Thème : Avant les congruences

Corrigé de l'activité 2. Chiffrement affine

Voir le fichier tableur pf5372a02.chiffrement_affine.xls ou pf5372a02.chiffrement_affine.ods

Remarque préalable sur le vocabulaire :

Conformément au programme, on définit :

- Le **codage** comme une association simple d'un objet avec un nombre. Par exemple le sexe masculin est codé 1 dans le numéro INSEE, la lettre A est codée 65 sur un ordinateur.
- Le **chiffrement** comme cryptage par un processus plus complexe. Par exemple le chiffrement affine, de Vigenère ou de Hill.

1) **Exemple 1** $a = 3$ et $b = 5$
   a) On fait le tableau des rangs n des 26 lettres de l'alphabet :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Rang n	0	1	2	3	4	5	6	7	8	9	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

- E a pour rang $n = 4$
  $3n + 5 = 17.$
  Le reste de la division de 17 par 26 est $n' = 17$
  Donc E est chiffré par R.
- U a pour rang $n = 20$
  $3n + 5 = 65.$
  Le reste de la division de 65 par 26 est $n' = 13$
  Donc U est chiffré par N.
- C a pour rang $n = 2$
  $3n + 5 = 11.$
  Le reste de la division de 11 par 26 est $n' = 11$
  Donc C est chiffré par L.
- L a pour rang $n = 11$
  $3n + 5 = 38.$
  Le reste de la division de 38 par 26 est $n' = 12$
  Donc L est chiffré par M.
- I a pour rang $n = 8$
  $3n + 5 = 29.$
  Le reste de la division de 29 par 26 est $n' = 3$
  Donc I est chiffré par D.
- D a pour rang $n = 3$
  $3n + 5 = 14.$
  Le reste de la division de 14 par 26 est $n' = 14$
  Donc D est chiffré par O.

Donc **EUCLIDE** est chiffré en **RNLMDOR**

b) On remplit le tableau en utilisant la calculatrice :

Clé	$a=$	3		$b=$	5							
Lettre en clair	A	B	C	D	E	F	G	H	I	J	K	L
Rang n	0	1	2	3	4	5	6	7	8	9	10	11
$an+b$	5	8	11	14	17	20	23	26	29	32	35	38
Rang n'	5	8	11	14	17	20	23	0	3	6	9	12
Lettre chiffrée	F	I	L	O	R	U	X	A	D	G	J	M

Par lecture du tableau depuis la ligne « lettre chiffrée », on déchiffre :

- U est déchiffré en F
- F est déchiffré en A
- L est déchiffré en C
- D est déchiffré en I
- M est déchiffré en L
- R est déchiffré en E

On réalise avec un tableur le tableau proposé dans l'énoncé.

- On peut fixer la largeur des colonnes assez petite (largeur 2 ou 3) pour les colonnes B à AM.
- On saisit les lignes 1 et 2 et la colonne A avec les valeurs présentes dans le tableau de l'énoncé.
- Dans la cellule B3, on entre la formule =CODE(B2)-65 puis on recopie B3 automatiquement, à l'aide de la poignée de recopie située en bas à droite de la cellule B3, jusqu'en AA3.
- Dans la cellule B4, on entre la formule =$C1*B3+$F1 puis on recopie B4 automatiquement jusqu'en AA4. Le symbole $ placé devant les lettres de colonnes C et F permet de fixer ces références de colonnes afin qu'elles restent inchangées dans la recopie automatique.
- Dans la cellule B5 on entre la formule =MOD(B4;26) puis on recopie B5 automatiquement jusqu'en AA5.
- Dans la cellule B6, on entre la formule =CAR(B5+65) puis on recopie B6 automatiquement jusqu'en AA6.

2) Exemple 2

- R a pour rang $n=17$
  $13n+4=225$.
  Le reste de la division de 225 par 26 est $n'=17$
  Donc R est chiffré par R.
- A a pour rang $n=0$
  $13n+4=4$.
  Le reste de la division de 4par 26 est $n'=4$
  Donc A est chiffré par E.
- G a pour rang $n=6$
  $13n+4=82$.
  Le reste de la division de 82 par 26 est $n'=4$
  Donc A est chiffré par E.
- E a pour rang $n=4$
  $13n+4=56$.
  Le reste de la division de 56 par 26 est $n'=4$
  Donc E est chiffré E.

