Solution TD2

Exercice 1

Le chiffrement de César prend un texte composé de lettres, et décale chaque lettre d'un nombre constant de positions dans l'alphabet. Ce nombre de positions est la clé.

Tableau1. *Code de l'alphabet*

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
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

- **Q1** : Chiffrer le message suivant avec clé =4 : **CHIFFREMENT DE CESAR**

  R1 : le chiffrement de César est un chiffrement symétrique c.-à-d la même clé est utilisée pour chiffrer et déchiffrer des messages M + K = C (M : message en clair , K la clé secrète et C le message chiffré)

  Le message M est composé de lettres M = {m_1, m_2, m_3,…m_n} donc pour chiffrer le message M il faut calculer le chiffre de chaque lettre

  $m_1 + K = c_1 \pmod{26}$, $m_2 + K = c_2 \pmod{26}$ …. $m_n + K = c_n \pmod{26}$

  Le message chiffre C = {c_1, c_2, c_3, … c_n}

Remarque : vous observez que pour les opérations d'addition ci-dessus le résultat est modulo 26, parce qu'en cryptographie on travaille avec des ensembles finis dans notre cas on travaille avec un ensemble de 26 caractères {0,1,2….,25} donc si M+K est supérieur à 25 il suffit juste de soustraire le résultat par 26

Tableau 2. *Chiffrement de César*

Message (M)	C	H	I	F	F	R	E	M	E	N	T	D	E	C	E	S	A	R
Code (M)	2	7	8	5	5	17	4	12	4	13	19	3	4	2	4	18	0	17
Clé (K)	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
$E_k(m_i) = (m_i + k) mod 26$	6	11	12	9	9	21	8	16	8	17	23	7	8	6	8	22	4	21
Message chiffré (C)	G	L	M	J	J	V	I	Q	I	R	X	H	I	G	I	W	E	V

Maintenant pour chiffrer notre message on doit d'abord coder chaque lettre selon le Tableau 1, par la suite on additionne le code de chaque lettre avec la clé secrète afin d'obtenir le code des lettres chiffrer et on termine par convertir le code obtenue avec les lettres qui correspondes selon le Tableau 1. Le Tableau 2 illustre le chiffrement du message M = **CHIFFREMENT DE CESAR** avec la clé K = **4**

Le message chiffre C = **GLMJJVIQIRX HI GIWEV**

- **Q2** : Déchiffrer le message suivant avec clé=5 :
  HJHTIJUJZYJYWJHFXXJ KFHNQJRJSY

  R1 : Le message chiffré C est composé de lettres C = C = {c_1, c_2, c_3, … c_n} donc pour déchiffrer le message C il faut calculer le message en clair pour chaque lettre

  c_1 - K = m_1 (mod 26), c_2 - K = m_2 (mod 26)…. c_n - K = m_n (mod 26)

  Le message en clair M = {m_1, m_2, m_3,…m_n}

Remarque : pareillement pour le déchiffrement le résultat est modulo 26, donc si M-K est inférieur à 0, il suffit juste d'additionner le résultat par 26.

Maintenant pour déchiffrer notre message on doit d'abord trouver le code de chaque lettre selon le Tableau 1, par la suite on soustrait le code de chaque lettre avec la clé secrète afin d'obtenir le code des lettres en clair et on termine par convertir le code obtenue avec les lettres qui correspondes selon le *Tableau 1*. Le *Tableau 3* et Le *Tableau 4* illustrent le déchiffrement du message M = **HJHTIJUJZYJYWJHFXXJ KFHNQJRJSY** avec la clé K = **5.**

Tableau 3. *Déchiffrement de César (1/2)*

Message chiffré (C)	H	J	H	T	I	J	U	J	Z	Y	J	Y	W	J	H
Code (C)	7	9	7	19	8	9	20	9	25	24	9	24	22	9	7
Clé (K)	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
$D_k(m_i) = (m_i - k) mod 26$	2	4	2	14	3	4	15	4	20	19	4	19	17	4	2
Message (M)	C	E	C	O	D	E	P	E	U	T	E	T	R	E	C

Tableau 4. *Déchiffrement de César (2/2)*

Message chiffré (C)	F	X	X	J	K	F	H	N	Q	J	R	J	S	Y
Code (C)	5	23	23	9	10	5	7	13	16	9	17	9	18	24
Clé (K)	5	5	5	5	5	5	5	5	5	5	5	5	5	5
$D_k(m_i) = (m_i - k) mod 26$	0	18	18	4	5	0	2	8	11	4	12	4	13	19
Message (M)	A	S	S	E	F	A	C	I	L	E	M	E	N	T

