1. Introduction

La cryptographie est une science très ancienne. Des recherches indiquent qu'un scribe égyptien a employé des hiéroglyphes non conformes à la langue pour écrire un message.
De ce temps-là et au long de l'histoire, la cryptographie a été utilisée exclusivement à des fins militaires. Aujourd'hui, les réseaux informatiques exigent une phase de cryptographie comme mécanisme fondamental afin d'assurer la confidentialité de l'information numérique. Dans ce chapitre nous pressentons les notions de base de la cryptographie.

2. Terminologie

- **Texte en clair** : c'est le message à protéger.
- **Texte chiffré** : c'est le résultat du chiffrement du texte en clair.
- **Chiffrement** : c'est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré.
- **Déchiffrement** c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
- **Clé** : c'est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.
- **Cryptographie** : cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour quiconque n'est pas en possession de la clé à utiliser pour le déchiffrer.
- **Cryptanalyse** : c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.
- **Cryptologie** : il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires : la cryptographie et la cryptanalyse.
- **Décrypter** : c'est l'action de retrouver le texte en clair correspondant à un texte chiffré sans posséder la clé qui a servit au chiffrement. Ce mot ne devrait donc être employé que dans le contexte de la cryptanalyse.

- **Crypter** : en relisant la définition du mot décrypter, on peut se rendre compte que le mot crypter n'a pas de sens et que son usage devrait être oublié. Le mot cryptage n'a pas plus de sens non plus.
- **Coder, décoder** : c'est une méthode ou un algorithme permettant de modifier la mise en forme d'un message sans introduire d'élément secret. **[s21]**

2.1. Définition Cryptographie

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le verbe crypter est parfois utilisé mais on lui préfèrera le verbe *chiffrer*.

Le fait de coder un message de telle façon à le rendre secret s'appelle *chiffrement*. La méthode inverse, consistant à retrouver le message original, est appelée *déchiffrement*

Le chiffrement se fait généralement à l'aide d'une *clef de chiffrement*, le déchiffrement nécessite quant à lui une *clef de déchiffrement*. On distingue généralement deux types de clefs :

- ***Les clés symétriques***: il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.
- ***Les clés asymétriques***: il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé *chiffrement à clé publique*). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement **[s22]**

2.2. Qu´entend-on par clé ?

On appelle clé une valeur utilisée dans un algorithme de cryptographie, afin de chiffrer une donnée. Il s´agit en fait d´un nombre complexe dont la taille se mesure en bits. On peut imaginer que la valeur numérique correspondant à 1024 bits est absolument gigantesque. Voir aussi Bits and bytes. Plus la clé est grande, plus elle contribue à élever la sécurité à la solution. Toutefois, c´est la combinaison d´algorithmes complexes et de clés importantes qui sera la garantie d´une solution bien sécurisée.

Les clés doivent être stockées de manière sécurisée et de manière à ce que seul leur propriétaire soit en mesure de les atteindre et de les utiliser. **[1]**

3. Buts de la cryptographie

La cryptographie permet de résoudre quatre problèmes différents :

- **La confidentialité**. Le texte chiffré ne doit être lisible que par les destinataires légitimes. Il ne doit pas pouvoir être lu par un intrus.
- **L'authentification**. Le destinataire d'un message doit pouvoir s'assurer de son origine. Un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre.
- **L'intégrité.** Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin. Un intrus ne doit pas être capable de faire passer un faux message pour légitime.
- **La non répudiation**. Un expéditeur ne doit pas pouvoir, par la suite, nier à tort avoir envoyé un message. **[s21]**

4. Mécanismes de la cryptographie

Un algorithme de cryptographie ou un chiffrement est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clef (un mot, un nombre, ou une phrase). Afin de crypter une donnée avec des clés différentes le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clef.

