**République Algérienne Démocratique et Populaire**
**Université Abou Bakr Belkaid– Tlemcen**
**Faculté des Sciences**
**Département d'Informatique**

**Mémoire de fin d'études**

**pour l'obtention du diplôme de Master en Informatique**

***Option:*** *Réseaux et systèmes distribué (R.S.D)*

# Thème

**Etude et comparaison entre blowfish et 3-ways pour le cryptage de flux audio d'un fichier vidéo en utilisant la bibliothèque FFmpeg**

**Réalisé par :**

- **Mr BOUCHACHIA ABDERRAHIM**

*Présenté le 03 Juillet 2022 devant le jury composé de :*

- *Mme ABDELDJELIL Hanane* *(Présidente)*
- *Mr BELHOCINE Amine* *(Examinateur)*
- *Mr BENAISSA Samir Mohamed* *(Encadreur)*

Année universitaire : 2021-2022

# *Remerciement*

*Je remercie dieu le tout puissant de m' avoir donné la santé et la volonté d'entammer et de terminer ce mémoire.*

*Tout d'abord, ce travail ne serait pas aussi riche et n'aurait pas pu avoir le jour sans l'aide et l'encadrement de Mr Benaissa Mahamed, je le remercie pour la qualité de son encadrement exceptionnel, pour sa patience, sa rigueur et sa disponibilité durant ma préparation de ce mémoire.*

*Je tiens enfin à exprimer ma gratitude aux membres de jury pour avoir accepté de juger ce travail.*

# Table de matière

# Liste des figures

# Liste des tableaux

# Introduction générale

# Introduction générale:

La sécurité est le problème de l'homme depuis longtemps. Le développement de l'informatique et des télécommunications ainsi que la généralisation élargie des communications par Internet ont accentué la complexité des problèmes de sécurité et de leurs solutions. En effet de nouveaux phénomènes en résultent tels que les virus informatiques, accès non autorisés aux données, fausses informations, engendrant un besoin impérieux de sécurisation des informations et des technologies associées.

Pour construire un système de sécurité il est nécessaire de comprendre les notions de la cryptologie et être au courant du développement quotidien dans ce domaine. Les crypto-systèmes modernes reposent sur le principe que le secret ne doit pas résider dans l'algorithme mais plutôt dans la clé.

De nombreux systèmes de codage qui répondent à ce principe ont été proposés. Parmi les classes de ces systèmes nous pouvons citer les algorithmes de chiffrement symétrique (DES, IDEA, AES,Blowfish ...) qui reposent sur le secret de la clé et les algorithmes de chiffrement asymétriques (RSA, ...) qui se basent sur la difficulté de factoriser les grandes nombres.

Les travaux réalisés dans ce mémoire ont pour objectif d'étudier et d'implémenter deux systèmes de cryptage/décryptage en utilisant la bibliothèque Ffmpeg et le langage c, l'un est symétrique basé sur un chiffrement en bloc avec taille de block fixe et taille de clé variable, la clé et le block ont de taille fixe dans l'autre algorithme ,deux algorithmes simple ont été ajoutés à cette étude dans le but d' observer plus clairement les résultats de chiffrement. Le deuxième objectif est d'appliquer le chiffrement symétrique sur le flux audio d'une vidéo .Pour cela, j'ai organisé le mémoire comme suit :

Dans le premier chapitre, j'ai présenté des définitions et des généralités sur la cryptographie ainsi que des terminologies dans ce domaine. Ce chapitre traite le but de la cryptographie et le développement des techniques cryptographiques qui ont marqué l'histoire, du chiffrement classique vers le chiffrement moderne représenté par les méthodes symétriques et asymétriques.

Le chapitre 2 est dédié à la présentation des fondements théoriques de Blowfish et 3-way

En présentant le principe de fonctionnement et la logique derrière chaque algorithme en citant quelques avantages et inconvénients.

Le chapitre 3 est consacré aux notions basiques sur le son, incluant sa définition ses caractéristiques et les formats des fichiers audios.

Le chapitre 4 est pour la présentation de la bibliothèque Ffmpeg utilisé et l'application des différents algorithmes de chiffrement implémentés en c (blowfish,3-way,ou-exclusif,substitution simple) sur des flux audios des vidéos choisi selon la taille de leur fichiers audio et son contenu (son, parole, son et parole) .

# Chapitre 1 :

# Introduction à la cryptographie

## 1.1 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.

## 1.2 Terminologie [1]

• **Texte en clair** : c'est le message à protéger.

• **Texte chiffré** : c'est le résultat du chiffrement du texte en clair.

• **Chiffrement** : Transformation d'un message de façon à le rendre incompréhensible.

• **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** : La cryptographie est une composante de la cryptologie. C'est la science du chiffrement.

• **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** : Branche des mathématiques qui traite de la cryptographie et de la cryptanalyse.

• **Décrypter** : Décrypter un message, c'est déchiffrer le document original sans connaître la clé, c'est à dire en cassant le chiffrement.

• **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.