Donc **RAGE** est chiffré en **REEE**.

On constate que des lettres distinctes sont chiffrées en une même lettre.

Ceci provient du fait que :

$13 \times 0 + 4 = 26 \times 0 + 4$, $13 \times 6 + 4 = 26 \times 3 + 4$ et $13 \times 4 + 4 = 26 \times 2 + 4$ ont le même reste dans la division par 26.

Une même lettre chiffrée correspond à des « lettres en clair » différentes. Le déchiffrement est donc impossible. La clé $(a; b) = (13; 4)$ ne peut donc pas être utilisée.

Remarque :
On peut se demander quelle condition nécessaire et suffisante il y a sur la clé $(a; b)$ pour qu'elle soit utilisable.

Soit n_1 et n_2 les rangs de deux lettres en clair. Soit n'_1 et n'_2 les rangs des lettres chiffrées correspondantes.

On a $n'_1 \equiv an_1 + b \quad (26)$ avec $0 \leq n'_1 \leq 25$ et $0 \leq n'_2 \leq 25$

- A quelle condition sur $(a; b)$ a-t-on $n'_1 = n'_2 \implies n_1 = n_2$?

$$n'_1 = n'_2 \iff an_1 + b \equiv an_2 + b \quad (26)$$

$$n'_1 = n'_2 \iff a(n_1 - n_2) \equiv 0 \quad (26)$$

D'après le théorème de Gauss, $\begin{cases} a(n_1 - n_2) \equiv 0 \quad (26) \\ 26 \text{ est premier avec } a \end{cases} \implies (n_1 - n_2) \equiv 0 \quad (26)$

Autrement dit, puisque $-25 \leq n_1 - n_2 \leq 25$,

$$\begin{cases} a(n_1 - n_2) \equiv 0 \quad (26) \\ 26 \text{ est premier avec } a \end{cases} \implies (n_1 - n_2) = 0$$

On voit qu'une condition suffisante sur la clé est que a soit premier avec 26.

- Est-elle nécessaire ?

Si a n'est pas premier avec 26 alors a est divisible par 2 ou 13. Dans ce cas, le produit $a(n_1 - n_2)$ peut-être un multiple de 26 tout en ayant $n_1 - n_2$ non nul. C'est le cas lorsque $n_1 - n_2$ est un multiple de 2 ou de 13.

Donc elle est nécessaire.

<u>Conclusion :</u> Pour que, quels que soient les rangs n_1 et n_2, $n'_1 = n'_2 \implies n_1 = n_2$ il faut et il suffit que a soit premier avec 26.

3) Exemple 3

Comme le suggère l'énoncé, ce chiffrement peut être cassé par une analyse fréquentielle.

On relève donc l'effectif de chaque lettre présente et l'effectif total.

On calcule les fréquences.

Pour plus de facilité, on trie la liste par ordre décroissant de fréquences.

Lettre	Effectif	Fréquence
V	27	0,171
Z	16	0,101
F	15	0,095
S	13	0,082
L	10	0,063
Q	10	0,063
I	10	0,063
H	8	0,051

A	8	0,051
N	7	0,044
J	6	0,038
B	5	0,032
Y	5	0,032
K	5	0,032
E	3	0,019
O	2	0,013
U	2	0,013

M	2	0,013
D	2	0,013
R	1	0,006
X	1	0,006
TOTAL	**158**	**1**

- Le V a une fréquence nettement plus élevée. On suppose donc qu'il chiffre le E.
- Le Z a la deuxième fréquence la plus élevée. Donc il chiffre probablement le A ou le S. Si c'est le A alors le cinquième mot comporte deux A à suivre ce qui est très improbable. On suppose donc que Z chiffre le S.
- Le F a la troisième fréquence la plus élevée. On suppose donc qu'il chiffre le A.
- Le quatrième mot est très probablement ASSEZ, ce qui montre que O chiffre le Z.

Et ainsi de suite, on procède en s'aidant des fréquences et en regardant la vraisemblance des conjectures.

Après quelques minutes, on obtient le texte en clair :

MAINTENANT VOUS EN SAVEZ ASSEZ POUR VOUS CONVAINCRE QUE LES CHIFFRES DE CETTE NATURE SONT AISES A DEVINER MAIS ASSUREMENT CE SPECIMEN APPARTIENT AU GENRE LE PLUS SIMPLE DE LA CRYPTOGRAPHIE