Un système de cryptographie est constitué d'un algorithme de cryptographie, ainsi que de toutes les clefs et tous les protocoles nécessaires à son fonctionnement. **[6]**

5. La cryptographie classique

5.1. La cryptographie par substitution mono alphabétique

Le codage par substitution mono-alphabétique (on dit aussi les alphabets désordonnés) est le plus simple à imaginer. Dans le message clair, on remplace chaque lettre par une lettre différente.

- **Application**

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

Tableau 2.1. Substitution mono alphabétique

Le texte que nous souhaitons coder est le suivant :

CRYPTAGE SELECTIF

Le texte codé est alors :

IUEJGNPC VCQCIGLW

Un des problèmes avec le code par substitution est de se souvenir de la clé (c'est-à-dire la permutation) employée. Il n'est en effet pas facile de se souvenir de 26 lettres dans un ordre abscon. C'est pourquoi il existe des variantes :

Le chiffre de César, fondé sur un simple décalage de lettres.

Le chiffre AtBash**.** Il consiste simplement à écrire l'alphabet en sens contraire :

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

Tableau 2.2. Le chiffre AtBash. **[s6]**

Bien sûr, la sûreté d'un tel codage est quasi-nulle, puisqu'il suffit de connaitre l'algorithme de codage pour pouvoir décoder immédiatement. Remarquons toute fois une propriété du code Atbash : il est réversible, c'est-à-dire que c'est le même algorithme qui code et décode le texte. L'une des façons les plus courantes de définir une substitution est de se mettre d'accord sur un mot-clé facile à retenir, mettons MATHWEB, et de compléter ensuite le tableau par ordre alphabétique. Ceci donne ici :

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

Tableau 2.3. La méthode MATHWEB. **[s6]**

Il existe aussi d'ordres méthodes pour remplir un tel tableau à partir de matrices. **[s6]**

◆ **Le code de César**

➢ **Principe**

Le code de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Il consiste en une substitution mono-alphabétique, où la substitution est définie par un décalage de lettres. Par exemple, si on remplace A par D, on remplace B par E, C par F, D par G, etc...

Il n'y a que 26 façons différentes de crypter un message avec le code de César. Cela en fait donc un code très peu sûr, puisqu'il est très facile de tester de façon exhaustive toutes les possibilités. Pourtant, en raison de sa grande simplicité, le code de César fut encore employé par les officiers sudistes pendant la guerre de Sécession, et même par l'armée russe en 1915. **[s10]**

5.2. La cryptographie par substitution poly alphabétique

◆**Le chiffre de Vigenere**

➢ **Principe**

Vigenère, né en 1523, fut l'initiateur d'une nouvelle façon de chiffrer les messages qui domina 3 siècles durant. Vigenère était quelqu'un de très hétéroclite, tantôt alchimiste, écrivain, historien, il était aussi diplomate au service des ducs de Nevers et des rois de France. C'est en 1586 qu'il publie son Traicté des chiffres ou secrètes manières d'écrire, qui explique son nouveau chiffre.

L'idée de Vigenère est d'utiliser un chiffre de César, mais où le décalage utilisé change de lettres en lettres. Pour cela, on utilise une table composée de 26 alphabets, écrits dans l'ordre, mais décalés de ligne en ligne d'un caractère. On écrit encore en haut un alphabet complet, pour la clé, et à gauche, verticalement, un dernier alphabet, pour le texte à coder : **[s19]**

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

Tableau 2.4. Le chiffre de Vigenere. **[s19]**

- **Application**

On veut coder le texte "CRYPTOGRAPHIE DE VIGENERE" avec la clé "MATHWEB". On commence par écrire la clef sous le texte à coder :

C	R	Y	P	T	O	G	R	A	P	H	I	E	D	E	V	I	G	E	N	E	R	E
M	A	T	H	W	E	B	M	A	T	H	W	E	B	M	A	T	H	W	E	B	M	A

Pour coder la lettre C, la clé est donnée par la lettre M. On regarde dans le tableau l'intersection de la ligne donnée par le C, et de la colonne donnée par le M
On trouve O. Puis on continue. On trouve : ORRWPSHDAIOEI EQ VBNARFDE. **[s19]**

