .. ....E. ..

....E .E .. .......E .E

..E.E..E E. .E....E .

E...E. .... .. .... .... .E

.....E. ... ..E .... .

..... .. .E .E.. ... ...

......E. . E...EE

AJVFS YQFQT NXJIW JXXJQ JLFWI

NJSIJ QFUTW YJZSM TRRJI JQFHF

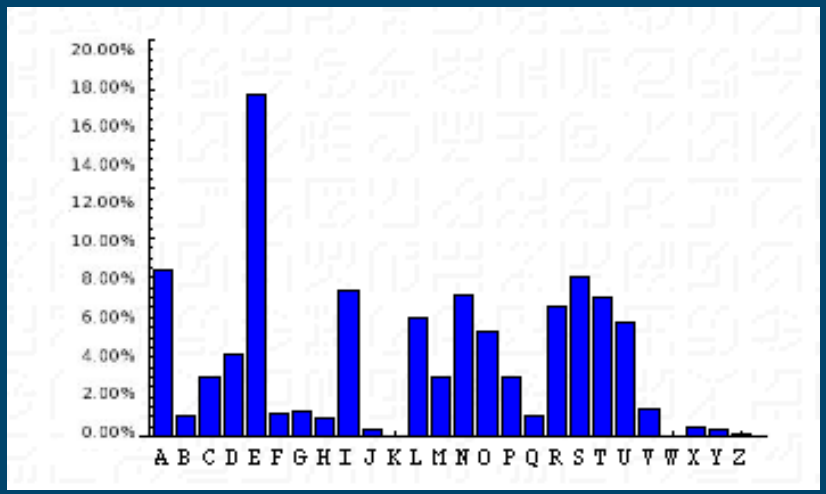
RUFLS JXJUW JXJSY JJYIJ RFSIJ

FJSYW JWIFS XQFQT NRFNX

QJLFW INJSI NYVZJ UTZWQ NSXYF

SYNQS JUJZY UFXQZ NFHHT

WIJWQ JSYWJ J




.E.A.. .A ... .E ..E..E .E

.A...E. .E .A ....E. ..

....E .E .A .A..A..E .E

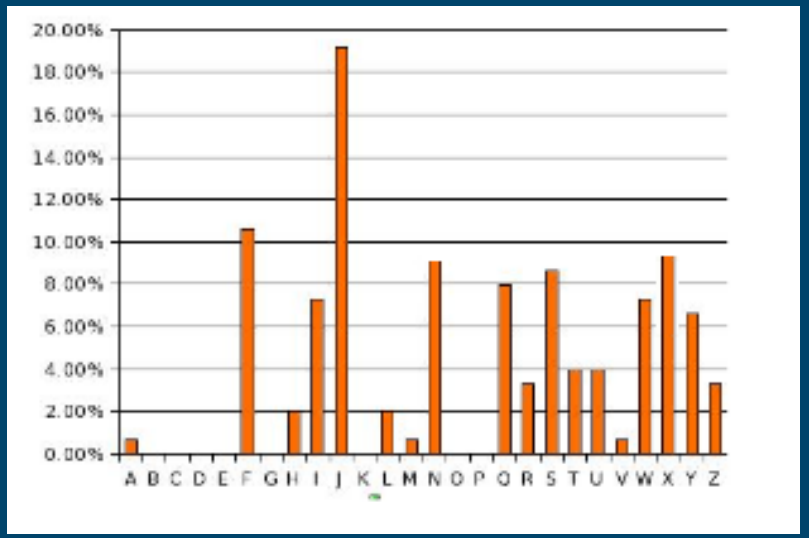
..E.E..E E. .E....E A

E...E. .A.. .A .... .A.. .E

.A...E. ... ..E .... .

....A.. .. .E .E.. .A. ...

