

Navigation

Accueil

Sommaire

Introduction

Historique

Clé secrète

Clé publique

Applications

Stéganographie

Conclusion

Annexes

Outils

Bibliographie

A propos

Contact

Le site

1. Le Chiffre de César



Jules César était un général, homme politique et écrivain romain, né à Rome le 12 juillet ou le 13 juillet 100 av. J.-C. et mort le 15 mars 44 av. J.-C. Il aurait été assassiné par une conspiration, son propre fils Brutus lui portant le coup de grâce.

César s'est illustré lors de la guerre des Gaules, ce qui a donné des siècles plus tard son personnage dans la bande dessinée Astérix le Gaulois. Il utilisait une méthode de

chiffrement qui porte aujourd'hui son nom.

Principe

Le chiffre de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Il consiste en une **substitution mono-alphabétique** : chaque lettre est remplacée("substitution") par une *seule* autre("mono-alphabétique"), selon un certain décalage dans l'alphabet ou de façon arbitraire. D'après Suétone, César avait coutume d'utiliser un décalage de 3 lettres : **A** devient **D**, **B** devient **E**, **C** devient **F**, etc. Il écrivait donc son message normalement, puis remplaçait chaque lettre par celle qui lui correspondait :

CLAIR	Α	В	С	D	Ε	F	G	Н	I	J	K	L	М	N	0	Р	Q	R	S	T	U	٧	W	X	Υ	Z
-> décalage = 3																										
CODE	D	Ε	F	G	Н	I	J	Κ	L	М	N	О	Р	Q	R	S	Т	U	٧	W	Χ	Υ	Z	Α	В	С

exemple : d'après cette méthode, "VIVE LES MATHS" devient donc "YLYH OHV PDWKV"

Sécurité

Niveau sécurité, le chiffre de César n'est pas fiable du tout, et ce pour deux raisons :

- Il n'existe que 26 façons différentes de crypter un message : puisqu'on ne dispose que de 26 lettres, il n'y a que 26 décalages possibles. Dès lors, des attaques exhaustives (tester toutes les décalages un à un) ne demanderaient que très peu de temps.
- Le chiffre de César est très vulnérable à l'analyse des fréquences



Outil javascript : cryptez vos messages avec le chiffre de César

Découvrez dans cette section un outil permettant d'utiliser le chiffre de César!



<< Chapitre précédent - Chapitre suivant >>

Page exécutée en 0.027794 secondes.