

Cryptographie, découverte des codes

Objectifs : Découverte de l'histoire des codes ou des codes à travers l'Histoire. Méthodes de cryptages et de décryptages. Création d'un code personnel.

Le Chiffre de César

Le chiffre de César consiste simplement à **décaler les lettres** de l'alphabet de quelques crans vers la droite ou la gauche. Par exemple, décalons les lettres de 3 crans vers la gauche, comme le faisait Jules César (d'où le nom de ce chiffre):

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
Chiffré	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

Ainsi, le message "Ave Caesar morituri te salutant" devient DYHFD HVDUP RULWX ULWHV DOXWD QW.

Le chiffre de César (on parle aussi d' **alphabet décalé**) est un cas particulier d'alphabet désordonné .

Le petit programme javascript ci-dessous vous permettra de chiffrer/déchiffrer un message non accentué avec le chiffre de César. Écrivez votre texte puis choisissez le décalage.

Message clair



CHIFFRE DE CESAR

Décalage



3

+

-



Chiffrer



Déchiffrer

Effacer

A partir du site <http://www.apprendre-en-ligne.net/crypto/menu/index.html>, et des différents pdf fournis, étudier les procédés de chiffrement de l'information.

Les programmes correspondant au code Hébreux et au code de César sont fournis. Etudier plus particulièrement les fonctions utilisées en JavaScript pour obtenir le chiffrement ou le déchiffrement pour chaque programme proposé.

Parmi le code de Wolseley et le code de Vigenère, en utilisant le logiciel firebug associé à Firefox, expliquer comment sont faites les fonctions qui permettent de crypter ou de décrypter.

L'utilisation de firebug est détaillée ici :

<https://openclassrooms.com/courses/firebug-une-merveille-de-plus-pour-firefox>

https://getfirebug.com/wiki/index.php/Main_Page

<https://www.gregoirenoyelle.com/css3-les-outils-pour-inspecter/>

En vous basant sur les acquis ainsi obtenus, créer en l'expliquant un code personnel et les fonctions JavaScript qui permettront de le réaliser. Présenter votre programme fonctionnel sous forme d'une page web (HTML, CSS, JS).