- **Avantage**

Cet algorithme de cryptographie comporte beaucoup de points forts. Il est très facile d'utilisation, et le décryptage est tout aussi facile si on connait la clé. Il suffit, sur la colonne de la lettre de la clé, de rechercher la lettre du message codé. A l'extrémité gauche de la ligne, on trouve la lettre du texte clair. **[s19]**

6. Algorithmes de la cryptographie

6.1. Algorithmes symétriques (clef secrète)

Un algorithme symétrique est un algorithme qui permet de transformer un texte en clair en texte chiffré en utilisant une clé et de retransformer le texte chiffré en texte en clair en utilisant la même clé.

Le secret de la communication est uniquement assuré par la clé qui est utilisée lors de la phase de chiffrement et de déchiffrement. L'algorithme utilisé ne fait pas partie du secret. **[7]**

On parle d'algorithmes symétriques car c'est la même clé qui sert à la fois au chiffrement et au déchiffrement du message.

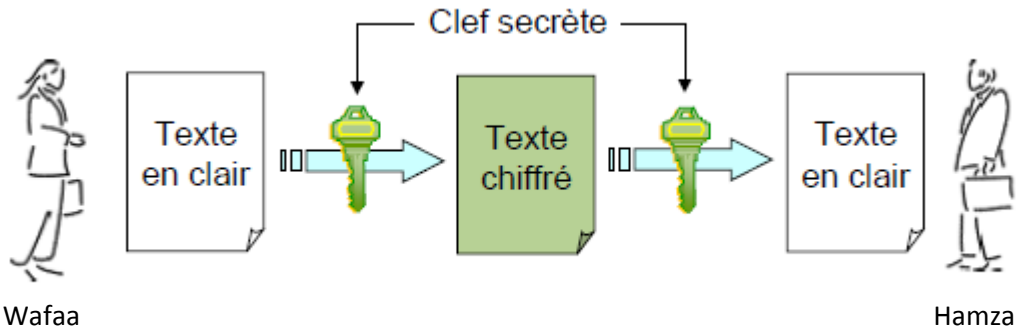

Figure 2.1. Principe de l'algorithme symétrique **[s7]**

Les algorithmes symétriques sont de deux types :

- ✓ Les algorithmes de chiffrement en continu, qui agissent sur le message en clair un bit à la fois.
- ✓ Les algorithmes de chiffrement par bloc, qui opèrent sur le message en clair par groupes de bits appelés bloc. **[s7]**

➢ **Algorithmes de chiffrement en continu**

Qui opèrent sur le message en clair un bit à la fois. Le principe consiste à générer un flux pseudo aléatoire et de le combiner avec l'information bit à bit par l'opération XOR. A la réception, on applique le même mécanisme, et on restitue l'information. **[s8]**

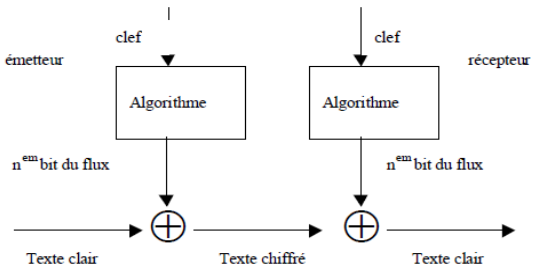

Figure 2.2. Chiffrement en continu **[s8]**

➢ **Algorithmes de chiffrement par bloc**

Qui opèrent sur le message en clair par groupe de bit. La taille typique des blocs est 64 bits, ce qui est assez grand pour interdire l'analyse et assez petit pour être pratique. **[s8]**

