Arithmétique TI-Nspire	Cryptographie, chiffrement affine

Vocabulaire

Cryptographie (du grec *kruptos*, caché et *graphein*, écrire) : technique consistant à transformer un message (par un procédé mathématique, par exemple) en un message codé, de telle sorte qu'un lecteur indésirable n'en comprenne pas le sens et que le destinataire soit capable de le traduire.

Clés : procédés (mathématiques, par exemple) permettant de crypter un message (*clé de chiffrement*) ou de le retranscrire en clair (*clé de déchiffrement*).

Cryptanalyse : activité ayant pour but de décoder un message codé, sans en connaître la clé.

L'usage fait que l'on emploie indifféremment les mots de codage ou de chiffrement ; mais, contrairement au premier, le second manifeste la volonté explicite de cacher le message aux yeux indiscrets par un procédé cryptographique.

Objectifs

La charmante Alice souhaite envoyer le message suivant à Bob – une phrase de Cantor – en utilisant un chiffrement affine :

L'essence des mathématiques, c'est la liberté.

Dans un souci de simplification, Alice a choisi de ne se préoccuper ni des accents ou apostrophes, ni des majuscules, ni des espaces.

Première étape : codage des lettres par leur rang dans l'alphabet

En utilisant leur rang dans l'alphabet, on peut naturellement associer à chaque lettre un nombre entier, selon le tableau suivant :

a	b	c	d	e	f	g	h	i	j	k	l	m
00	01	02	03	04	05	06	07	08	09	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

1) Coder à la main chacune des huit premières lettres du message d'Alice.

2) On souhaite automatiser ce procédé à l'aide du logiciel ou de la calculatrice TI-Nspire, en s'appuyant sur les instructions **ord**, qui donne le code d'un caractère alphanumérique et **char**, qui donne le caractère correspondant à un code donné, comme le montre l'écran suivant.

ord("a")	97
ord("b")	98
ord("z")	122
char(97)	"a"
char(98)	"b"
char(122)	"z"

On se propose d'abord d'utiliser le tableur pour coder chacune des lettres du message d'Alice :

	A clair	B	C	D	E	F	G	H	I	J
◆										
1	l	11								
2	e	4								
3	s	18								
4	s	18								
5	e	4								
6	n	13								

a) Quelle instruction doit-on saisir en B1 pour coder la lettre "l" par l'entier 11, comme on le voit sur la figure ci-dessus ?
Recopier vers le bas cette instruction jusqu'à la dernière lettre du message.

b) Remarquons que l'on peut raisonner directement sur la liste en saisissant dans la zone grisée de la colonne B : **ord(clair)–97** ou **ord(A[])–97**. Tester cette possibilité.

Deuxième étape : le chiffrement affine en action

Ce que nous venons de faire n'est qu'un banal codage, où chaque lettre a été transformée en chiffre en suivant l'ordre alphabétique. Si le message était intercepté, l'infâme Charles parviendrait sans peine à en rétablir le sens.

Nous allons procéder maintenant au chiffrement *affine* proprement dit, pour masquer le sens du message.

> a et b sont deux entiers naturels, appelés les clés du chiffrement et conservées secrètement par l'émetteur du message, Alice, et par celui qui le reçoit, Bob.
>
> La lettre X est supposée avoir le rang x déterminé selon la méthode précédente.
>
> On calcule alors $y = \text{mod}(ax+b,26)$, c'est-à-dire le reste dans la division de $ax + b$ par 26.
>
> On associe à ce nombre y compris entre 0 et 25 la lettre Y qui lui correspond.

Nous supposerons dans la suite que $a = 3$ et $b = 7$. On peut placer ces valeurs dans les cellules H1 et H2 et les mémoriser dans les variables **a** et **b**.

1) Indiquer par un calcul à la main comment seront codées les deux premières lettres "l" et "e" du message d'Alice.

2) a) Coder l'ensemble du message d'Alice dans la feuille de calcul précédemment ouverte. On obtient ainsi le message envoyé à Bob.

b) Plutôt que de travailler cellule par cellule comme on vient de le faire, on aurait pu remplir en une seule instruction (saisie dans la zone grisée) l'intégralité de la colonne C : **=mod('a*b[]+'b,26)**. Le calcul s'effectue alors sur la liste **a*b[]+b** , donc sur chacun de ses termes. Cette méthode nous dispense de la recopie vers le bas.
Si l'on veut procéder de la même façon pour obtenir la colonne D, que doit-on saisir dans le zone grisée de cette colonne ?