• **Coder, chiffrer, crypter : les** opérations de chiffrement et de codage font partie de la théorie de l'information et de la théorie des codes. La différence essentielle réside dans la volonté de protéger les informations et d'empêcher des tierces personnes d'accéder aux données dans le cas du chiffrement. Le codage consiste à transformer de l'information (des données) vers un ensemble de mots. Chacun de ces mots est constitué de symboles. La compression est un codage : on transforme les données vers un ensemble de mots adéquats destinés à réduire la taille, mais il n'y a pas de volonté de dissimuler (bien que cela se fasse implicitement en rendant plus

difficile d'accès le contenu).Si on comprend le mot « décrypter » on réalise que, le mot «crypter» n'a pas de sens.

### 1.2.1 Définition Cryptographie [2]

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 clé de chiffrement, le déchiffrement nécessite quant à lui une clé de déchiffrement. On distingue généralement deux types de clés :

• **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

### 1.2.2 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 seront 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.

**Clé ou clef :**

Les deux graphies sont correctes, mais clé tend de plus en plus à remplacer clef dans l'usage contemporain.

Employé comme épithète, peut s'écrire avec ou sans trait d'union : mot clé ou mot-clé, porte-clés ou porte-clés, secteur clé ou secteur-clé, etc.

## 1.3 Buts de la cryptographie [3]

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.

## 1.4 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 clé (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 clé.

Un système de cryptographie est constitué d'un algorithme de cryptographie, ainsi que de toutes les clés et tous les protocoles nécessaires à son fonctionnement.

## 1.5 La cryptographie classique

### 1.5.1 La cryptographie par substitution mono alphabétique [4]

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 1 Substitution mono alphabétique*

Le texte que nous souhaitons coder est le suivant :

CRYPTAGE SELECTIF

Le texte codé est alors :

EQBGNWTY MYIYENCZ

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 tel ordre. 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 le chiffre AtBash*

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 3 La méthode MATHWEB*

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

#### ❖ 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.

## 1.5.2 La cryptographie par substitution poly alphabétique

#### ❖ Le chiffre de Vigenere [5]

### ➢ 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 :

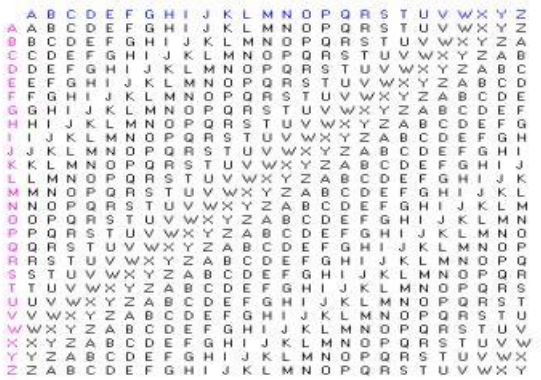

*Figure 1 le chiffre de Vigénere*

- **Application**

On veut coder le texte "CRYPTOGRAPHIE DE VIGENERE" avec la clé "MATHWEB". On commence par écrire la clé 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 |

*Tableau 4 exemple de chiffrement avec la clé 'MATHWEB'*

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.

- **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.

# 1.6 Algorithmes de la cryptographie

## 1.6.1 Algorithmes symétriques (clé secrète) [6]

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.

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

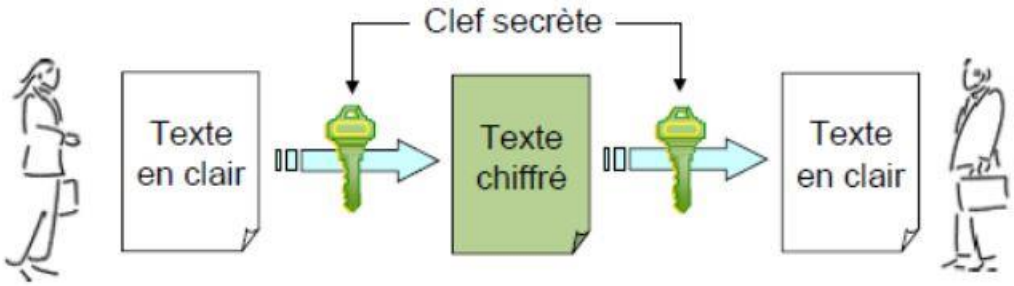


*Figure 2 Principe de l'algorithme symétrique*

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.

### ➢ 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.

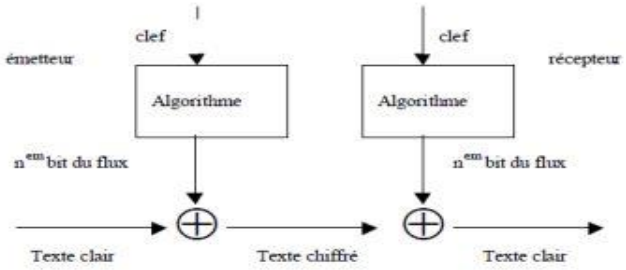


*Figure 3 Chiffrement en continu*

### ➢ 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.

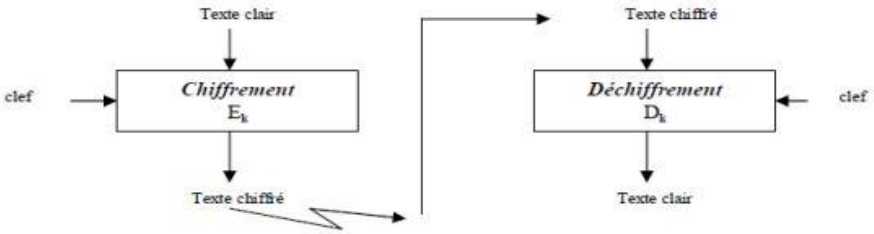


*Figure 4 Chiffrement par bloc*

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) .

