Projet:
Chiffre de César et Chiffre de Vigenère

SABABADY Kamala et SELVARAJAH Dinusan

January 12, 2018

1 Partie 1 : *Le chiffre déchiffrable de Jules César*

Jules Cesar (100 av.J.-C - 44 av.J.-C), celebre empereur romain

Jules César , célèbre empereur romain a utilisé la cryptographie en inventant le chiffrement par décalage c'est à dire il rendait illisibles ses messages pour se protéger de ses ennemis au cas où ses messages tombent entre leurs mains. Vous allez voir que sa technique était très simple à comprendre mais aussi à pirater .

Par exemple imaginons que Jules veut envoyer ce message " allez les bleus " , il aimait utiliser le chiffre 3 comme clé pour procéder à son cryptage mais nous on peut changer ce chiffre donc voyons ce que ça donne avec le chiffre 2 :

La première lettre du message est " ". Il s'agit de la première lettre de l'alphabet. $1+2=3$. " C " est la troisième lettre de l'alphabet. " A " est donc remplacé par " C ".

La deuxième lettre du message est " L ". Il s'agit de la douzième lettre de l'alphabet. $12+2=14$. " N " est la quatorzième lettre de l'alphabet. " L " est donc remplacé par " N ". Et ainsi de suite... Le message crypté donne à la fin

"CNNGABNGUBDNGWU".

Nous avons crée un programme qui code un message par la méthode de César, qui dès le début demande à l'utilisateur le message à crypter et la clé , qui renvoie un message crypté.

On a commencé à créer une variable "lettres" avec les 26 lettres de l'alphabet puis on a créé une variable "crypted" qui reçoit notre message crypté. Pour chercher chaque caractère du message on a définit une boucle *for*.

Pour décrypter les messages, le code est essentiellement le même, sauf qu'on remplace le message original par le message crypté. Aussi, on soustraie la clé au lieu de l'additionner.

Voici quelques exemples:

- **Message:** *licence maths*
- **Clé:** *3*
- **Message crypté:** *olfhqfh pdwkv*

- **Message:** *python*
- **Clé:** *9*
- **Message crypté:** *yhcqxw*

Jules César se disait que personne ne pourrait déchiffrer ses messages mais le problème c'est que sa méthode est simpliste et dans un alphabet de 26 lettres, Jules César n'avait que 26 choix de décalage c'est peu pour crypter donc il est facilement décryptable.

2 Partie 2 : *Le chiffre indéchiffrable de Blaise de Vigenère*

Blaise de Vigenere (1523-1596), diplomate francais.

À la fin du Moyen-Âge, en France, *le diplomate français Blaise de Vigenère* (qui avait de toute évidence un intérêt pour les mathématiques) met au point un algorithme que personne ne réussira à briser pendant plus de **250 ans!**

De Vigenère a présenté sa méthode devant la cour d'Henri III en 1586. L'algorithme se révèle particulièrement coriace pour les scientifiques et savants de l'époque qui tentent de le déchiffrer, ce qui lui vaudra le surnom de ***chiffre indéchiffrable***.

La méthode de Vigenère consistait à choisir une clé et à s'en servir pour crypter le message lui-même. Par exemple, imaginons la situation suivante:

- **Message:** *Le chiffre indéchiffrable*
- **Clé:** *python*

Voici comment nous nous y prendrions pour crypter notre message dans Excel. Les deux premières lignes représentent notre alphabet avec le chiffre correspondant à chaque lettre (en Python, on commence toujours nos listes par 0).

Nous avons ensuite la ligne de notre message, avec le numéro de chaque lettre, puis notre clé, qui se répète pour couvrir tout le message, et avec encore

une fois le chiffre correspondant à chaque lettre.

Pour crypter notre message, il suffit de faire la somme des chiffres correspondant à la lettre en clair et à la lettre de notre clé. Par exemple, la première lettre du message est " L ", qui est associé à 11. La lettre correspondante pour notre clé est " P ", qui est le numéro " 15 ". $11 + 15 = 26$. Nous n'avons pas de lettre 26, donc nous retournons au début, ce qui nous donne la lettre " A "!

	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
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

MESSAGE	L	E		C	H	I	F	F	R	E		I	N	D	E	C	H	I	F	F	R	A	B	L	E
	11	4		2	7	8	5	5	17	4		8	13	3	4	2	7	8	5	5	17	0	1	11	4
CLÉ	P	Y		T	H	O	N	P	Y	T		H	O	N	P	Y	T	H	O	N	P	Y	T	H	O
	15	24		19	7	14	13	15	24	19		7	14	13	15	24	19	7	14	13	15	24	19	7	14
CRYPTÉ	A	C		V	O	W	S	U	P	X		P	B	Q	T	A	A	P	T	S	G	Y	U	S	S
	26	28		21	14	22	18	20	41	23		15	27	16	19	26	0	15	19	18	32	24	20	18	18
-26	0	2							15				1			0					6				

La grande force de cette technique réside dans le fait qu'une lettre peut servir à en crypter plusieurs autres. Par exemple, le " Y " de notre clé " PYTHON " sert à crypter " E ", " R ", " C " et " A ". À l'inverse, les lettres cryptées peuvent aussi renvoyer à plusieurs lettres en clair. Dans le message crypté, " A " renvoie tant " L " qu'à " C " et " H ".

De plus, avec six lettres, il existe $26^6 = 308915776$ clés possibles! Et si on avait fait un petit effort supplémentaire avec une clé de 10 lettres, on aurait eu le choix entre 141167095653376 combinaisons différentes! Pas étonnant que les mathématiciens se soient cassés les dents pendant près de trois siècles sur cet algorithme. Il y a beaucoup trop de possibilités pour toutes les tester, même avec un ordinateur!

Nous avons crée un programme qui code un message par la méthode de Vigenère, qui dès le début demande à l'utilisateur le message à crypter et la clé , qui renvoie un message crypté.

Nous avons testé notre programme avec quelques exemples:

- **Message:** *Bonjour*
- **Clé:** *hello*
- **Message crypté:** *ISYUCBV*

- **Message:** *no pain no gain*

- **Clé:** *motivate*
- **Message crypté:** *ZC IIDN GS SOBV*

- **Message:** *sans effort il n'y a pas de résultat*
- **Clé:** *qui ne tente rien n'a rien*
- **Message crypté:** *IUVR RJEHVG BP M'P I TNR QD RÉRLTXNJ*

Enfin pour décrypté il sufffit de inverser le processus. Nous avons également crée un programme qui décrypte un message.