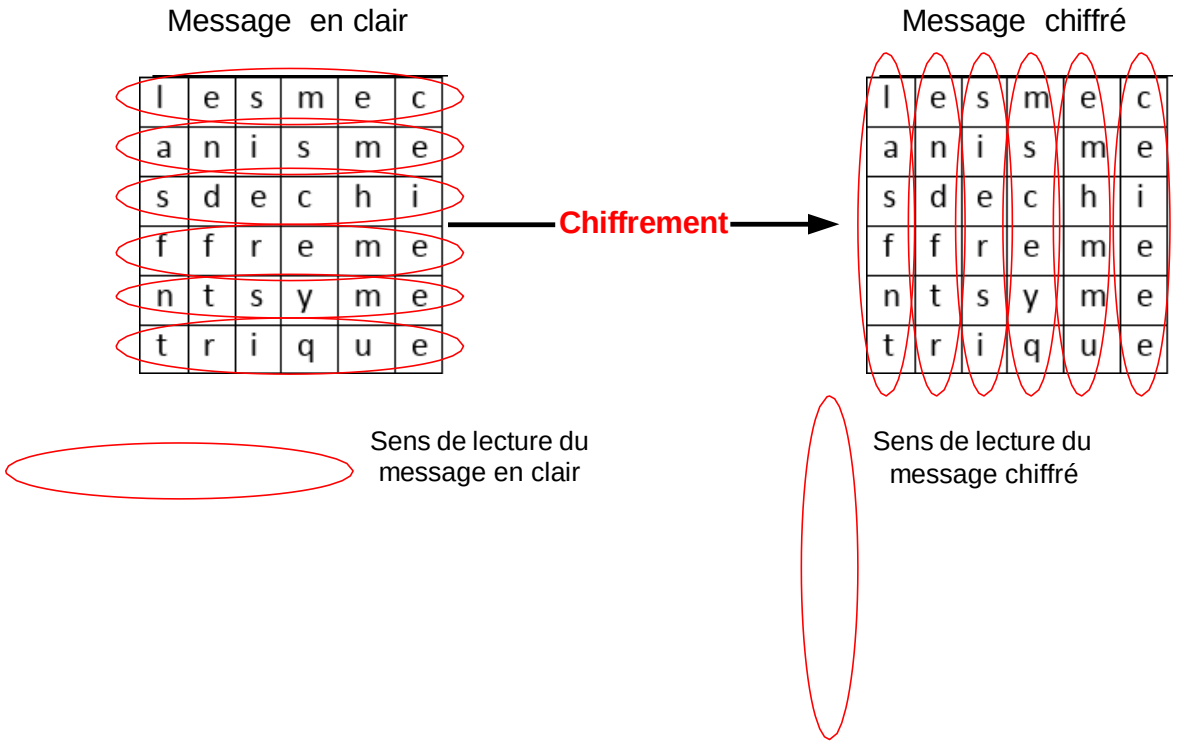
Solution TD4

Exercice 1 :

Le message m : les mécanismes de chiffrement symétrique
Taille du message m =36 caractères
Matrice carrée : nombre de lignes = nombre de colonnes
Taille du message est de 36 caractères ➔ matrice carrée de 6*6

L'écriture du message en clair dans la matrice carrée 6*6 se fait ligne par ligne

l	e	s	m	e	c
a	n	i	s	m	e
s	d	e	c	h	i
f	f	r	e	m	e
n	t	s	y	m	e
t	r	i	q	u	e



La lecture du message chiffré dans la matrice carrée 6*6 se fait colonne par colonne
Le message chiffré est : las fntendftrs ie rsimsceyqem hmmuceieee

Exercice 2 :

Positions des lettres de l'alphabet

Lettre	a	b	c	d	e	f	g	H	i	j	k	l	m
position	0	1	2	3	4	5	6	7	8	9	10	11	12

Lettre	n	o	p	q	r	s	t	u	v	w	x	y	z
position	13	14	15	16	17	18	19	20	21	22	23	24	25

1) m_1 : Le système solaire

La lettre la plus fréquente est e → fréquence = 4 ➔décalage k_1 =4

Le message en clair m : le système solaire

Le chiffrement du message avec le chiffre de César avec le décalage $k_1$consiste à adopter la règle de chiffrement suivante :

Position de lettre chiffrée= (position de la lettre en clair + décalage) mod (26)

→ position de la lettre chiffrée = (position de la lettre en clair +4)mod (26)

Lettre en clair	l	e	s	y	s	t	e	m	e	s	o	l	a	i	r	e
Position (lettre en clair)	11	4	18	24	18	19	4	12	4	18	14	11	0	8	17	4
Chiffrement :(Position+4)mod26																
Position (lettre chiffrée)	15	8	22	2	22	23	8	16	8	22	18	15	4	12	21	8
Lettre chiffrée	p	i	w	c	w	x	i	q	i	w	s	p	e	m	v	i

Donc le message chiffré est : pi wcwxiqi wspemvi

Règle de chiffrement :

Position de lettre chiffrée= (position de la lettre en clair + décalage) mod (26)

Règle de déchiffrement :

Position de lettre en clair= (position de la lettre chiffrée - décalage) mod (26)

Si (position de la lettre chiffrée – décalage) < 0 alors ajoutez 26

➔(position de la lettre chiffrée – décalage)+26

---

2) Soit le message chiffré e_2 : jsvbk jvtwbapun

Taille du message e_2 =14

a) Quel est le diviseur premier impair de la taille du message e_2 ?

