Problèmes de chiffrement

Chiffrement affine

On numérote les 26 lettres de l'alphabet de 0 pour la lettre A à 25 pour la lettre Z.
On calcule les images de ces 26 entiers par une fonction affixe $f : x \mapsto ax + b$ où a et b sont deux entiers naturels avec $a \neq 0$.
On prend les restes de ces images dans la division euclidienne par 26.
On remplace les lettres composant le message initial par celles qui correspondent à ces restes.

Le couple $(a\,;\,b)$ est la clé secrète du codage. Quand $a = 1$, il ne s'agit que d'un simple décalage, comme celui qu'utilisait César qui décalait chaque lettre de trois rangs.

Exercice n°1

A2 fx Σ = =MOD(11*A1+8;26)

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

1. A quel chiffrement affine correspond la feuille de calcul ci-dessus ?
2. Coder le message « LES MATHS DE JEAN KEVIN ».
3. Reproduire la feuille de calcul ci-dessous et modifier la formule en A2 pour observer les chiffrements obtenus avec les clés $(2\,;\,5)$, $(4\,;\,6)$ et $(13\,;\,3)$.
   Pourquoi ces clés ne sont-elles pas satisfaisantes ?
4. Montrer que si a et 26 sont premiers entre eux, alors la clé $(a\,;\,b)$ est satisfaisante.
5. On considère une clé $(a\,;\,b)$ satisfaisante.
   Montrer qu'il existe un entier relatif u tel que $au \equiv 1\ (26)$.
6. Montrer que si $y \equiv ax + b\ (26)$ alors $x \equiv uy - bu\ (26)$.
   En déduire une fonction affixe permettant de lire un message codé.

Chiffrement de Vigenère

Au XV$^{\text{ème}}$ siècle, le savant italien Léon Battista Alberti eut l'idée d'utiliser deux alphabets comme système de chiffrement, sorte d'amélioration du chiffrement affine. Ses idées furent approfondies par l'abbé allemand Jean Trithème et la forme finale de cette méthode de chiffrement a été attribuée au diplomate français Blaise de Vigenère.

La méthode est la suivante.
On utilise un mot-clé à la place de la formule affine pour déterminer le décalage. Par exemple, on souhaite coder le mot « mathématiques » en choisissant comme mot-clé « zero ».

Chiffrement de Vigenère : suite et fin

- On code la lettre M dans la ligne commençant par Z ce qui donne le L.
- On code la lettre A dans la ligne commençant par E ce qui donne le E.
- On code la lettre T dans la ligne commençant par R ce qui donne le K.

et ainsi de suite. On s'aide pour cela du carré ci-dessous.

Si x est le rang de la lettre initiale et y le rang de la lettre codée, on obtient : $y \equiv x + c$ (26).
Ainsi, le codage d'une lettre dépend de sa place dans le message et la méthode résiste davantage aux méthodes d'analyse des fréquences d'apparition des lettres.

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
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	A
C	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
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
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	D
...																									
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	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

Exercice n°2

1. Coder le mot JEAN KEVIN avec la clé BATMAN.
2. Déterminer une formule permettant de déchiffrer un message en connaissant c.

> Correction des exercices

Exercice n°1

1. On a utilisé le chiffrement à l'aide de la clé $(11\,;\,8)$.
2. Le message devient ZAY KIJHY PA DAIV OAFSV.
3. Plusieurs lettres différentes sont codées par la même lettre. Ces clés ne sont donc pas satisfaisantes.
4. Il suffit d'utiliser le théorème de Gauss.
5. Puisque $y \equiv ax + b\ (26)$ alors $ax \equiv y - b\ (26)$.
   Puisque a est premier avec 26 alors d'après le théorème de Bezout, il existe un entier u tel que $au \equiv 1\ (26)$.
6. $ax \equiv y - b\ (26) \Leftrightarrow aux \equiv u(y - b)\ (26) \Leftrightarrow x \equiv uy - ub\ (26)$.
7. En notant a^{-1} l'inverse de a modulo 26, la fonction affine recherchée est $x = a^{-1}y - a^{-1}b$

Exercice n°2

1.

Message à coder	J	E	A	N	K	E	V	I	N
Clé	B	A	T	M	A	N	B	A	T
Message codé	K	E	T	Z	K	R	W	I	B

2. La formule est $x \equiv y - c\ (26)$.