2) Chiffrement de VIGENERE :

a) Principe : **Pour le codage :** La méthode repose sur une **clé (constituée d'un ou plusieurs mots)**. On **répète les lettres de cette clé sous le texte à chiffrer** écrit sans accent , ni ponctuation , ni de séparation . Pour chiffrer une lettre du texte , **on la décale (vers la droite) dans l'alphabet d'autant de lettres que le rang (entre 0 et 25) de la lettre correspondante de la clé.**

Pour le décodage : On utilise le même principe mais en décalant vers la gauche

b) Exemple : En utilisant pour clé le mot CODE

1) Chiffrer le message VIGENERE $x + a \equiv y\,(26)$

Texte en clair	V	I	G	E	N	E	R	E
Rang x	21	8	6	4	13	4	17	4
clé	C	O	D	E	C	O	D	E
Décalage a	2	14	3	4	2	14	3	4
Rang y de la lettre décodée	23	22	9	8	15	18	20	8
Texte chiffré	X	W	J	I	P	S	U	I

2) Déchiffrer : LSVYKGHRVSUQKBDPG $y - a \equiv x\,(26)$

Texte chiffré	L	S	V	Y	K	G	H	R	V	S	U	Q	K	B	D	P	G
Rang y	11	18	21	24	10	6	7	17	21	18	20	16	10	1	3	15	6
Clé	C	O	D	E	C	O	D	E	C	O	D	E	C	O	D	E	C
Décalage : a	2	14	3	4	2	14	3	4	2	14	3	4	2	14	3	4	2
Rang x	9	4	18	20	8	$-8 \equiv 18\,(26)$	4	13	19	4	17	12	8	$-13 \equiv 13\,(26)$	0	11	4
Texte en clair	J	E	S	U	I	S	E	N	T	E	R	M	I	N	A	L	E

SE SUIS EN TERMINALE

II -] Chiffrement affine :

1) Principe de codage :

Chaque lettre de l'alphabet est remplacée par son rang x entre 0 et 25 (les autres signes : espace, trait d'union ,...etc sont supprimés)

Le rang de la lettre chiffrée est alors le reste y de la division euclidienne de la transformation affine : ax + b par 26 d'où on a :

$$ax + b \equiv y\,(26) \quad \text{avec } 0 \leqslant y \leqslant 25$$

Le couple d'entiers (a , b) s'appelle la clé de codage .

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

$y \equiv f(x)$ où $f(x) \equiv ax + b$ est la fonction de codage

2) Exemples :

a) Si la clé est le couple $(3, 11) = (a, b)$

Déterminer le codage de la lettre T : a= 3 et b = 11

Lettre à coder	Rang x de la lettre à coder	$ax + b = 3x + 11 = f(x) \equiv y\,(26)$	$y \equiv f(x)\,(26)$	Lettre codée correspondant au rang y
T	19	$3 \times 19 + 11 = 68 = 2 \times 26 + 16 \equiv 16\,(26)$	16	Q

Donc T est codée par ....Q.....

b) Coder le mot SOLUTION avec la clé (15 , 16) a = 15 b = 16

Lettre à coder	Rang x	$ax + b = 15x + 16 = f(x)$	$y \equiv f(x)\,(26)$	lettre codée
S	18	$286 \equiv 0\,(26)$	0	A
O	14	$226 \equiv 18\,(26)$	18	S
L	11	$181 \equiv 25\,(26)$	25	Z
U	20	$316 \equiv 4\,(26)$	4	E
T	19	$301 \equiv 15\,(26)$	15	P
I	8	$136 \equiv 6\,(26)$	6	G
O	14	$226 \equiv 18\,(26)$	18	S
N	13	$211 \equiv 3\,(26)$	3	D

2) A quelles conditions un codage affine est-il exploitable :

On considère qu'un cryptage est exploitable (et donc décryptable) si 2 lettres distinctes sont codées par 2 lettres distinctes. JP me faut pas que l'on ait la même valeur de $y \equiv ax+b(26)$ pour 2 valeurs de x différentes

On considère la transformation affine $x \longmapsto ax + b$ avec a et b entiers naturels, et à chaque rang x, on lui associe le reste y dans la division euclidienne par 26. soit $f(x) = ax + b$ fonction affine

a) Si a = 13 : Montrer qu'il existe 2 lettres qui seront codées de la même façon et donc que le codage n'est pas exploitable. Existe-t-il le même y pour 2 valeurs de x différentes ?

