Chiffrements

1 Affine

Le chiffrement affine est une méthode de cryptographie basée sur un chiffrement par substitution mono-alphabétique, c'est-à-dire que la lettre d'origine est remplacée que par une unique autre lettre. Le chiffrement affine consiste à associer à tout nombre entier x compris entre 0 et 25 (correspondant à une lettre) un unique nombre entier y compris entre 0 et 25 par le procédé suivant :

$$x \longmapsto y \equiv ax + b\,(26)$$

a et b sont appelés les clefs de notre chiffrement.

L	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
x	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
y																										
L																										
x																										
L																										

1. Dans cette exemple, on prend $a = 21$ et $b = 7$.
   a. Compléter les deux premières lignes du tableau ci-dessus.
   b. En déduire le chiffrement du message suivant : « JADORELASPE ».
2. Imaginons que l'on reçoive le message crypté suivant : « GTGNENVZHQYV ». On va chercher deux réels a' et b' qui permettent de décrypter le message, c'est à dire tels que :

$$y \longmapsto x \equiv a'y + b'\,(26)$$

   a. Démontrer que $aa' \equiv 1\,(26)$. Que peut-on dire de a, a' et 26 ? En déduire l'entier a' cherché.
   b. Démontrer que $a'b + b' \equiv 0\,(26)$. En déduire l'entier b' cherché.
   c. Compléter les deux dernières lignes du tableau ci-dessus puis décrypté le message « GTGNENVZHQYV ».
3. Déterminer tous les couples $(a; a')$ possibles.
4. Compléter le feuille de tableur 1415_TS_spe_affine.ods
5. Que se passe t'il si a n'est pas premier avec 26 ?

2 Vignère

Le chiffrement de Vignère est une méthode de cryptographie basée sur un chiffrement par substitution poly-alphabétique, c'est-à-dire que la lettre d'origine peut être remplacée selon sa position dans le message par plusieurs autres lettres. Ce chiffrement introduit la notion de clé. Une clé se présente généralement sous la forme d'un mot ou d'une phrase. Pour pouvoir chiffrer notre texte, à chaque caractère nous utilisons une lettre de la clé pour effectuer la substitution. Évidemment, plus la clé sera longue et variée et mieux le texte sera chiffré.

1. Crypter le message « VIVELASPEMATHS » avec la clé « BAC ».

L	V	I	V	E	L	A	S	P	E	M	A	T	H	S
x														
Clé														
y														
L														

2. Compléter le feuille de tableur 1415_TS_spe_vignere.ods.
3. Décrypter le message « AAJSXXTTEMSIEPMF » avec la clé « SPE ».