1-Le mode ECB (Electronic Code Book) :

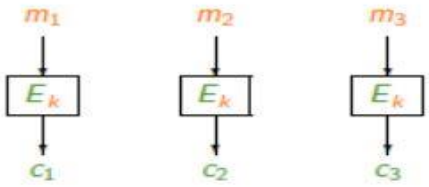


*Figure 5 Le mode ECB*

- **Chiffrement** : Chaque bloque clair mi est chiffré indépendamment et donne un bloc chiffré ci=Ek(mi).
- **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.

## 2-Le mode CBC (Cipher Block Chaining) :

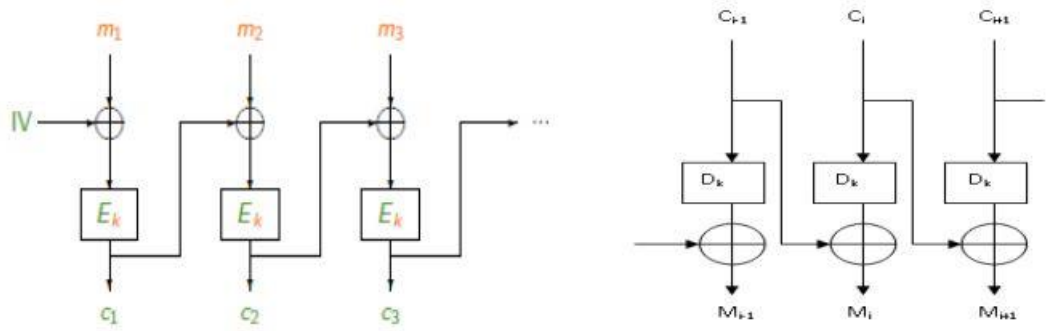


*Figure 6 Chiffrement/ Déchiffrement CBC*

- Chiffrement : Un vecteur d'initialisation IV est généré aléatoirement Ci =Ek (Mi ⊕ Ci-1).Le vecteur IV est transmis avec les blocs chiffrés.
- Déchiffrement : Mi= Ci-1 ⊕ Dk(Ci).

**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.

**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 |

*Figure 7 comparaison entre different algorithme de chiffrement*

### 1.6.2 Algorithmes asymétriques (clé publique) [6]

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.

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.

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.

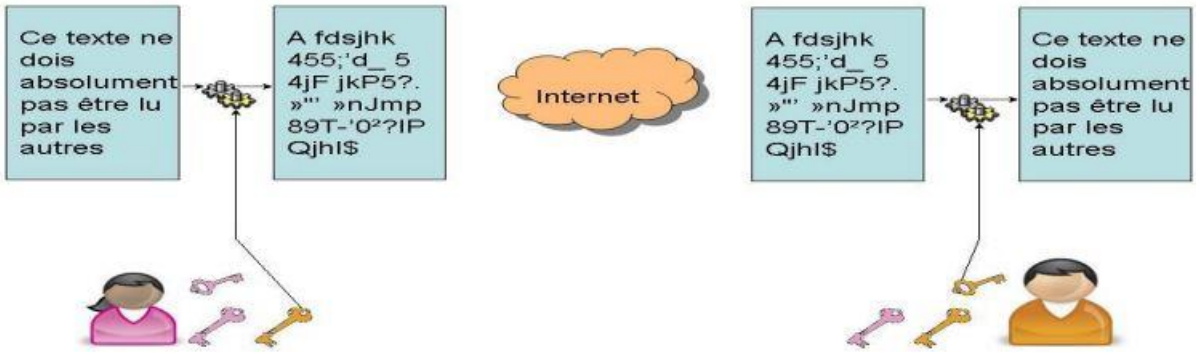


*Figure 8 Chiffrement avec l'algorithme asymétrique*

- 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.

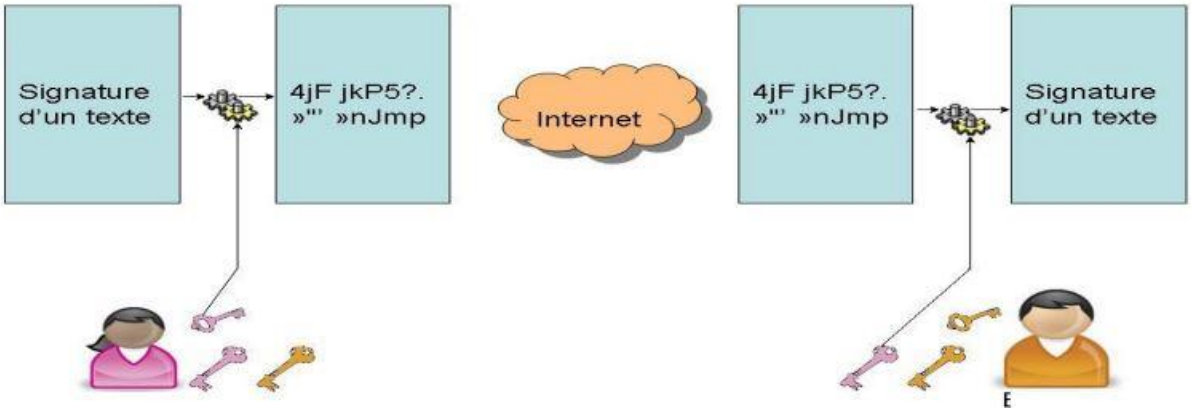


*Figure 9 Signature avec l'algorithme asymétrique*

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.