Le message en clair M = **CE CODE PEUT ETRE CASSER FACILEMENT**

- **Q3** : Montrer qu'il est très aisé de déchiffrer le message suivant sans connaitre la clé :
  ZSGAS HWSFG RWBHS FBSH

R3 : Le crypto-système de César est très simple à casser (cryptanalyser). Une méthode primaire est d'essayer les 26 combinaisons possibles (attaque par force brute) et voir si

l'on peut obtenir un message compréhensible. Une méthode plus évoluée consiste à calculer les fréquences d'apparition des lettres dans le message codé (ce qui est beaucoup plus facile lorsque le message est long).

Selon la langue, certaines lettres reviennent plus couramment que d'autres (en français, par exemple, la lettre la plus utilisée est la lettre E), ainsi la lettre apparaissant le plus souvent dans un texte chiffré par la méthode de César correspondra probablement à la lettre E, une simple soustraction donne alors la clé de cryptage.
Dans notre message chiffré le nombre d'apparition de chaque lettre est comme suit :
Z→ 1 S→ **5** G→2 A→1 H→ 3 W→2 B→2 F→2
Comme vous pouvez remarquer la lettre qui revient le plus et le **S**, par conséquent, on suppose que la lettre **S** représente la lettre **E.**

M + K = C → E + K = S → 4 + K = 18 → K = 18 - 4 → K = 14

Le *Tableau 5* illustre le décryptage du Message **ZSGAS HWSFG RWBHS FBSH** en utilisant la clé **K = 14**

Tableau 5. *Décryptage de César*

Message chiffré (C)	**Z**	**S**	**G**	**A**	**S**	**H**	**W**	**S**	**F**	**G**	**R**	**W**	**B**	**H**	**S**	**F**	**B**	**S**	**H**
Code (C)	25	18	6	0	18	7	22	18	5	6	17	22	1	7	18	5	1	18	7
Clé (K)	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14
$D_k(m_i) = (m_i - k) mod 26$	11	4	18	12	4	19	8	4	17	18	3	8	13	19	4	17	13	4	19
Message (M)	**L**	**E**	**S**	**M**	**E**	**T**	**I**	**E**	**R**	**S**	**D**	**I**	**N**	**T**	**E**	**R**	**N**	**E**	**T**

Le message en clair M = **LES METIERS D INTERNET** et la clé de chiffrement
K = 14

- **Q4** : Est-il plus facile de déchiffrer un texte long ou un texte court ?
  R4 : Un texte long. Car on aura plus de précision sur les fréquences d'apparition des lettres.

- **Q5** : Que remarquez-vous dans le cas où clé =13 ?
  R5 : Dans le cas spécifique où la clé de chiffrement est 13 (la lettre N), on appelle ce chiffrement ROT13 (le nombre 13, la moitié de 26) a été choisi pour pouvoir chiffrer et déchiffrer facilement les messages.

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

Quand la clé = 13, on remarque que
E(M) = M' } $E_k(E_k(M)) = M$.
E(M') = M }

On appelle ça une clé faible. Une clé faible, est une clé dont le comportement dans le système cryptographique est indésirable.

Exemple : Si on veut renforcer le système par un double chiffrement de césar, alors avec une clé faible = 13, le double chiffrement va retourner le message claire de départ. On peut le qualifier comme un comportement indésirable.

Comment trouver les clés faibles pour le chiffrement de césar :

$E_k\big(E_k(M)\big) = M$

$\Rightarrow E_k(M + k) = M$

$\Rightarrow M + k + k\ mod26 = M$

$\Rightarrow 2k\ mod26 = 0$

Les clés faibles sont toutes les valeurs de k où $2k\ mod26 = 0 \Rightarrow \begin{cases} k = 0 \\ k = 13 \end{cases}$

Exercice 2

Remarque :

Le chiffrement de Vigenère est une sorte de chiffrement de César amélioré. La clé est constituée non pas d'un, mais de plusieurs décalages. Cette clé est spécifiée sous la forme d'un mot.
Par exemple, la clé « BAC », de longueur trois, spécifie que pour chiffrer un message, on décale la première lettre d'une position (lettre B), la deuxième de zéro positions (lettre A), la troisième de deux positions (lettre C), et ainsi de suite en reprenant la clé au début.
(Les lettres ont une valeur de A=0 à Z=25).