.....E. L E...EE




AJVFS YQFQT NXJIW JXXJQ JLFWI

NJSIJ QFUTW YJZSM TRRJI JQFHF

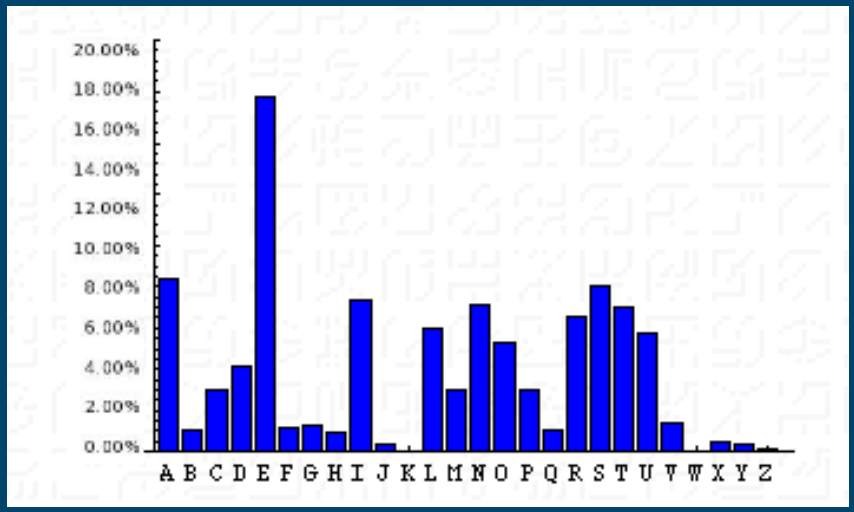
RUFLS JXJUW JXJSY JJYIJ RFSIJ

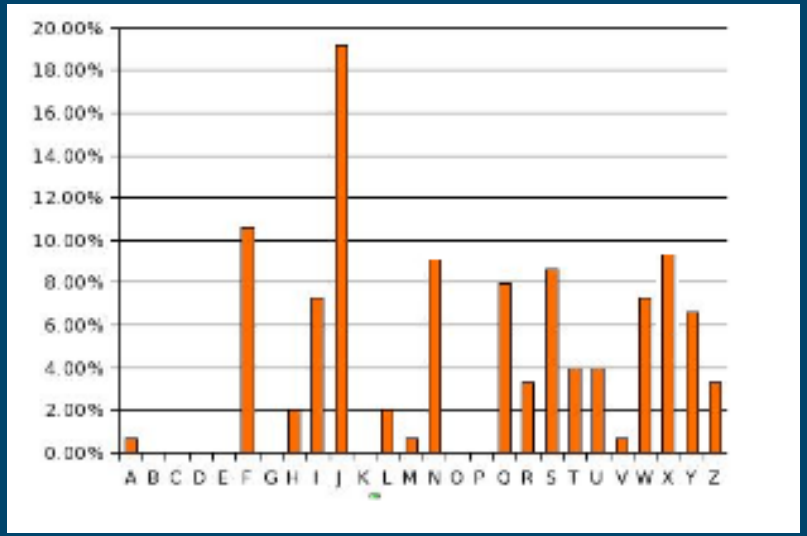
FJSYW JWIFS XQFQT NRFNX

QJLFW INJSI NYVZJ UTZWQ NSXYF

SYNQS JUJZY UFXQZ NFHHT

WIJWQ JSYWJ J




.E.A.. .A ... .E ..ESSE .E

.A...E. .E .A ....E. ..

....E .E .A .A..A..E SE

..ESE..E E. .E....E A

E...E. .A.S .A .... .A.S .E

.A...E. ... ..E .... .

..S.A.. .. .E .E.. .AS ...

.....E. . E...EE

AJVFS YQFQT NXJIW JXXJQ JLFWI

NJSIJ QFUTW YJZSM TRRJI JQFHF

RUFLS JXJUW JXJSY JJYIJ RFSIJ

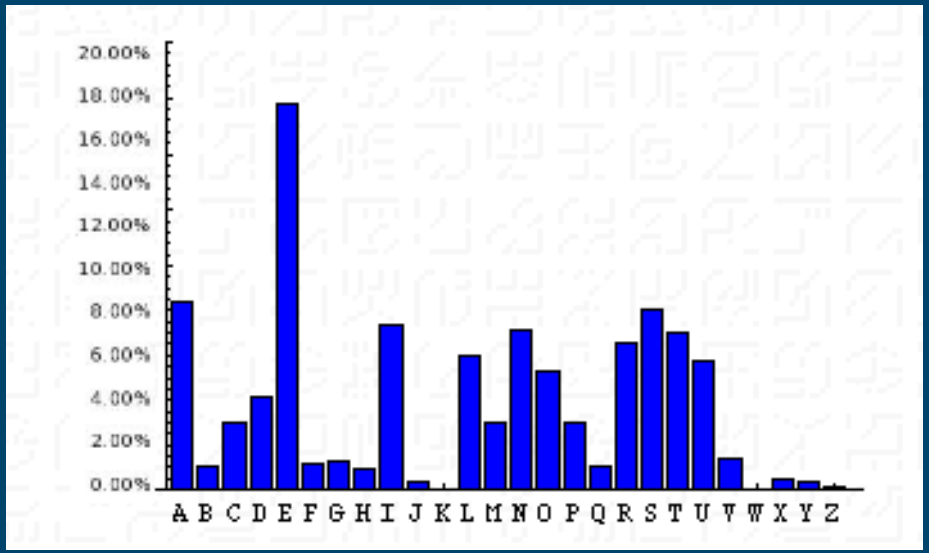
FJSYW JWIFS XQFQT NRFNX

QJLFW INJSI NYVZJ UTZWQ NSXYF

SYNQS JUJZY UFXQZ NFHHT

WIJWQ JSYWJ J

DEVANT LA LOI SE DRESSE LE GARDIEN DE LA PORTE UN HOMME DE LA CAMPAGNE SE PRESENTE ET DEMANDE A ENTRER DANS LA LOI MAIS LE GARDIEN DIT QUE POUR L INSTANT IL NE PEUT PAS LUI ACCORDER L ENTREE



# THANK’S FOR YOUR ATTENTION