✓ 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).

### 1.6.3 Cryptage symétrique vs cryptage asymétrique

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

*Tableau 5 comparaison entre cryptage symétrique et cryptage asymétrique*

## 1.7 Conclusion

Dans ce chapitre J'ai présenté une introduction générale sur la cryptographie, en distinguant deux classes importantes des méthodes de chiffrement, c'est le cryptage symétrique à clé secrète et le cryptage asymétrique a clé publique. J'ai aussi montré la puissance et la faiblesse de chaque type d'algorithme de chiffrement

# Chapitre 2 Les algorithmes de cryptage Blowfish et 3-way :

# 2.1 Introduction

Les problèmes de sécurité sont l'un des aspects les plus importants d'un système d'information. Données ou informations ne seront plus utiles si des personnes non autorisées ont volé les données ou informations. Le niveau de sécurité doit être en outre renforcé. Le fichier est une donnée importante qui contient des informations à échanger. Le dossier doit avoir un bon système de protection de sécurité pour être dans la livraison de l'archive ne fuit pas. Compte tenu de là l'utilisation des technologies de l'information dans tous les aspects tels que l'éducation, le gouvernement, l'industrie et autres, la sécurité des données doit être correctement prise en compte. Le système utilisé pour sécuriser les données est la cryptographie. Beaucoup des techniques cryptographiques peuvent être appliquées aux informations qui seront protégées, dont parmi eux blowfish et 3-way.

# 2.2 L'algorithme blowfish :[7]

Blowfish est une technique de cryptage conçue par Bruce Schneider en 1993 comme alternative à la technique de cryptage DES. Il est nettement plus rapide que DES et fournit un bon taux de cryptage sans qu'aucune technique de cryptanalyse efficace n'ait été trouvée à ce jour .C'est l'un des premiers chiffrement par blocs sécurisés non soumis à aucun brevet et donc librement accessible à tous.

Taille de bloc : 64 bit

KeySize : taille variable de 32 bit à 448 bits.

Nombre de sous-clés : 18 [tableau P]

Nombre de tours : 16

Nombre de boites de substitution : 4 [chacune ayant 512 entrées de 32 bits chacune]

## 2.2.1 Processus de chiffrement :

Le processus de cryptage complet peut être élaboré comme suit :

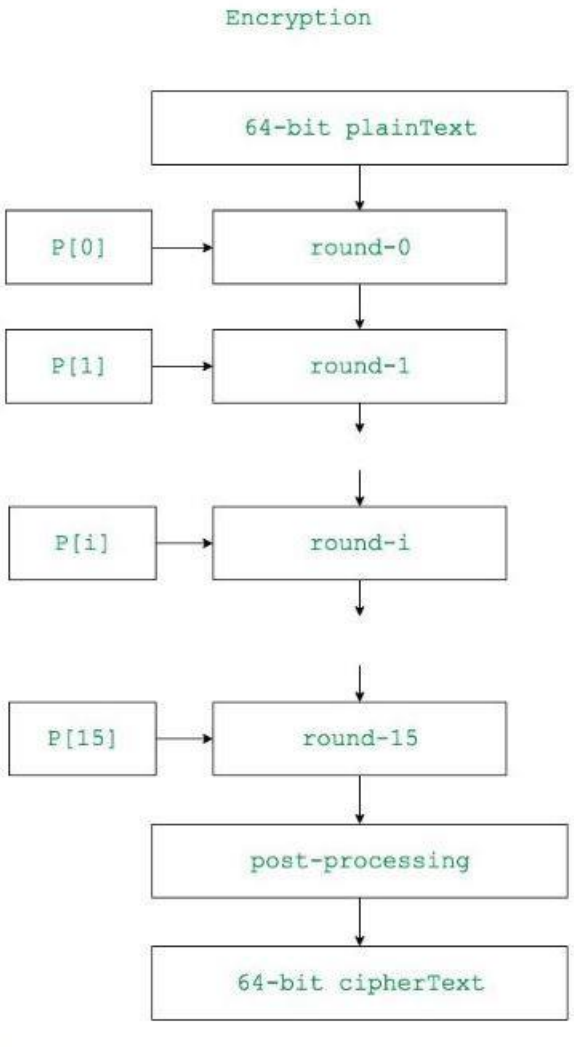


*Figure 10 processus de cryptage blowfish*

Voyons chaque étape une par une :

**Etape 1 : génération des sous-clés**

18 sous-clés {P [0]…P [17]} sont nécessaires à la fois dans le processus de chiffrement et de déchiffrement et les mêmes sous-clés sont utilisées pour les deux processus.

Ces 18 sous-clés sont stockées dans un tableau P, chaque élément du tableau étant une entrée de 32 bits.

Il est initialisé avec les chiffres de pi (0<=i<18).

La représentation hexadécimale de chacune des sous-clés est donnée par :

P [0] = "243f6a88"

P [1] = "85a308d3"

.

.

.