Exemple : on chiffre le message M= CRYPT avec la clé K = BAC

La lettre C on la chiffre avec la lettre B → 2+1 = 3 = D
La lettre R on la chiffre avec la lettre A → 17+0 = 17 = R
La lettre Y on la chiffre avec la lettre C → 24+2 = 26-26 = 0 = A
La lettre P on la chiffre avec la lettre B → 15+1 = 16 = Q
La lettre T on la chiffre avec la lettre A → 19+0 = 19 = T

1- Chiffrer le message suivant en utilisant la clé = **SECU :**
CHIFFREMENT DE VIGENERE

R1 :

Message (M)	**C**	**H**	**I**	**F**	**F**	**R**	**E**	**M**	**E**	**N**	**T**	**D**	**E**	**V**	**I**	**G**	**E**	**N**	**E**	**R**	**E**
Encodage(M)	2	7	8	5	5	17	4	12	4	13	19	3	4	21	8	6	4	13	4	17	4
K = S E C U = 18 4 2 20	18	4	2	20	18	4	2	20	18	4	2	20	18	4	2	20	18	4	2	20	18
$E_{ki}(m_i) = (m_i + k_i) mod26$	20	11	10	25	23	21	6	32 ≡ 6	22	17	21	23	22	25	10	26 ≡ 0	22	17	6	37 ≡ 11	22
Message chiffré C	U	L	K	Z	X	V	G	G	W	R	V	X	W	Z	K	A	W	R	G	L	W

Le message chiffré = **ULKZXVGGWRVXWZKAWRGLW**

2- Sachant que le message a été chiffré, par la méthode de Vigenère, en utilisant la clé « CRYPTO », quel est le message en clair obtenu en déchiffrant le cryptogramme suivant :

OFBJESUVAJKWVVGCYCTDYIBEWV

R2 :

Message chiffré C	**O**	**F**	**B**	**J**	**E**	**S**	**U**	**V**	**A**	**J**	**K**	**W**	**V**	**V**	**G**	**C**
Encodage(C)	14	5	1	9	4	18	20	21	0	9	10	22	21	21	6	2
K= C R Y P T O = 2 17 24 15 19 14	2	17	24	15	19	14	2	17	24	15	19	14	2	17	24	15
$D_{ki}(m_i) = (m_i - k_i) mod 26$	12	-12 ≡ 14	-23 ≡ 3	-6 ≡ 20	-15 ≡ 11	4	18	4	-24 ≡ 2	-6 ≡ 20	-9 ≡ 17	8	19	4	-18 ≡ 8	-13 ≡ 13
Message (M)	**M**	**O**	**D**	**U**	**L**	**E**	**S**	**E**	**C**	**U**	**R**	**I**	**T**	**E**	**I**	**N**

Message chiffré C	**Y**	**C**	**T**	**D**	**Y**	**I**	**B**	**E**	**W**	**V**
Encodage(C)	24	2	19	3	24	8	1	4	22	21
K= C R Y P T O = 2 17 24 15 19 14	19	14	2	17	24	15	19	14	2	17
$D_{ki}(m_i) = (m_i - k_i) mod 26$	5	-12 ≡ 14	17	-14 ≡ 12	0	-7 ≡ 19	-18 ≡ 8	-10 ≡ 16	20	4
Message (M)	**F**	**O**	**R**	**M**	**A**	**T**	**I**	**Q**	**U**	**E**

Le message en claire= **MODULE SECURITE INFORMATIQUE**

3- Déchiffrer le message suivant chiffré par la méthode de Vigenère avec une clé de longueur 2 (sans connaître la clé)

OSFFBDWCJFDAPSGSYWJSQSUSQSVHSZXGFCQ
GLRHFHRHBRGMCXFVQRAPSXBSFRHRQRZHGXF

R3 :

La cryptanalyse du cryptosystème de Vigenère peut se faire à texte chiffré connu sur les messages assez long.

La première étape consiste à trouver la taille de la clé. A ce niveau, il existe plusieurs méthodes dont :

- Le calcul de **l'indice de coïncidence**
- La méthode de **kasiski**.

Dans notre cas la longueur de la clé est donnée : m = 2.

Une fois que l'on a déterminé la longueur de la clé, on peut constituer des sous messages qui sont décalés à la manière du chiffrement de César. Le décodage est le même que celui de m messages de César, en utilisant l'analyse de fréquence pour chaque sous messages.

