

# Rapport

## SAE Crypto 3.04



ETAVE Nathan

&

LEBEAUPIN Louis

21 A/B

2023/2024



## Table des matières :

<a href="#">Message n°1</a>	<a href="#">2</a>
<a href="#">Message n°2</a>	<a href="#">3</a>
<a href="#">Message n°3</a>	<a href="#">4</a>
<a href="#">Dépot GitHub :</a>	<a href="#">4</a>

## Message n°1

Pour déchiffrer ce message, nous avons utilisé la méthode du chiffrement de César. Le chiffrement de César (chiffrement symétrique) est une technique de cryptage où chaque lettre dans le texte est déplacée d'un certain nombre de positions dans l'alphabet. Dans notre cas, le nombre de décalage à effectuer pour retrouver la lettre d'origine est de **12**. Nous avons trois programmes qui permet de déchiffrer un message chiffré avec César, un qui nécessite de renseigner la clé, un autre avec une approche "stupide" qui va lister les 26 possibilités de déchiffrement et une version "intelligente" qui va renvoyer le déchiffrement ayant le plus de correspondance avec des mots d'un dictionnaire français de (336451 mots).

### Message chiffrés:

BDQE PG OTQYUZ EQ OMOTQ GZ FDQEAD  
MOODAOTQ M GZ MDNDQ FAGF DQOAGHQDF P'AD  
ZQ ZQXSUSQ BME XM VQGZQ BAGOQ RQGUXXG  
SDMZP QEF EAZ EQODQF YMXSDQ EM FMUXXQ YQZGQ  
DAZPQE QF OAXADQQE EAZF XQE NMUQE CG'UX BADFQ  
MZUEQQE QF EGODQQE, XQGDE EMHQGDE EAZF RADFQE.  
YMUE MFFQZFUAZ M ZQ BME XQE ODACGQD,  
YQYQ EU XM RMUY FUDMUXXQ FQE QZFDMUXXQE,  
QZ MGOGZ OME FG ZQ PAUE EGOOAYNQD

### Message claire:

PRES DU CHEMIN SE CACHE UN TRESOR  
ACCROCHE A UN ARBRE TOUT RECOUVERT D'OR  
NE NEGLIGE PAS LA JEUNE POUCE FEUILLU  
GRAND EST SON SECRET MALGRE SA TAILLE MENUE  
RONDES ET COLOREES SONT LES BAIES QU'IL PORTE  
ANISEES ET SUCREES, LEURS SAVEURS SONT FORTES.  
MAIS ATTENTION A NE PAS LES CROQUER,  
MEME SI LA FAIM TIRAILLE TES ENTRAILLES,  
EN AUCUN CAS TU NE DOIS SUCCOMBER

## Message n°2

Pour déchiffrer le message 2, nous avons utilisé la méthode de Vigenère.

Dans le chiffrement de Vigenère (chiffrement symétrique), la clé utilisée pour chiffrer le message a la même longueur que le message lui-même. Chaque lettre du message est associée à une lettre correspondante dans la clé, et ce lien détermine le décalage appliqué à chaque caractère du message. Dans notre cas, la clé est "**PANGRAMME**" trouvé dans le message 1, nous allons donc multiplier la clé pour qu'elle ait la même taille que le message.

### Message chiffrés:

AE IOW ZQBLXR WASIXQ WJR YKJ KGYUJAGY UU OXSLN TXRCUQYM  
IY IRCTQ HPNF RR RQBIIIGOFN XQ WTCEKK DQ OIH MHXDUDQW BAYNVUDQYM  
NR MRRPQD SU CXVMUQV HOHLWLQ CYT LRY GRQYMTRRY RPB MVXTVUES  
QF EXNFO UEHAMAEM RV MQEWPGR IRCTQ HTREOVRQ XE HUOYKIFGXXOA

### Message claire:

LE VIF ZEPHIR JUBILE SUR LES KUMQUATS DU CLOWN GRACIEUX  
IL CACHE DANS LA REPETITION LE SECRET DE CES MURMURES MALHEUREUX  
NE GARDEZ DU PREMIER SOUFFLE QUE LES PREMIERES APPARITIONS  
ET AINSI DEVOILEZ LE MESSAGE CACHE DERRIERE LA **SUBSTITUTION**

## Message n°3

Pour déchiffrer le message 3, nous avons utilisé la méthode de substitution monoalphabétique (chiffrement symétrique). Cette méthode consiste à mélanger un alphabet pour en faire une clé. On utilise ensuite cette clé pour chiffrer et déchiffrer un message. Pour ce faire, on remplace chaque lettre du message par la lettre correspondante dans la clé. Par exemple, si la clé est "NZERTYUIOPQSDFGHJKLMWXCVB", alors la lettre "A" sera remplacée par "N", la lettre "B" sera remplacée par "Z", la lettre "C" sera remplacée par "E", etc. Pour déchiffrer le message, on fait l'opération inverse. Pour déchiffrer le message 3, nous avons utilisé la clé suivante : "RXUTBEJHDYOAWPVGMQNSLCKZIF".

### Message chiffrés:

EALOK, OKCT LOFX PLPSF! UF VKIF L ZKCASYA FTD: FUYXFEFDH

### Message claire:

BRAVO, VOUS AVEZ GAGNE! LE CODE A FOURNIR EST: **ELIZEBETH**

## Dépot GitHub :

[https://github.com/LouisL18/SAE\\_Crypto](https://github.com/LouisL18/SAE_Crypto)