P [17] = "8979fb1b"

| | |
|---|---|
| P[0] : 243f6a88 | P[9] : 38d01377 |
| P[1] : 85a308d3 | P[10] : be5466cf |
| P[2] : 13198a2e | P[11] : 34e90c6c |
| P[3] : 03707344 | P[12] : c0ac29b7 |
| P[4] : a4093822 | P[13] : c97c50dd |
| P[5] : 299f31d0 | P[14] : 3f84d5b5 |
| P[6] : 082efa98 | P[15] : b5470917 |
| P[7] : ec4e6c89 | P[16] : 9216d5d9 |
| P[8] : 452821e6 | P[17] : 8979fb1b |

*Figure 11 représentation hexadécimal sur 32-bit des valeurs de sous-clés*

Maintenant, chacune des sous-clés est modifiée par rapport à la clé d'entrée comme :

P[0] = P[0] xor 1er 32 bits de la clé d'entrée

P[1] = P[1] xor 2ème 32 bits de la clé d'entrée

.

.

.

P[i] = P[i] xor (i+1)ème 32 bits de la clé d'entrée

(passez au 1er 32 bits en fonction de la longueur de la clé)

.

.

.

P[17] = P[17] xor 18e 32 bits de la clé d'entrée

(roulez sur les 32 premiers bits en fonction de la longueur de la clé)

Le tableau P-array contient 18 sous-clés qui sont utilisées pendant tout le processus de chiffrement

**Etape 2** : **initialiser les Boîtes de Substitution**

4 boîtes de substitution (boîtes S) sont nécessaires{S[0]…S[4]} à la fois dans le processus de cryptage et de décryptage, chaque boîte S ayant 256 entrées{S[i][0]…S[i][ 255]} où chaque entrée est de 32 bits.

Il est initialisé avec les chiffres de pi après l'initialisation du P-array.

**Étape 3** : **Cryptage**

La fonction de chiffrement se compose de deux parties :

**a**. Tours : le cryptage consiste en 16 tours, chaque tour (Ri) prenant en entrée le texte en clair (P.T.) du tour précédent et la sous-clé correspondante (Pi). La description de chaque manche est la suivante :

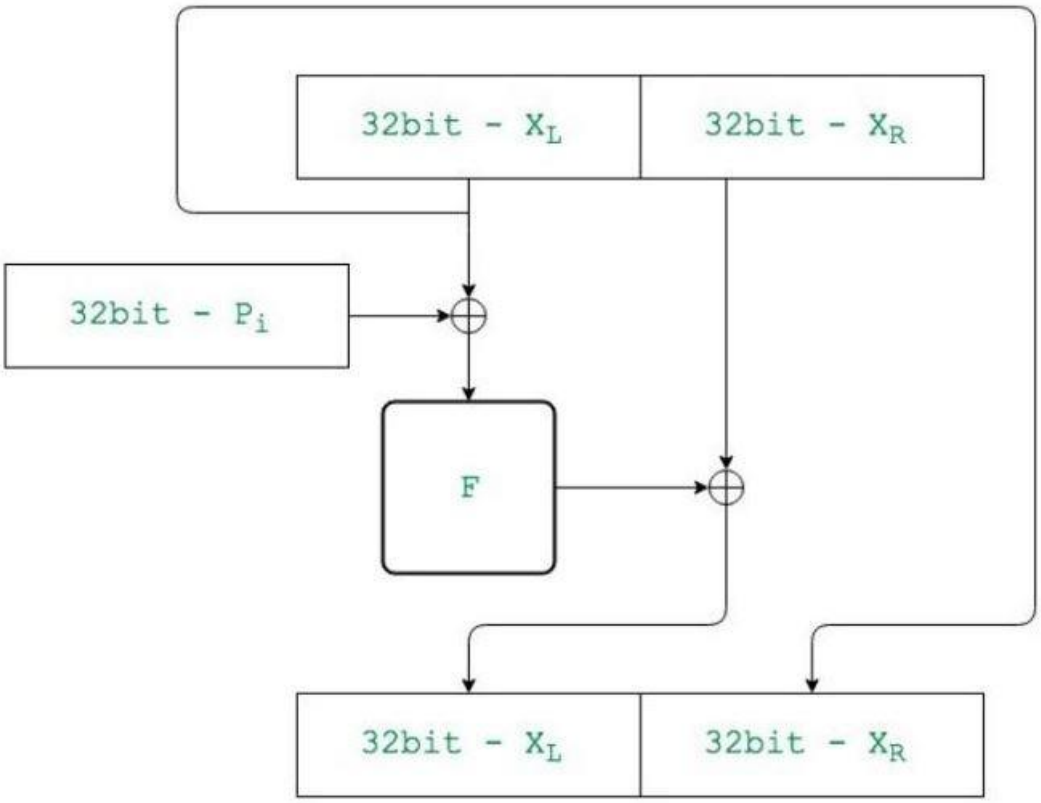


*Figure 12 organigramme de chaque tour de r1*

La description de la fonction « F » est la suivante :