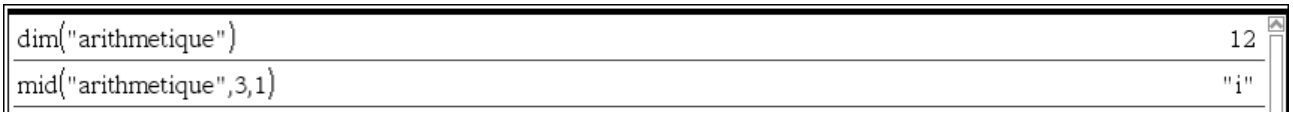
3) Coder, sur cette feuille de calcul, en chiffrement César (voir ci-dessous la description par Suétone de cette méthode utilisée par Jules César), le message : « veni, vidi, vici. »

> *Il y employait, pour les choses tout à fait secrètes, une espèce de chiffre qui en rendait le sens inintelligible (les lettres étant disposées de manière à ne pouvoir jamais former un mot), et qui consistait, je le dis pour ceux qui voudront les déchiffrer, à changer le rang des lettres dans l'alphabet, en écrivant la quatrième pour la première, c'est-à-dire le d pour le a, et ainsi de suite.*
>
> Suétone, Vie des douze Césars, Livre I, paragraphe 56. Source wikipedia

Troisième étape : l'écriture d'une fonction

L'écriture d'une fonction automatise encore un peu plus le travail de chiffrement.

On peut s'appuyer sur les deux instructions **dim** et **mid**, la première donnant le nombre de caractères d'une chaîne, la seconde permettant d'extraire le caractère à une position donnée dans la chaîne, comme le montrent les deux exemples suivants :



Rappelons que l'on concatène des chaînes de caractères comme indiqué ci-après :

On considère la fonction suivante, incomplète, dont le but est de coder un message par chiffrement affine.

1) Expliciter ce que vont contenir les variables **mes**, **a** et **b** en paramètres d'entrée de la fonction.

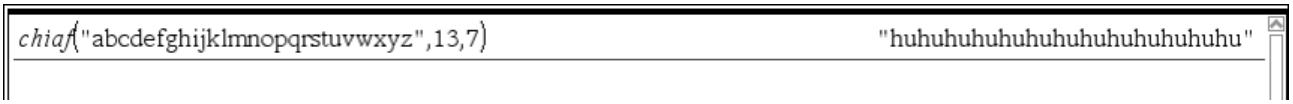
2) À quoi servent les deux instructions en ligne 4, celles qui suivent **Local** ?

3) Décrire ce que l'on se propose de faire à chaque passage dans la boucle **For**.

4) Compléter la fonction pour qu'elle réalise un chiffrement affine du contenu de la variable **mes**. Vérifier que l'on obtient bien le même résultat que dans le tableur.

5) Choix de a et b

a) On se propose de coder l'alphabet "abcd…xyz" à l'aide de la fonction **chiaf**.
En faisant $a = 13$ et $b = 7$, on obtient le résultat suivant :



Expliquer pourquoi un tel chiffrement pose problème.

b) En essayant diverses valeurs de a et de b, donner une condition nécessaire et suffisante pour qu'un chiffrement satisfaisant soit possible.

c) Démontrer cette condition.

d) En déduire combien de chiffrements affines sont possibles.

Quatrième étape : déchiffrement par Bob du message d'Alice

Bob reçoit donc le message chiffré précédent et connaît les clés de chiffrement d'Alice, à savoir $a = 3$ et $b = 7$:

"otjjtuntqtjrhmctrhmfdptjntjmohofktgmt"

1) La première lettre du message "o" se code 14. Il faut cette fois-ci travailler à l'envers et remonter à la lettre non chiffrée, autrement dit résoudre modulo 26 l'équation : $14 \equiv 3x + 7$.
Cette équation équivaut à $3x \equiv 7$.

a) Montrer que l'inverse de 3 modulo 26 est 9.

b) En déduire le déchiffrement de la première lettre du message.

2) Déchiffrer de la même façon la deuxième lettre du message.

3) Écriture d'une fonction dechiaf pour le déchiffrement des messages

L'étude précédente montre que $y \equiv ax + b$ équivaut à dire que $x \equiv k(y - b)$ ou encore $x \equiv ky - kb$, toutes les congruences étant modulo 26 avec *k* qui désigne précisément l'inverse de *a* modulo 26.

À bien regarder la formule, on se rend compte que le déchiffrement équivaut à un chiffrement avec les paramètres *k* et *–kb*, chacun de ces entiers étant pris modulo 26.

Toute la difficulté est donc de déterminer l'entier *k*, inverse de *a* modulo 26, le plus simplement possible.

