Le chiffre affine.xlsm

Cryptographie

Le chiffre Affine.xls

Chiffrement affine et calcul modulo 26

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
Rang	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

Ce chiffrement se fonde sur les bijections affines

$$f : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}, \quad x \mapsto ax + b$$

f est bijective <==> pgcd(a ; 26) = 1 (a inversible modulo 26)

$$f^{-1} : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}, \quad x \mapsto u(x - b)$$

on inverse a en résolvant Bezout :
au + 26v = 1
u est l'inverse de a

a devant être premier avec 26, a doit être impair et différent de 13.
les couples (a ; b) sont les clefs de chiffrement. ----- > 12 x 26 = 312 clefs

a	1	3	5	7	9	11	15	17	19	21	23	25
1/a = u	1	9	21	15	3	19	7	23	11	5	17	25

Le chiffre affine.xlsm

Cryptographie

Le chiffre Affine.xls

Chiffrement affine et calcul modulo 26

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
Rang	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

Le chiffre Affine

On Chiffre

CLAIR		S	A	P	E	R	L	I	P	O	P	E	T	T	E
RANG		18	0	15	4	17	11	8	15	14	15	4	19	19	4
Clef	a = 5														
	b= -2														
CHIFFRE 1		10	24	21	18	5	1	12	21	16	21	18	15	15	18
CHIFFRE 2		K	Y	V	S	F	B	M	V	Q	V	S	P	P	S

clef a =	5	
PGCD (a , 26) =	1	
Inverse de a_mod26 =	21	

Inverse Modulo 26 VBA

On déchiffre	a' =	21
Clef Inverse	b' =	16

CHIFFRE	K	Y	V	S	F	B	M	V	Q	V	S	P	P	S
Rang	10	24	21	18	5	1	12	21	16	21	18	15	15	18
CLAIR	18	0	15	4	17	11	8	15	14	15	4	19	19	4
CLAIR	S	A	P	E	R	L	I	P	O	P	E	T	T	E

CHIFFRE	D	M	S	L	Z	S	L	U	S	Y	P	Q	U	K
Rang	3	12	18	11	25	18	11	20	18	24	15	16	20	10
CLAIR	1	8	4	13	21	4	13	20	4	0	19	14	20	18
CLAIR	B	I	E	N	V	E	N	U	E	A	T	O	U	S

Cryptographie

Le chiffre de Hill. Calcul matriciel et Calcul modulo 26

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
Rang	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

on chiffre les lettres par paquets de longueur m, ……

φ est bijective <==> det (M) /\ 26 = 1

$$\varphi : (\mathbb{Z}/26\mathbb{Z})^m \longrightarrow (\mathbb{Z}/26\mathbb{Z})^m \qquad \begin{pmatrix} x_1 \\ . \\ . \\ x_m \end{pmatrix} \longmapsto M \times \begin{pmatrix} x_1 \\ . \\ . \\ x_m \end{pmatrix}$$

en résolvant Bezout : det(M)u + 26v = 1
u est l'inverse de det(M) [u.det(M) = 1 mod26]

$M^{-1} = u \,.\, {}^t\mathrm{com}(M)$

Si m =2 alors
M est une matrice (2x2)

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

alors $$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Le cassage par force brute nécessite de tester toutes les matrices carrées inversibles (mod26)
soit (pour m = 2) : $(2^2 - 1)(2^2 - 1)(13^2 - 1)(13^2 - 13) = 157\,248$ matrices .

Cryptographie

Le chiffre de Hill. Calcul matriciel et Calcul modulo 26

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
Rang	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

Le chiffre de Hill

On Chiffre

CLAIR			S	A	P	E	R	L	I	P	O	P	E	T	T	E	
RANG			18	0	15	4	17	11	8	15	14	15	4	19	19	4	
Clef	11	3															
	7	4															
CHIFFRE 1			16	22	21	17	12	7	3	12	17	2	23	0	13	19	
CHIFFRE 2			Q	W	V	R	M	H	D	M	R	C	X	A	N	T	

Déterm(clef) =	23
PGCD(Déterm , 26) =	1
Inverse_mod =	17

Inverse Modulo 26 VBA

On déchiffre

Clef Inverse	16	1															
	11	5															
CHIFFRE			Q	W	V	R	M	H	D	M	R	C	X	A	N	T	
Rang			16	22	21	17	12	7	3	12	17	2	23	0	13	19	
CLAIR			18	0	15	4	17	11	8	15	14	15	4	19	19	4	
CLAIR			S	A	P	E	R	L	I	P	O	P	E	T	T	E	

CHIFFRE			J	N	F	C	J	H	V	P	S	C	R	H	O	E	
Rang			9	13	5	2	9	7	21	15	18	2	17	7	14	4	
CLAIR			1	8	4	13	21	4	13	20	4	0	19	14	20	18	
CLAIR			B	I	E	N	V	E	N	U	E	A	T	O	U	S	

Cryptographie

L'exercice du Bac. avril 2012 de Pondichéry

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
Rang	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

$$(S_1)\begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases} \quad M = \begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix}$$

det(M) = 23 or 17x23 = 1 (mod 26)

L'inverse de M

$$M^{-1} = 17 \times \begin{pmatrix} 4 & -3 \\ -7 & 11 \end{pmatrix} = \begin{pmatrix} 68 & -51 \\ -119 & 187 \end{pmatrix} = \begin{pmatrix} 16 & 1 \\ 11 & 5 \end{pmatrix} \pmod{26}$$

Codage du mot **ST** :

$$\begin{pmatrix} 18 \\ 19 \end{pmatrix}$$

$$\begin{pmatrix} 11 & 3 \\ 7 & 4 \end{pmatrix} \begin{pmatrix} 255 \\ 202 \end{pmatrix} = \begin{pmatrix} 21 \\ 20 \end{pmatrix} \pmod{26}$$

ST est chiffré par : **VU**

Le chiffre de Hill.xlsm

Le chiffre de Hill.xls

Décodage du mot **YJ**

$$\begin{pmatrix} 24 \\ 9 \end{pmatrix}$$

$$\begin{pmatrix} 16 & 1 \\ 11 & 5 \end{pmatrix} \begin{pmatrix} 393 \\ 309 \end{pmatrix} = \begin{pmatrix} 3 \\ 23 \end{pmatrix} \pmod{26}$$

YJ est en clair : **DX**