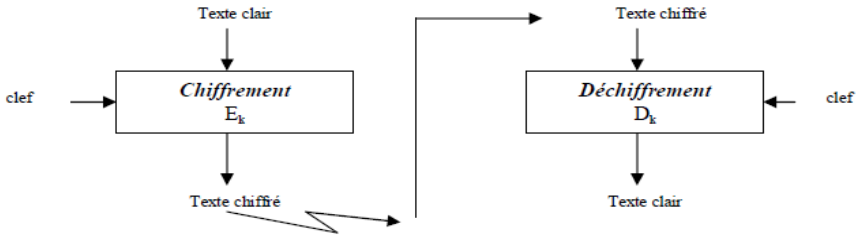

Figure 2.3. Chiffrement par bloc **[s8]**

Les algorithmes de chiffrement par blocs peuvent être utilisés suivant différents modes, dont les deux principaux sont le mode ECB (Electronic Code Boock)et le mode CBC(Chipher Block Chaining) . **[s8]**

1-Le mode ECB (Electronic Code Book) :

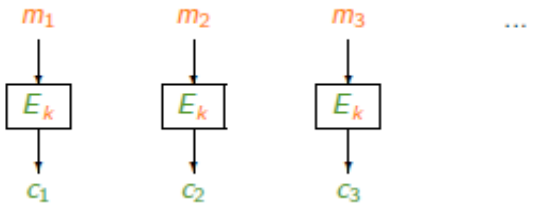

Figure 2.4. Le mode ECB **[s8]**

- **Chiffrement :** Chaque bloque clair m_i est chiffré indépendamment et donne un bloc chiffré $c_i=E_k(m_i)$.
- **Déchiffrement :** Chaque chiffré est déchiffré indépendamment pour donner le clair correspondant $m_i=D_k(c_i)$.

Avantage : Ce mode permet le chiffrement en parallèle des différents blocs composant un message.

Inconvénient : Même bloc de message en clair sera toujours chiffré en un même bloc de message chiffré. Or, dans le chiffrement sur un réseau par exemple, les données à chiffrer ont des structures régulières facilement repérables par un cryptanalyste, qui pourra donc obtenir beaucoup d'informations. D'autre part, un attaquant actif pourra facilement manipuler les messages chiffrés en retirant, répétant ou inter changeant des blocs. Un autre inconvénient,

qui s'applique au chiffrement par blocs en général, est l'amplification d'erreur : si un bit du message chiffré est modifié pendant le transfert, tout le bloc de message en clair correspondant sera faux. **[s8]**

2-Le mode CBC (Cipher Block Chaining) :

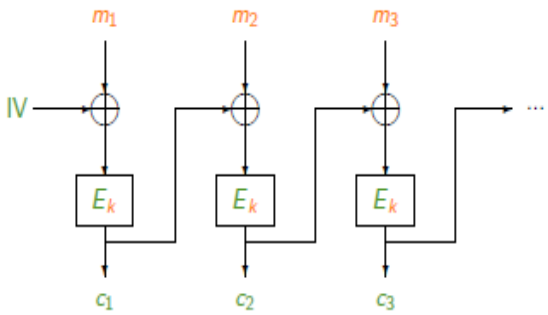

Figure 2.5. Chiffrement CBC **[s8]**

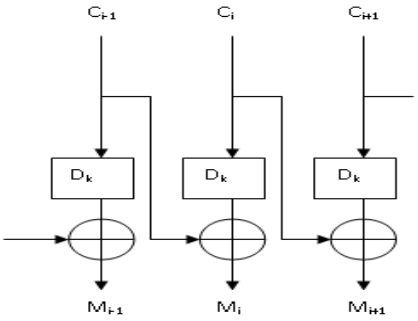

Figure 2.6. Déchiffrement CBC

- **Chiffrement :** Un vecteur d'initialisation IV est généré aléatoirement Ci =Ek (Mi ⊕ Ci-1).Le vecteur IV est transmis avec les blocs chiffrés.
- **Déchiffrement :** $M_i = C_{i-1} \oplus D_k(C_i)$. **[s8]**

Avantage : La structure du message en clair est masquée par le chaînage. Un attaquant ne peut plus manipuler le cryptogramme, excepté en retirant des blocs au début ou à la fin. Un inconvénient est qu'il n'est plus possible de paralléliser le chiffrement des différents blocs (le déchiffrement reste parallélisable).