Pour décoder le message, on tient compte des hypothèses suivantes :

$$\begin{cases} H0 : Le\ chiffrement\ de\ Vigenère \\ H1 : La\ longueur\ de\ la\ clé : m = 2 \\ H2 : Le\ message\ est\ en\ langue\ française\ (Fréquence\ de\ lettres\ de\ la\ langue\ française). \end{cases}$$

A partir de H_0 et H_1 on peut constituer 2 sous messages qui sont décalés de la même manière que le chiffrement de césar où la fréquence des lettres est préservée :

c_1 = sous message constitué de toutes les lettres de position (2i+1) ➔ {1, 3, 5, 7, …}

c_2 = sous message constitué de toutes les lettres de position (2i) ➔ {1, 3, 5, 7, …}

Ainsi on construit c1 et c2 :

c1 = **OFBWJDPGYJQUQVSXFQLHHHRMXVRPXSRRRHX**
c_2 = **SFDCFASSWSSSSHZGCGRFRBGCFQASBFHQZGF**

1. Analyse de fréquence de c_1:
   1.1. Trouver la fréquence des lettres du sous message c_1 :

Lettres	R	H	X	Q	V	J	P	S	…
Fréquences	5	4	4	3	2	2	2	2	…

   1.2. Calculer la clé probable k_1 :

$H3 : La\ lettre\ \boldsymbol{R}\ message\ chiffré \Rightarrow \boldsymbol{E}\ message\ claire$

La lettre la plus fréquente du message chiffré ***R*** peut correspondre à la lettre la plus fréquente en langue française ***E***.

$$D_{k1}(R) = E \Longrightarrow R - k_1 = E \Longrightarrow 17 - k_1 = 4 \Longrightarrow k_1 = 13$$

2. Analyse de fréquence de c_2:
   2.1. Trouver la fréquence des lettres du sous message c_2 :

Lettres	S	F	G	C	A	H	Z	R	…
Fréquences	8	6	4	3	2	2	2	2	…

   2.2. Calculer la clé probable k_2 :

$H4 : La\ lettre\ \boldsymbol{S}\ message\ chiffré \Rightarrow \boldsymbol{E}\ message\ claire$

La lettre la plus fréquente du message chiffré ***S*** peut correspondre à la lettre la plus fréquente en langue française ***E***.

$D_{k1}(S) = E \Longrightarrow S - k_2 = E \Longrightarrow 18 - k_2 = 4 \Longrightarrow k_2 = 14$

Décodant le message C avec la clé probable : K = k_1k_2 = 13 14 = 'N O'

En décodant le message, on va trouver un message M, qui ne correspond pas à la langue française, ce qui contredit l'hypothèse *H2*.

M = BESROPJOWRQMCETELIWEDEHEDEITFLKSSOD
SYDURUDUNESZOKRICEMCEKNFRETECELUSKR

Donc la clé probable que nous avons calculée ne correspond pas à la clé utilisée. A cet effet on va calculer une nouvelle clé probable.

Soit on change H3, ou H4 ou bien les deux.

On va choisir de changer H3.

Calculer la clé probable k_1 avec une autre hypothèse :

$\boldsymbol{H3'}$: *La lettre* $\boldsymbol{H}$ *message chiffré* $\Rightarrow$ $\boldsymbol{E}$ *message claire*

La lettre du message chiffré ***H*** peut correspondre à la lettre la plus fréquente en langue française ***E***.

$D_{k1}(H) = E \Longrightarrow H - k_1 = E \Longrightarrow 7 - k_1 = 4 \Longrightarrow k_1 = 3$

Décodant le message C avec la nouvelle clé probable : K = k_1k_2 = 3 14 = 'D O'

Message chiffré C	**O**	**S**	**F**	**F**	**B**	**D**	**W**	**C**	**J**	**F**	**D**	**A**	**P**	**S**	**G**	**S ...**
Encodage(C)	14	18	5	5	1	3	22	2	9	5	3	0	15	18	6	18
K= D O **= 3 14**	3	14	3	14	3	14	3	14	3	14	3	14	3	14	3	14
$\boldsymbol{D_{ki}(m_i)}$ $\boldsymbol{= (m_i - k_i) mod 26}$	11	4	2	-9 ≡ 17	-2 ≡ 24	-11 ≡ 15	19	-12 ≡ 14	6	-9 ≡ 17	0	-14 ≡ 12	12	4	3	4
Message (M)	**L**	**E**	**C**	**R**	**Y**	**P**	**T**	**O**	**G**	**R**	**A**	**M**	**M**	**E**	**D**	**E...**

Le message en clair M = **LE CRYPTO GRAMME DE VIGENERE N EST PLUS CONSIDERE DE NOS JOURS COMME UN PROTOCOLE SUR**

Donc la clé : **K = DO**

Exercice 3

Un groupe de *N* personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.