$f : x \longmapsto 13x + b$ $f(x) : 13x + b \equiv y\ (26)$ avec $0 \leqslant b \leqslant 25$ et $0 \leqslant y \leqslant 25$

Si x = 0 alors $13x + b = b$ $\equiv b\ (26)$ donc $y = b$.

Si x = 2 alors $13x + b = 26 + b$ $\equiv b\ (26)$ donc $y = b$

Donc A et C seront codées par la même lettre de rang $y = b$

donc le codage n'est pas exploitable

b) Si a et 26 sont premiers entre eux :

On suppose qu'il existe 2 entiers y et y' tels que $ax + b \equiv y\ (26)$ avec $0 \leqslant y \leqslant 25$

$ax' + b \equiv y'\ (26)$ avec $0 \leqslant y' \leqslant 25$

Montrer que si $y \equiv y'\ (26)$ alors $x \equiv x'\ (26)$. Que peut-on conclure ?

Si $y \equiv y'\ (26)$ alors $ax + b \equiv ax' + b\ (26)$

alors $ax - ax' \equiv 0\ (26)$ donc $a(x - x') \equiv 0\ (26)$

donc 26 divise $a(x - x')$

or 26 et a sont premiers entre eux. donc d'après le th de Gauss

26 divise $x - x'$

donc $x - x' \equiv 0\ (26)$ donc $x \equiv x'\ (26)$

Donc si 2 lettres correspondantes au rang x et x' sont codées par la même lettre correspondante au rang $y = y'$ alors elles sont identiques. Donc le codage est exploitable

En effet par contraposée, si $x \not\equiv x'\ (26)$ alors $y \not\equiv y'\ (26)$

b) Si a et 26 ne sont pas premiers entre eux :

On note $d = PGCD(a, 26)$ avec $0 \leqslant a \leqslant 25$ donc d divise a et 26 donc il existe 2 entiers k et k' tels que :

on sait que $d \neq 1$

$26 = kd$ avec k et k' premiers entre eux.

et $a = k'd$

Montrer que si L est la lettre de rang k alors A et L sont codées par la même lettre et donc que le codage est inexploitable.

PGCD(26, a) = PGCD(kd, k'd) = d | PGCD(k, k')

lettre	Rang x	$ax + b = f(x) \equiv y\ (26)$	y	Lettre codée
L	$x = k$	$dk + b = k'dk + b$ $\equiv k'(kd) + b$ $\equiv k'26 + b \equiv b\ (26)$	$y = b$	Lettre correspondante au rang b
A	$x = 0$	$a \times 0 + b = b \equiv y\ (26)$	$y = b$	Lettre correspondante au rang b

c) Conclusion : L et A sont codées par la même lettre correspondant au rang b

Un codage affine est exploitable ssi a et 26 sont premiers entre eux

donc le codage est inexploitable

3) **Décodage :**

a) Principe :

Avant de décoder un message dont on connait la clé de codage (a, b), il faut déterminer la clé de décodage (a', b')

On sait que $ax + b \equiv y\ (26)$; on connait y et on cherche x

Donc $ax \equiv y - b\ (26)$

Mais les congruences ne sont pas compatibles avec la division. Donc on ne peut pas diviser par a.

Par conséquent **cherchons un entier a' tel que $a'a \equiv 1\ (26)$ avec $0 \leqslant a' \leqslant 25$**

$a'a \equiv 1\ (26)$

d'où $a'a = 1 + 26q$ et $a'a - 26q = 1$ $a(a') + 26(-q) = 1$

donc **(a', -q) est une solution particulière de l'équation diophantienne** $ax + 26y = 1$