Les Diviseurs premiers de 14 sont 2 et 7

7 est le diviseur premier impair ➔K_2=7

b) e_2 étant le résultat de chiffrement d'un message m_2 via le chiffre de césar en utilisant un décalage le décalage k_2=7.

Pour déchiffrer e_2 et restituer le message m_2, il faut adopter la règle de déchiffrement suivante :

Position de lettre en clair= (position de la lettre chiffrée - décalage) mod (26)
Si (position de la lettre chiffrée – décalage) < 0 alors ajoutez 26
➔position de la lettre en clair =(position de la lettre chiffrée – décalage)+26

Lettre en chiffrée	j	s	v	b	k	j	v	t	w	b	a	p	u	n
Position (lettre en chiffrée)	9	18	21	1	10	9	21	19	22	1	0	15	20	13
déchiffrement :(Position-7)mod26														
Position (lettre en clair)	2	11	14	20	3	2	14	12	15	20	19	8	13	6
Lettre en clair	c	l	o	u	d	c	o	m	p	u	t	i	n	g

le message en clair m_2 est cloud computing

Exercice 3 :

1) Soit le message suivant : « Sécurité Informatique ».
a) Le premier mot du message m : sécurité
Taille du mot sécurité =8 ➔ décalage k=8
Alors on applique le chiffre de césar au mot sécurité avec le décalage k=8 pour obtenir la clé de chiffrement du chiffre de Vigenère.
→ position de la lettre chiffrée = (position de la lettre en clair +8)mod (26)

Lettre en clair	s	e	c	u	r	i	t	e
Position (lettre en clair)	18	4	2	20	17	8	19	4
Chiffrement :(Position+8)mod26								
Position (lettre chiffrée)	0	12	10	2	25	16	1	12
Lettre chiffrée	a	m	k	c	z	q	b	m

➔La clé de chiffrement est amkczqbm
b) On applique la méthode de chiffrement de Vigenère en utilisant la table de Vigenère.

clé	a	m	k	c	z	q	b	m	a	m	k	c	z	q	b	m	a	m	k	c
Message en clair	s	e	c	u	r	i	t	e	i	n	F	o	r	m	a	t	i	q	u	e
	s	Q	m	w	q	y	u	q	i	z	p	q	q	c	b	f	i	c	e	g

Le message chiffré est : sqmwqyuq izpqqcbficeg
2) Soit le message en clair m : secoupes volontes
Le message m étant chiffré avec le chiffre de Vigenère en message e
e : wwrowtik konsrlts
Alors, on utilise la table de Vigenère : on selectionne la ligne de la lettre en clair, on cherche dans cette ligne la lettre chiffrée et à partir de cette lettre, on se déplace verticalement vers le haut pour déterminer la lettre de la clé. Dès qu'on remarque la répétition des lettres de la clé, on s'arrête.
➔la clé de chiffrement = **espace**

Exercice 4 :

Pour décrypter ce message chiffré par le chiffrement de César, nous devons essayer toutes les possibilités de décalage jusqu'à ce que nous trouvions le décalage qui donne un message en clair cohérent.
Nous allons essayer chaque décalage possible, de 1 à 25, pour voir si nous obtenons un message cohérent.
Pour un décalage de 1, le message en clair serait :

⇨ ng qqfwng ugewtkvg kphqtocvkswg guv vtgu kpvguigucpv

Ce n'est pas un message cohérent.

Nous pouvons continuer à essayer les autres décalages, mais nous pouvons également utiliser une méthode plus intelligente pour accélérer le processus. Nous pouvons utiliser la fréquence des lettres dans la langue française pour identifier le décalage probable. Par exemple, la lettre la plus fréquente en français est "e", donc si nous trouvons la lettre la plus fréquente dans le message chiffré, nous pouvons supposer qu'elle correspond à la lettre "e" dans le message en clair et utiliser le décalage correspondant pour trouver le message complet.
En utilisant cette méthode, nous pouvons rapidement identifier le décalage probable comme étant **k=3**.

Position de lettre en claire = (position de la lettre chiffrée - décalage) mod26

Lettre chiffrée	O	H	P	R	G	X	V	F	U	L	W	T	D	I	Q
Position lettre chiffrée	15	8	16	18	7	24	22	6	21	12	23	20	4	9	17
Position lettre en claire	12	5	13	15	4	21	19	3	18	9	20	17	1	6	14
Lettre en claire	L	E	M	O	G	U	S	C	R	I	T	Q	A	F	N

Le message en claire : le module sécurité informatique est très intéressant.

Exercice 5 :

1- Déchiffrement de Vigenère par la clé = **secret**

M.Chiffrée	L	E	M	R	F	T	D	E	N	R	L	H	M	Q	K	E	E	P	S	Q	K	E	O	H	M	Q
Clé	S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T	S	E
m. claire	T	A	K	A	B	A	L	A	L	A	H	O	U	M	I	N	A	W	A	M	I	N	K	O	U	M

2- Trouve la clé de chiffrement utilisé

M. Claire	C	R	Y	P	T	O	G	R	A	P	H	I	E	C	L	A	S	S	I	Q	U	E
M. chiffrée	K	E	D	D	K	A	G	K	I	F	B	M	M	P	Q	O	J	E	I	J	E	U
La clé	I	N	F	O	R	M	A	T	I	Q	U	E	I	N	F	O	R	M	A	T	I	Q

- Clé de chiffrement est : **informatique**