Comme il n'y a que 25 candidats possibles, nous procéderons, comme plus haut, par un balayage systématique.

a) Tenant compte de ce qui précède, compléter la fonction suivante :

```
* dechiaf                                                    4/6
Define dechiaf(cod,a,b)=
Func
Local k
2→k
While mod(a·k,26)≠1

EndWhile
Return
EndFunc
```

b) Déchiffrer le message suivant, envoyé par Alice à Bob, sachant que *a* = 19 et *b* = 25.

"oxmxtxdpvdoztzvdykvixexefmmxktfmwxtydzpudlvxmlxdyzkazdlvxmlxozvexmfpxaxdrpxarpxdmfxpedefsdlpkddxlkxwdzykxddfvuzmwxefpgxzmmxxdexkxqaxuvfmdzmdofpkexwkxixtfmvjmfkzmlxoxazdzvd"

Quel en est l'auteur ? À quelle époque a-t-il vécu ?

Un dernier rebondissement : l'infâme Charles essaie d'intercepter la correspondance d'Alice et Bob

Voici le message intercepté :

"djcbdfbgdgbxovjbgsktdzhbcbdrtsubrtsjzhbddvgsdjrkcbdxbdsktoxbzhjcdgbdtwbgsktdtzhbckvjgsctwjbbdsxvrkcjzhbb"

Charles ne connaît pas les clés d'Alice mais sait qu'elle utilise le chiffrement affine.

1) La force brute

a) Que fait cette fonction ?

```
"forcebrute" enregistrement effectué
Define forcebrute(cod)=
Func
Local a,b
For a,1,25
  If gcd(a,26)=1 Then
    For b,0,25
      Disp chiaf(cod,a,b)
    EndFor
  EndIf
EndFor
Return "fin de la force brute"
EndFunc
```

b) Peut-on penser qu'elle donne une réponse rapide au déchiffrement du message d'Alice ?

c) La tester.

2) L'intelligence en action ?

```
"frequencelettres" enregistrement effectué
Define frequencelettres(cod)=
Func
Local l,i,lettre
newList(26)→l
For i,1,dim(cod)
  mid(cod,i,1)→lettre
  l[ord(lettre)-96]+1→l[ord(lettre)-96]
EndFor
Return l
EndFunc
```

La fonction qui précède donne la fréquence des différentes lettres apparaissant dans le message chiffré.
On obtient dans le tableur les résultats suivants :

	A	B	C	D	E	F	G	H	I
◆		=frequencelettres(cod)							
1	a	0							
2	b	18							
3	c	7							
4	d	14							
5	e	0							
6	f	1							
7	g	7							
8	h	5							
9	i	0							
10	j	8							
11	k	6							
12	l	0							
13	m	0							
14	n	0							
15	o	2							
16	p	0							
17	q	0							
18	r	4							

B =frequencelettres(cod)

	A	B	C	D	E	F	G	H	I
◆		=frequencelettres(cod)							
19	s	8							
20	t	8							
21	u	1							
22	v	4							
23	w	2							
24	x	4							
25	y	0							
26	z	5							
27									

Les lettres les plus fréquentes du message sont, dans cet ordre, b (18 occurrences), d (14), j, s et t (8).
En français, ce sont le e, s, a, r, etc.

a) Déduire des occurrences de b et d deux égalités modulo 26.

b) Quelle valeurs de *a* et de *b* en déduit-on ?

c) Ces valeurs permettent-elles de déchiffrer le message ?

Défi : Quel est le célèbre poème suivant, codé par un chiffrement affine ?

"sqgsvyxqjzcalwdywgkqgvyvwsyajyyzjqswcqglsfwgzaveggavcyjsqgnayjjyvwhqaynyjwazzqghqglswxlysvwxyajynayjj
yvwjgazsqjjyvtyglyvyshqglssyjnqjzhyrycyglyvyscwajsrwjsvyscwajslyszqjsfwkywfwkyzwjrasegysqgsvyxqjzryjqsdlwsx
wssyrysyzyljyvslymwlrsvqjrysavwssynayjjyvwjgazsqjjyvtyglyvyshqglssyjnqjzhyrycyglyvwcqglsyjnwkqccykyzzyywgk
qglwjzyvwcqglsyjnwkqccyvwnayyszvyjzyyzkqccyvysxylwjkyysznaqvyjzynayjjyvwjgazsqjjyvtyglyvyshqglssyjnqjzhyr
ycyglyxwssyjzvyshqglsyzxwssyjzvyssycwajysjazycxsxwssyjavyswcqglslynayjjyjzsqgsvyxqjzcalwdywgkqgvyvwsyajyn
ayjjyvwjgazsqjjyvtyglyvyshqglssyjnqjzhyrycygly"