Cette équation admet des solutions ssi $PGCD(a, 26) = 1$ d'après le théorème de BEZOUT

ssi a et 26 sont premiers entre eux

Résolution de cette équation diophantienne : $ax + by = 1$

Recherche d'une solution particulière : (x_0, y_0) on a alors $ax_0 + 26y_0 = 1$

D'où le système : $\begin{cases} ax + 26y = 1 \\ ax_0 + 26y_0 = 1 \end{cases}$

Et donc $ax + 26y = ax_0 + 26y_0$

$ax - ax_0 = 26y_0 - 26y$

$a(x - x_0) = 26(y_0 - y)$ et on utilise le th de Gauss voir feuille jointe

Réciproquement : si $x = x_0 + 26k$ et $y = y_0 - ka$ alors $ax + by = 1$

L'ensemble des solutions de cette équation sont les couples $(x_0 + 26k ; y_0 - ka)$

Donc a' est de la forme : $a' = x_0 + 26k$ avec $0 \leqslant a' \leqslant 25$

Cours CRYPTOGRAPHIE

feuille n°3 du cours

3) Décodage d'un chiffrement affine

$f : x \xmapsto{f} ax+b \equiv y\ (26)$ $f(x)=ax+b$ est la fonction affine de codage de clé (a,b)

$g : y \xmapsto{g=f^{-1}} a'y+b' \equiv x\ (26)$ $g(y)=a'y+b'$ est la fonction affine de décodage de clé (a',b')

Pour décoder un message, on veut trouver cette fonction affine g et donc $(a' ; b')$ la clé de décodage tel que $g(y)=a'y+b' \equiv x\ (26)$

on connait f la fonction de codage

$f(x)=\boxed{ax+b \equiv y\ (26)}$ But isoler x dans le 1er membre

(1) $ax \equiv y-b\ (26)$ compatibilité de la congruence avec la soustraction

↳ mais problème : pour isoler x, il faudrait diviser par a, or la division n'est pas compatible avec les congruences

Comme la multiplication, elle, est compatible avec la congruence on va chercher un entier a' (tel qu'en multipliant l'équation (1) par a', c'est-à-dire : $\boxed{a'a}x \equiv a'(y-b)\ (26)$) on ait : $\boxed{a'a \equiv 1\ (26)}$; et ainsi on isole bien x dans le 1er membre : $\boxed{1}x \equiv a'(y-b)(26)$

$\boxed{x \equiv a'(y-b)(26)} \equiv g(y)\ (26)$

avec $\boxed{g(y)=a'y-a'b}$

d'où $a'a \equiv 1\ (26)$ avec $\boxed{a' \leq 25}$

et par définition de la congruence $a'a = 1+26q$

$aa'-26q=1$

$\boxed{a(a')+26(-q)=1}$ donc $(a', -q)$ est une solution de l'équation diophantienne $\boxed{ax+26y=1}$

Comme a et 26 sont premiers entiers, il existe 2 entiers u et v d'après le th de Bezout tels que $au+26v=1$

$a(a')+26(-q)=1$

donc $\boxed{a'=u=x_0}$ et $\boxed{-q=v=y_0}$

* recherche d'une solution particulière (x_0, y_0) de $(E): ax+26y=1$

• d'où le système $\begin{cases} ax+26y=1 \\ ax_0+26y_0=1 \end{cases}$ donc $ax+26y = ax_0+26y_0$

$ax - ax_0 = 26y_0 - 26y$

$\boxed{a(x-x_0) = 26(y_0-y)}$

a divise donc $26(y_0-y)$

or a et 26 premiers entre eux donc d'après le Th de Gauss a divise y_0-y.

donc il existe un entier k tel que $\boxed{y_0-y = ka}$

$\boxed{y = y_0 - ka}$

par substitution on a: $a(x-x_0) = 26(ka)$

$x - x_0 = 26k$

$\boxed{x = x_0 + 26k}$

Réciproquement : $\begin{cases} \text{si } x = x_0+26k \\ \text{et } y = y_0 - ka \end{cases}$ on a: $ax+26y = a(x_0+26k)+26(y_0-ka)$