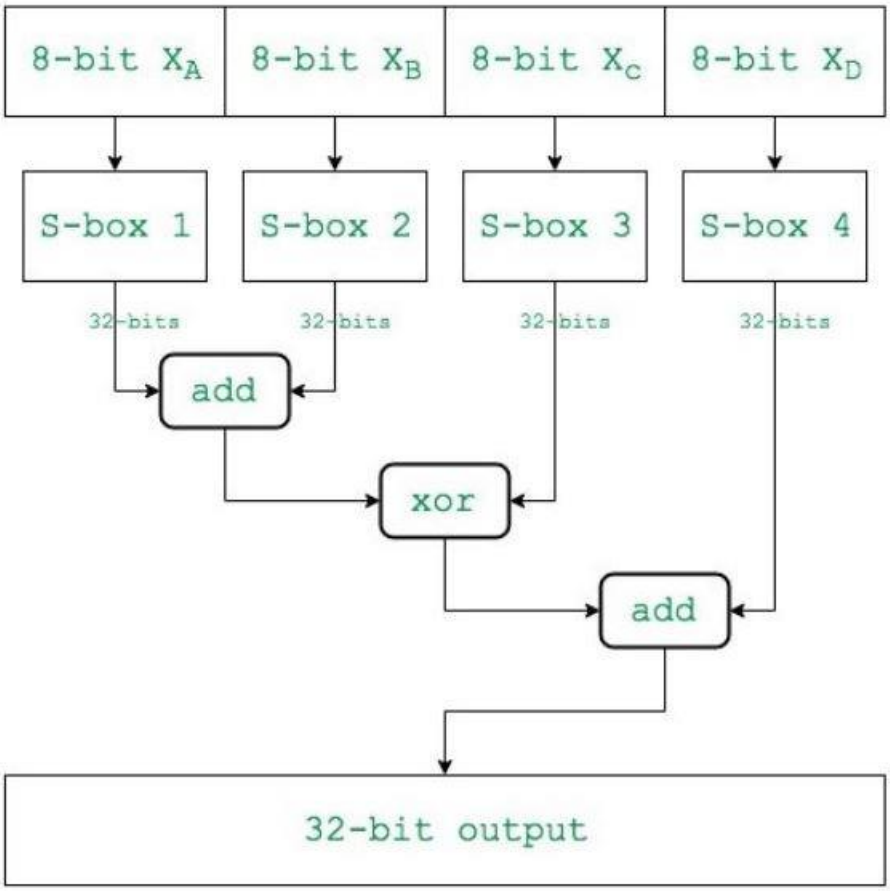


*Figure 13 organigramme de chaque fonction f*

Ici la fonction "add" est addition modulo 2^32.

**b**. Post-traitement : la sortie après les 16 tours est traitée comme suit :

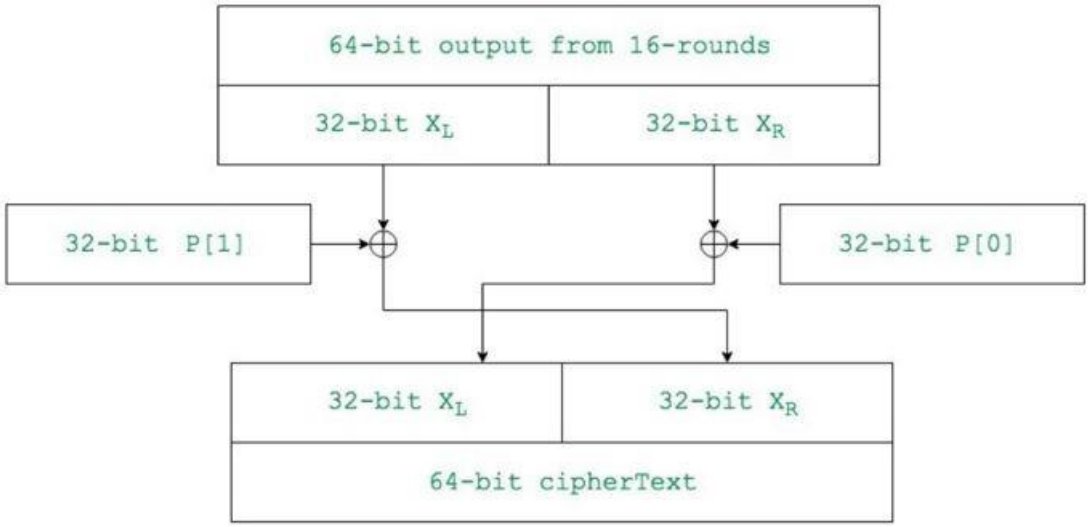


*Figure 14 organigramme de l'étape de post-traitement*

**Décryptage**

Le processus de décryptage est similaire à celui du cryptage et les sous-clés sont utilisés en sens inverse {P [17] – P [0]}. L'ensemble du processus de décryptage peut être élaboré comme suit :