Inconvénient : On pourrait craindre que le chaînage de bloc n'entraîne une propagation d'erreur importante. De fait, une erreur d'un bit sur le message en clair affectera tous les blocs chiffrés suivants. Par contre, si un bit du message chiffré est modifié au cours du transfert, seul le bloc de message en clair correspondant et un bit du bloc de message en clair suivant seront endommagés : le mode CBC est dit auto réparateur. **[s8]**

Exemple algorithmes symétrique

- **Chiffrement par bloc**

		DES	3DES	IDEA	RC4	RC5 et RC6	Blowfish	AES
Nom réel		Data Encryption Standard	Triple Data Encryption Standard	International Data Encryption Algorythm	Rivest Cipher 4	Rivest Cipher 5/6	Blowfish	Advanced Encryption Standard
Date		1973	1978	1992	1987	1994	1993	1998
Longueur	**Clé**	64 bits (56 effectifs)	192 bits (168 effectifs)	128 bits	jusqu'a 256 bits	entre 0 et 2040 bits	entre 40 et 448 bits	128, 192, 256 bits
	Bloc	64 bits	64 bits	64 bits	Flux	32, 64, 128 bits	64 bits	128 bits

6.2. Algorithmes asymétriques (clef publique)

Les algorithmes symétriques vus sont tous fiables mais ils posent un problème, c'est celui de l'échange de la clé : comment transmettre de manière fiable à mon interlocuteur la clé de chiffrement utilisée pour chiffrer le message que je lui envoie ? Il y a bien sûr le téléphone, mais il y a aussi les écoutes téléphoniques.

Les algorithmes asymétriques ont été inventés pour pallier précisément le problème de transmission sécurisée de la clé. **[s12]**

On parle d'algorithmes asymétriques car ce n'est pas la même clé qui sert au chiffrement et au déchiffrement. Dans le cas de ces algorithmes, on parlera alors de clé privée et de clé publique. Ces deux clés, clé privée et clé publique, sont intimement liées par une fonction mathématique complexe. **[5]**

Les algorithmes asymétriques possèdent 2 modes de fonctionnement ;

- Le mode chiffrement dans lequel l'émetteur chiffre un fichier avec la clé publique du destinataire pour chiffrer. Le destinataire utilise sa clé privée pour déchiffrer le fichier. Dans ce mode, l'émetteur est sûr que seul le destinataire peut déchiffrer le fichier.

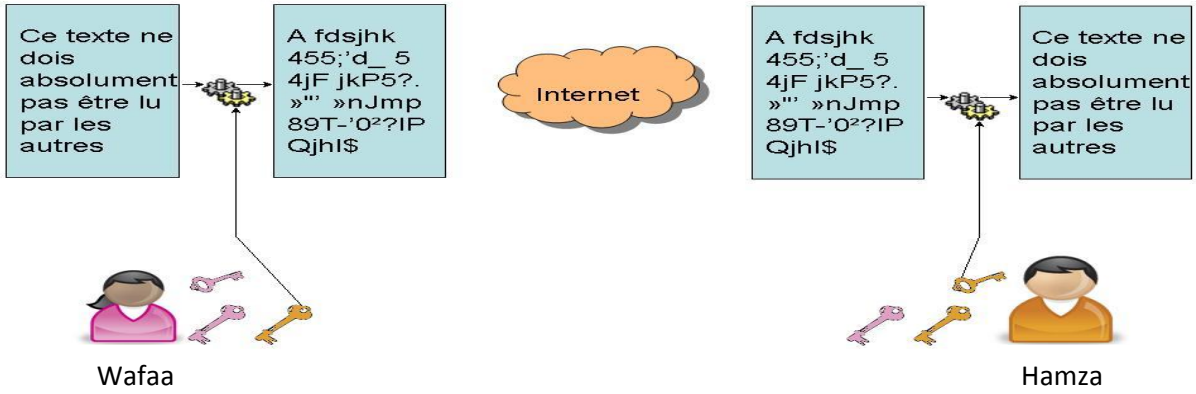

Figure 2.7. Chiffrement avec l'algorithme asymétrique. **[s21]**

- Le mode signature dans lequel l'émetteur signe un fichier avec sa propre clé privée. Le destinataire utilise la clé publique de l'émetteur pour vérifier la signature du fichier. Dans ce mode, le destinataire est sûr que c'est bien l'émetteur qui a envoyé le fichier.
-