$= ax_0 + 26ak + 26y_0 - 26ka$

$= \boxed{ax_0+26y_0}$

$= 1$

donc les solutions de $(E): ax+26y=1$ sont tous les couples de la forme $\boxed{(x,y) = (x_0+26k ; y_0-ka)}$

or $(a', -q)$ est une solution de (E) avec $0 \le a' \le 25$

donc $\boxed{a' = x_0+26k \text{ avec } 0 \le a' \le 25}$ et $-q = y_0 - ka$

on cherche l'entier k $0 \le x_0+26k \le 25$

$-x_0 \le 26k \le 25 - x_0$

$\boxed{\frac{-x_0}{26} \le k \le \frac{25-x_0}{26}}$ avec k entier

d'où la valeur de a' en remplaçant la valeur de $\boxed{k = k_0}$ trouvée

et on calcule $\boxed{a' = x_0 + 26k_0}$

puis on trouve : $x \equiv a'y - a'b \ (26)$

$\boxed{x \equiv a'y + b' \ (26)}$ en posant $\boxed{b' \equiv -a'b \ (26)}$

$\boxed{x \equiv g(y) \ (26)}$

où $g(y) = a'y + b'$ fonction de décodage

et la clé de décodage est (a', b')

Et cherchons l'entier k tel que $0 \leqslant x_0 + 26k \leqslant 25$

$-x_0 \leq 26k \leq 25 - x_0$

feuille n°4

avec k entier.

Prenons comme valeur de k l'entier k_0 compris entre $\frac{-x_0}{26}$ et $\frac{25-x_0}{26}$

D'où la valeur de a' = ...

Comme $ax \equiv y - b\ (26)$, on a par multiplication par a' : $a'ax \equiv a'(y-b)\ (26)$

or $a'a \equiv 1\ (26)$

$1x \equiv a'(y-b)\ (26)$

donc $x \equiv a'y - a'b\ (26)$ Posons $b' \equiv -a'b\ (26)$ avec $0 \leqslant b' \leqslant 25$, on obtient :

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

d'où la clé de décodage est le couple d'entiers $(a' ; b')$

b) Exemple : Décoder le message suivant avec comme clé de codage (17 , 0) : a = ... et b = ...

NRTKRXLLREP

lettre en clair	rang x	$a'y + b' \equiv x\ (26)$	rang y	lettre à décoder
				N
				R
				T
				K
				R
				X
				L
				L
				R
				E
				P

c) Comment décoder un message dont ne connait pas la clé de codage :

Soit le message suivant : **YMQMGGKAMMGNNELGMYZMN**

On sait qu'il est codé à l'aide d'une transformation affine . On sait que dans la langue française , **la lettre la plus fréquente est le E suivi de S .**

Donc comme **M apparait 6 fois suivi du G qui apparait 4 fois .** On suppose donc que **M correspond à E** et **G correspond à S** .

On écrit alors une **transformation affine** $x \to ax + b$ qui permet de **passer de E à M** et **de S à G .** Ce qui va permettre de trouver une clé de codage (a , b) , puis une clé de décodage (a' , b') en résolvant un système .

lettre	Rang x	$ax + b \equiv y\ (26)$	y	Lettre codée
E	4	$4a + b \equiv 12\ (26)$	12	M
S	18	$18a + b \equiv 6\ (26$	6	G

Résolution du système avec des congruences : $\begin{cases} 4a + b \equiv 12\ (26) & (2) \\ 18a + b \equiv 6\ (26) & (1) \end{cases}$

④ * Montrer que $14a \equiv 20\ (26)$ puis que $7a \equiv 10\ (13)$

② * Déterminer u_0 et v_0 2 entiers tels que $7u_0 + 13v_0 = 1$, en déduire une solution particulière (x_0, y_0) de l'équation diophantienne $7x + 13y = 10$ puis la résoudre .

③ * En déduire que $a = 7$ ou $a = 20$

④ * Trouver alors la clé de codage (a , b) puis celle de décodage (a' , b') et décrypter le message initial .

b) Exemple (feuille 4 du cours)

Décoder le message avec la clé de codage (17, 0)

donc $a = 17$ $b = 0$

donc $f(x) = ax + b = 17x \equiv y\ (26)$

f fonction affine de codage.