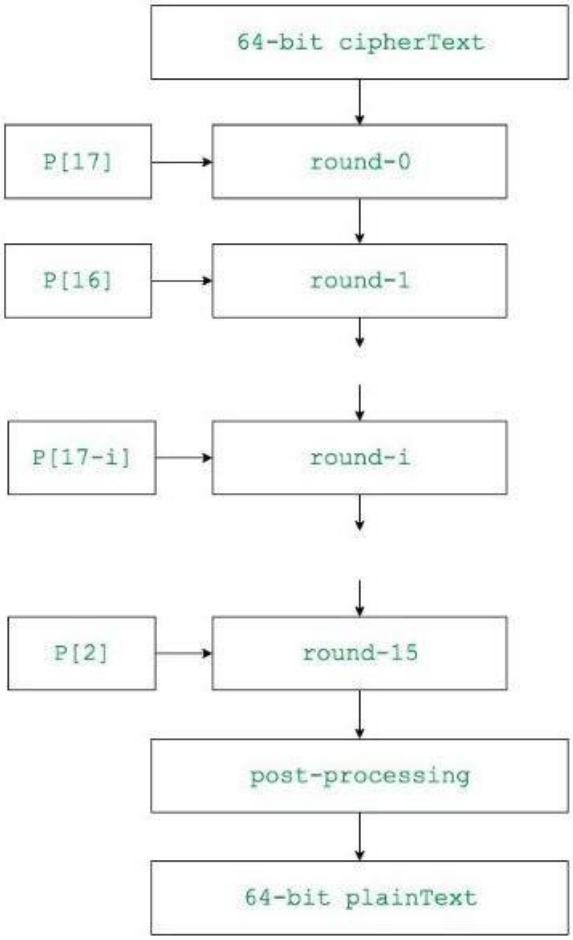


*Figure 15 Dechiffrement*

Voyons chaque étape une par une :

**Étape 1** : génération des sous-clés :

18 sous-clés {P[0]…P[17]} sont nécessaires dans le processus de déchiffrement.

Ces 18 sous-clés sont stockées dans un tableau P, chaque élément du tableau étant une entrée de 32 bits.

Il est initialisé avec les chiffres de pi (0=<i<18).

La représentation hexadécimale de chacune des sous-clés est donnée par :

P[0] = "243f6a88"

P[1] = "85a308d3"

.

.

.

P[17] = "8979fb1b"

Remarque : Voir chiffrement pour les valeurs initiales de P-array.

Maintenant, chacune des sous-clés est modifiée par rapport à la clé d'entrée comme :

P[0] = P[0] xou 1er 32 bits de la clé d'entrée

P[1] = P[1] xou 2ème 32 bits de la clé d'entrée

.

.

.

P[i] = P[i] xor (i+1)ème 32 bits de la clé d'entrée

(passez au 1er 32 bits en fonction de la longueur de la clé)

.

.

.

P[17] = P[17] xou 18e 32 bits de la clé d'entrée

(roulez sur les 32 premiers bits en fonction de la longueur de la clé)

Le tableau P résultant contient 18 sous-clés qui sont utilisées pendant tout le processus de chiffrement

**Etape 2** : initialiser les Boîtes de Substitution :

4 boîtes de substitution (boîtes S) sont nécessaires{S[0]…S[4]} à la fois dans le processus de cryptage et de décryptage, chaque boîte S ayant 256 entrées{S[i][0]…S[i][ 255]} où chaque entrée est de 32 bits.

Il est initialisé avec les chiffres de pi(?) après avoir initialisé le P-array.

**Étape 3** : Décryptage :

La fonction Déchiffrement se compose également de deux parties :

Tours : le décryptage consiste également en 16 tours, chaque tour (Ri) (comme expliqué ci-dessus) prenant en entrée le cipherText (C.T.) du tour précédent et la sous-clé correspondante (P[17-i]) (c'est-à-dire que pour le décryptage, les sous-clés sont utilisées dans inverse).

Post-traitement : la sortie après les 16 tours est traitée comme suit :

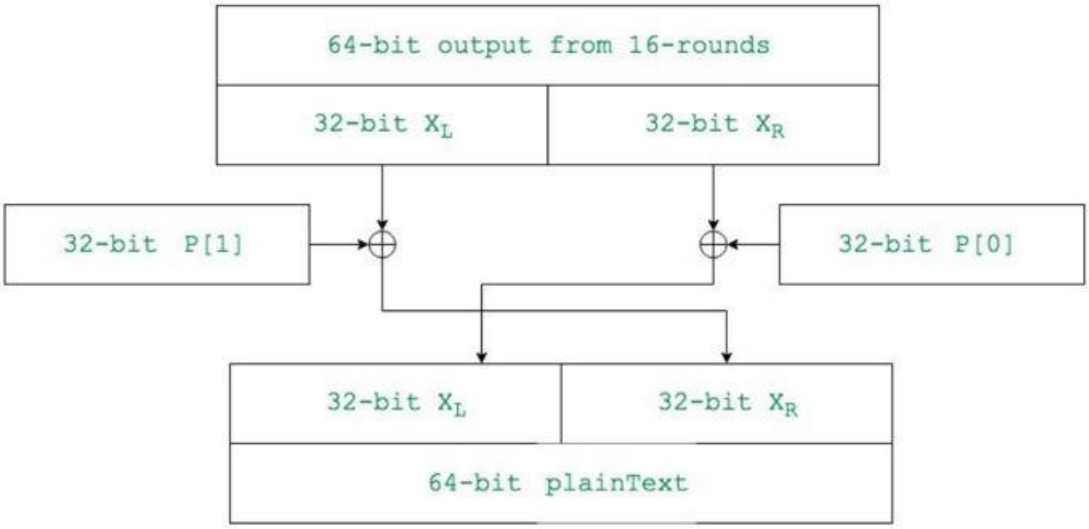


*Figure 16 organigramme de l'étape de post-traitement*

### 2.2.2 Avantages du blowfish :

L'un des chiffrements par blocs les plus rapides et les plus compacts d'usage public, Blowfish utilise une clé de chiffrement symétrique pour transformer les données en texte chiffré. Près de trois décennies après son premier développement, Blowfish est encore largement utilisé car il offre les avantages suivants :

Beaucoup plus rapide et plus efficace que les algorithmes DES et IDEA ;

Non breveté et peut être librement utilisé par n'importe qui, même sans licence ;

Malgré la phase complexe d'initialisation avant chiffrement, le processus de chiffrement des données est efficace sur les gros microprocesseurs ;

Fournit une sécurité étendue pour les logiciels et les applications développés en Java ;

Fournit un accès sécurisé aux outils de sauvegarde ; et prend en charge l'authentification sécurisée des utilisateurs pour l'accès à distance. [8]

### 2.2.3 Inconvénients du Blowfish

L'utilisation de Blowfish pour le chiffrement présente certains inconvénients, notamment les suivants :

La vitesse est affectée lors du changement de clé.