Le groupe décide d'utiliser un système symétrique de chiffrement.

- **Q1** : Quel est le nombre minimal de clés symétriques nécessaires ?

R1 : Pour un groupe de *N* personnes utilisant un crypto système à clés secrètes, il est nécessaire de distribuer un nombre de clés égal à ***N * (N-1) / 2***.

Combien de combinaison de clés entre 2 personnes peut-on faire à base de n personnes sachant que l'ordre n'est pas important.

$$C_n^2 = \frac{n!}{2!\,(n-2)!} \Rightarrow \frac{n\,(n-1)(n-2)!}{2!\,(n-2)!} \Rightarrow \frac{n\,(n-1)}{2}$$

- **Q2** : Donner le nom d'un algorithme de chiffrement symétrique connu.

R2 : DES.

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

- **Q3** : Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées/signées ?

  R3 : *N* couples de clés (privée, publique).

- **Q4** : Bob souhaite envoyer des informations chiffrées et signées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle(s) clé(s) Bob doit-il utiliser ?

  R4 : Pour chiffrer le message Bob utilise la clé publique d'Alice et pour signer le message Bob utilise sa clé privée (clé privée de Bob).

- **Q5** : Donner le nom d'un algorithme de chiffrement asymétrique connu.

  R5 : RSA.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).

- **Q6** : Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

  R6 : le groupe a décidé d'utiliser un système hybride afin de profiter des avantages des deux systèmes. Les crypto-systèmes symétriques sont connus par la rapidité de calcul, cependant, ils ont un problème de partage de la clé secrète en plus ils n'assurent pas la non-répudiation. Par ailleurs, les crypto-systèmes asymétriques permettent de résoudre le problème du partage de la clé secrète ainsi que de signer les messages (donc ils assurent la non-répudiation). Néanmoins, les crypto-systèmes asymétrique sont moins rapide et ils utilisent des clés de taille nettement plus grande.

Exercice 4

Bob, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clé privée mais dispose encore de la clé publique correspondante.

- **Q1** : Peut-il encore envoyer des courriers électroniques chiffrés ? En recevoir ?

  R1 : Oui il peut envoyer des chiffrés car il les chiffre avec la clé publique de correspondant, mais il ne peut pas déchiffrer les messages reçus vu qu'il a perdu sa clé privée.

- **Q2** : Peut-il encore signer des courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?

  R2 : Non il ne peut pas signer les courriers électroniques qu'il envoie parce que pour le faire il faudrait qu'il utilise sa clé privée que malheureusement il a perdue, mais il peut toujours vérifier les signatures des courriers électroniques qu'il reçoit en utilisant les clés publiques des émetteurs des messages.

- **Q3** : Que doit-il faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

  R3 : Il doit générer une nouvelle paire de clé (privée, publique), et révoquer sa clé perdue, pour que les personnes qui voudraient lui envoyer un message n'utiliseraient pas la clé perdue.

Exercice 5

Pour résoudre le problème de l'authentification d'une clé publique, on utilise très souvent la solution des certificats.

- **Q1** : Qu'est ce qu'un certificat et quelles sont les informations qu'il contient ?

  R1 : Le certificat numérique est une sorte de carte d'identité. Il est utilisé principalement pour identifier et authentifier une entité. Le certificat numérique est
  - Infalsifiable : il est crypté pour empêcher toute modification,
  - Nominatif : il est délivré à une entité (comme la carte d'identité est délivrée à une personne et une seule),
  - Certifié : il y a le "tampon" de l'autorité qui l'a délivré.

  Un certificat numérique contient :
    - Nom de l'autorité de certification.
    - Nom et prénom du propriétaire.
    - L'adresse mail du propriétaire.
    - Clé publique du propriétaire.
    - Date à laquelle le certificat numérique a été émis.
    - Date à laquelle le certificat numérique expire.
    - Signature numérique de l'autorité de certification.

- **Q2** : Discuter les deux scénarios suivants en termes de sécurité :
  - Deux certificats différents sont signés par la même clé privée.

    R2-a : Aucun problème, l'autorité de certification signe de nombreux certificats.
  - Deux certificats différents contiennent la même clé publique.

    R2-b :
      1- Si les deux certificats appartiennent à la même personne y a aucun problème.
      2- Si deux personnes différentes, c'est un problème, car cela veut dire que deux personnes ont la même clé publique, et peuvent donc lire les messages destinés à l'autre. Problème de sécurité.