Trouvons la fonction g de décodage

$y(y) = \boxed{a'y + b' \equiv x\ (26)}$ avec (a', b') clé de décodage

on a $17x \equiv y\ (26)$ $\times a'$

$17a'x \equiv a'y\ (26)$

Trouvons a' tel que $17a' \equiv 1\ (26)$ avec $0 \leq a' \leq 25$

par définition de la congruence $17a' = 26q + 1$

$17a' - 26q = 1$

$17a' + 26(-q) = 1$

donc $(a', -q)$ est une solution de l'équation diophantienne

Résolvons l'équation (E) : $17x + 26y = 1$ $\boxed{17x + 26y = 1}$

17 et 26 étant premiers entre eux, d'après le th de Bezout il existe 2 entiers u et v tel que $17u + 26v = 1$.

solution particulière (x_0, y_0) de (E) : $17x + 26y = 1$

en posant $x_0 = u = -3$

$y_0 = v = 2$

on a $17x_0 + 26y_0 = 17 \times (-3) + 26 \times 2$

$= -51 + 52 = 1$

donc $(x_0, y_0) = (-3, 2)$ est une solution particulière de (E)

$\begin{cases} 17x + 26y = 1 \\ 17x_0 + 26y_0 = 1 \end{cases}$

donc $17x + 26y = 17x_0 + 26y_0$

$17x - 17x_0 = 26y_0 - 26y$

$\boxed{17(x - x_0) = 26(y_0 - y)}$

17 divise $26(y_0 - y)$

or 17 et 26 sont premiers entre eux

donc d'après le th de Gauss, 17 divise $y_0 - y$

donc il existe un entier k tel que

$\boxed{y_0 - y = 17k}$

$y = y_0 - 17k$ or $y_0 = 2$

$\boxed{y = 2 - 17k}$

par substitution $17(x - x_0) = 26 \times 17k$

$x - x_0 = 26k$

$x = x_0 + 26k$ or $x_0 = -3$

$\boxed{x = -3 + 26k}$

Réciproquement si $x = -3 + 26k$ et $y = 2 - 17k$ alors $17x + 26y = 17(-3 + 26k) + 26(2 - 17k)$

$= -51 + 17 \times 26k + 52 - 26 \times 17k$

$= 1$

donc les solutions de (E) sont tous les couples de la forme $(x, y) = (-3 + 26k; 2 - 17k)$

or $(a', -q)$ est une solution de E

donc $a' = x = -3 + 26k$ et $-q = 2 - 17k$

Cherchons k de sorte que $0 \leq a' \leq 25$

$0 \leq -3 + 26k \leq 25$

$3 \leq 26k \leq 28$

$\frac{3}{26} \leq k \leq \frac{28}{26}$

$\frac{22}{22}$ $\quad$ $\frac{22}{22}$

$0,11$ $\quad$ $1,07$

l'entier k qui convient est $\boxed{k = 1}$

donc $a' = -3 + 26k = -3 + 26 = \boxed{23}$

donc $\boxed{a' = 23}$ et $17a'x \equiv a'y\ (26)$

$17 \times 23\ x \equiv 23y\ (26)$

or $17a' = 17 \times 23 \equiv 1\ (26)$

$1x \equiv 23y\ (26)$

$x \equiv 23y\ (26)$

donc $\boxed{g(y) = 23y} \equiv x\ (26)$ g fonction de décodage

avec $(a', b') = (23, 0)$ clé de décodage

lettre décodée	x	$g(y) = 23y \equiv x\ (26)$	rang y	lettre à décoder
N	$x = 13$	$23y = 299 \equiv 13\ (26)$	$y = 13$	N
B	$x = 1$	$23y \equiv 1\ (26)$	$y = 17$	R
V	$x = 21$	$23y \equiv 21\ (26)$	$y = 19$	T
W	$x = 22$	$23y \equiv 22\ (26)$	$y = 10$	K
B	$x = 1$	$23y \equiv 1\ (26)$	$y = 17$	R
J	$x = 9$	$23y \equiv 9\ (26)$	$y = 23$	X
T	$x = 19$	$23y \equiv 19\ (26)$	$y = 11$	L
T	$x = 19$	$23y \equiv 19\ (26)$	$y = 11$	L
B	$x = 1$	$23y \equiv 1\ (26)$	$y = 17$	R
O	$x = 14$	$23y \equiv 14\ (26)$	$y = 4$	E
H	$x = 7$	$23y \equiv 7\ (26)$	$y = 15$	P

NRTKRXLLREP est décodé en $\boxed{\text{NBVWBJTTBOH}}$