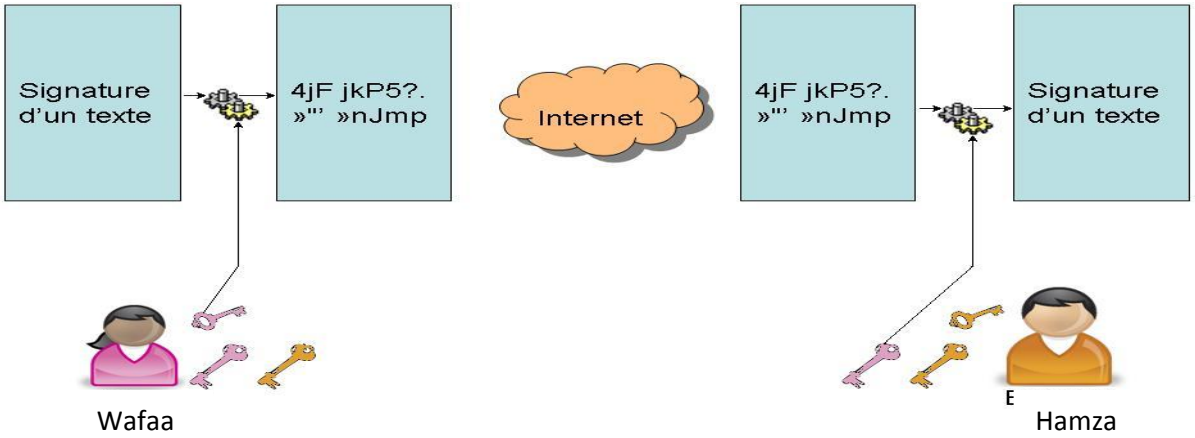

Figure 2.8. Signature avec l'algorithme asymétrique. **[s21]**

Donc pour résumer :

- L'émetteur chiffre avec la clé publique du destinataire, le destinataire déchiffre avec sa clé privée.
- L'émetteur signe avec sa clé privée, le destinataire vérifie la signature avec la clé publique de l'émetteur. **[s21]**

- **Exemple algorithmes asymétrique**

Quelques algorithmes de cryptographie asymétrique très utilisés :

- **RSA** (chiffrement et signature).
- **DSA** (signature).
- Protocole d'échange de clés **Diffie-Hellman** (échange de clé) .**[s21]**

6.3. Cryptage symétrique vs cryptage asymétrique

Cryptage symétrique :	***Cryptage asymétrique :***
-Chiffrement à clé privé (utilisation un clé pour crypter qui fonctionne aussi pour décrypter -Très facile -Très rapide -les clés de chiffrement symétrique doivent être conservées en toute sécurité - vous devez vous assurer que chaque personne qui a besoin de la clé, il obtient sans aucun risque de le sortir.	-Chiffrement à clé publique (utilisation deux clés un pour crypter **clé publique** et autre pour décrypter **clé privé** -Difficile par rapport au cryptage symétrique -Plus lent -les clés publiques qu'ils utilisent sont sans danger pour être publié n'importe où parce que pour obtenir la clé privée à partir d'une clé publique peut prendre des centaines d'années de travail. [2]

7. Conclusion

Dans ce chapitre nous avons présenté une introduction générale sur la cryptographie, nous avons distingué deux classe importante des méthodes de chiffrement, c'est le cryptage symétrique a clé secrète et le cryptage asymétrique a clé publique. Nous avons aussi montré la puissance et la faiblesse de chaque type d'algorithme de chiffrement.