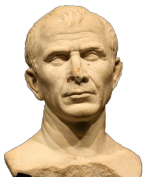

Le chiffrement de César

Par Sylvain BEAUVOIR, Collège François Brossette, Cours-la-Ville

Transmettre des informations de manière confidentielle et secrète est un enjeu depuis des siècles. En temps de guerre, cela permet de transmettre des ordres sans que l'ennemi les intercepte ; aujourd'hui, cela permet, par exemple, de sécuriser les achats par carte bancaire sur internet.

Nous allons voir comment, dès l'Antiquité, Jules César protégeait ses messages.

1. Le chiffrement de César

César utilisait une méthode très simple. Il remplaçait chaque lettre d'un texte par une autre située 3 rangs plus loin dans l'alphabet.

Exemples : *A devient D ;* *G devient J ;* *M devient P* *… etc*

Ainsi, « BONJOUR » devient « ERQMRXU ».

Nous allons donc créer un programme pour transformer, selon le chiffrement de César, des mots. Pour cela, nous allons utiliser un tableur.

2. Une machine à chiffrer …

1. Ouvrez une page de tableur

2. Saisissez le tableau suivant :

	A	B	C	D	E	F	G	H
1	Mot à transformer :	B	O	N	J	O	U	R
2	Rang de la lettre à transformer :							
3	Rang de la lettre après transformation							
4	Mot après transformation :							

NB : On ne rentrera qu'une lettre en majuscule du mot à transformer par case.

3. On va chercher à connaître le rang dans l'alphabet de chaque lettre, par exemple la lettre A est au rang 1, B au rang 2, … etc. Pour se faire nous avons besoin de la table ASCII.

La table ASCII ?!
Chaque caractère tapé au clavier a un numéro de code pour l'ordinateur. On peut résumer tous ses numéros dans un tableau, appelé table ASCII. Par exemple, les lettres majuscules ont les numéros allant de 65 pour le A à 91 pour le Z.

4. La fonction **code(*[lettre]*)** prend une lettre et renvoie son code dans la table ASCII.
Qu'affiche le tableur, si je tape *=code(B1)* dans la cellule B2 ? _____
Quelle formule faut-il taper alors en B2 pour obtenir le rang de la lettre située en B1 dans l'alphabet (pour B, on doit obtenir 2) ? _____
Copier cette formule tout au long de la ligne 2.

5. On transforme la lettre B (situé au rang 2 dans l'alphabet) par le chiffrement de César. Quelle sera le rang de la nouvelle lettre ? _____

6. Quelle formule faut-il taper en B3 pour trouver le rang des lettres du mot transformé ? _____

Copier cette formule sur toute la ligne 3.

7. Maintenant on va demander à l'ordinateur de nous dire quelle lettre correspond à chaque rang. Pour cela, on utilise la fonction **car(*[nombre]*)** qui prend un numéro et renvoie le caractère qui correspond dans la table ASCII.
Quelle formule faut-il taper en B4 pour obtenir la lettre après le chiffrement de César ?

_____

Copier cette formule sur tout la ligne 4.

8. Vérifier que « BONJOUR » devient « ERQMRXU ».

3. … qui a des limites

9. Que se passe-t-il si on essaie de transformer le mot « YEUX » ? _____

_____

10. Pour quelles lettres de départ aura-t-on un problème ? _____

11. Avec le tableur, on peut ajouter des conditions dans les formules avec la commande :

SI([test] ; [valeurV] ; [valeurF])

Par exemple la formule *=SI(B1>10;0;1)* pourrait se traduire par : « *Si le nombre dans la case B1 est plus grand que 10 alors j'affiche 0 sinon j'affiche 1* ».

En utilisant cet outil, améliorez votre machine pour qu'elle renvoie toujours la bonne lettre après le chiffrement de César.

4. A vous de jouer !

12. Choisissez un mot, transformez-le et donnez-le message codé à un autre groupe, arrivera-t-il à trouver le message d'origine ?

13. C'est long de décoder un message à la main …
En vous inspirant de la machine que l'on a réalisée, créez vous aussi une machine à décoder les messages.

5. Et si on jouait avec la clé ?!

Jules César avait décidé de décaler les lettres de 3 rangs, mais on pourrait très bien décaler de 4, 5, 6, … rangs. Ce décalage est appelé « clé de chiffrement ». Il suffit de choisir une clé et de se mettre d'accord avec le récepteur du message codé.

14. Quelles valeurs peuvent prendre la clé de chiffrement ? _____

15. Choisissez une clé de chiffrement et adaptez votre machine à chiffrer puis codez un mot.

16. Demander à un autre groupe, auquel vous aurez communiquer votre clé, de déchiffrer le message que vous avez codé.

6. Pirates !

17. Interceptez un message codé d'un autre groupe sans connaître la clé de chiffrement utilisée. Trouvez une solution pour décoder ce message.

Remarques :

- adapter ce travail avec d'autres méthodes de chiffrement
- travail en lien avec l'Histoire, Alan Turin et la machine Enigma, …
- doit-on rajouter une ligne pour le passage par le code ASCII
- complexité du chiffrement, fiabilité.