Le calendrier clé prend beaucoup de temps.

La petite taille de bloc de 64 bits rend l'algorithme vulnérable aux attaques d'anniversaire, une classe d'attaques par force brute.

Chaque nouvelle clé nécessite un prétraitement équivalent à 4 Ko de texte, ce qui nuit à sa rapidité, la rendant inutilisable pour certaines applications.[8]

### 2.2.4 Applications du Blowfish

Blowfish convient à une large gamme d'applications, notamment :

Cryptage en masse

Génération aléatoire de bits

Cryptage des paquets

Hachage et gestion des mots de passe

Processeurs mobiles

Cryptage des e-mails, des fichiers ou des disques

Sauvegarde de données

Enveloppe de protection

Blowfish est utilisé par de nombreux produits populaires, tels que CryptoDisk, PasswordWallet, Access Manager, Symantec NetBackup et SplashID. De nombreuses plateformes de médias sociaux et sites de commerce électronique utilisent également Blowfish pour protéger les données des utilisateurs.[8]

## 2.3 Algorithme de chiffrement 3-way :

En cryptographie, 3-Way est un chiffrement par bloc conçu en 1994 par Joan Daemen. Il est étroitement lié à BaseKing ; les deux sont des variantes de la même technique de chiffrement générale.

3-Way a une taille de bloc de 96 bits, notamment pas une puissance de deux comme les 64 ou 128 bits les plus courants. La longueur de la clé est également de 96 bits. Le chiffre 96 provient de l'utilisation de trois mots de 32 bits dans l'algorithme, dont dérive également le nom du chiffrement. Lorsque 3-Way a été inventé, les clés et les blocs de 96 bits étaient assez solides, mais les chiffrements plus récents ont un bloc de 128 bits, et peu ont maintenant des clés de moins de 128 bits. 3-Way est un réseau de substitution-permutation à 11 tours.

### 2.3.1 Description de 3-WAY

L'algorithme est simple à décrire. Pour chiffrer un bloc de texte en clair X, nous devons procédés comme suit:

Pour i variant de 0 à n 1, effectuer les opérations suivantes:

X = X XOR Ki

X = theta(X)

X = Pi l (X)

X = gamma(X)

X = Pi - 2(X)

X = X XOR Kn+1

X = theta(X)

Le déchiffrement se fait de la même manière en inversant les bits de l'entrée et ceux de la sortie. Jusqu'à présent, personne n'a réussi à cryptanalyser 3-WA y. L'algorithme n'est pas breveté. [9]

### 2.3.2 Implémentation de l'algorithme 3 WAY

Cet algorithme manipule des blocs de 96 bits avec une clé de taille égale.

Les fonctions qu'il utilise sont les suivantes:

- theta(X) est une fonction de substitution linéaire-en substance, un mélange de décalages circulaires et de ou exclusifs.

- $P_{i\_}$ 1(X) et $P_i$_2(X) sont des permutations simples. (Nous avons utilisé des permutations circulaires de 10 et de 1 l'une l'inverse de l'autre).

- gamma(x) est une fonction de substitution non linéaire. (Une telle fonction est facile à réaliser, nous pouvons combiner par exemple par un ou exclusif les 3 mots, l'un par l'inverse du second et combiner le résultat par un " et logique" du troisième).[9]

### 2.3.3 Avantages de 3-way :

3-Way est conçu pour être très efficace sur une large gamme de plates-formes, des processeurs 8 bits au matériel spécialisé, et possède des fonctionnalités mathématiques élégantes qui permettent à presque tout le décryptage d'être effectué exactement dans les mêmes circuits que le cryptage.[10]

### 2.3.4 Inconvénients de 3-way :

3-Way, tout comme son homologue BaseKing, est vulnérable à la cryptanalyse de clé associée. John Kelsey, Bruce Schneier et David Wagner ont montré comment il peut être rompu avec une requête clé associée et environ $2^{22}$ textes en clair choisis.[10]

## 2.4 Conclusion :

Dans ce chapitre j'ai présenté le principe de fonctionnement des deux algorithmes blowfish et

3-way ,leur avantages et inconvenients ainsi que leur domaine d'application

# Chapitre 3 : Notions  basiques sur le son

## 3.1 Introduction :

Le son est une chose familière dans notre vie quotidienne que l'on en oublie souvent la signification physique qui est loin d'être facile à comprendre.

D'un point de vue physique, un son est une énergie qui se propage sous forme de vibrations dans un milieu compressible (dans l'eau, dans l'air, dans les matériaux solides).

Le traitement du son est la branche du traitement du signal qui s'applique aux signaux audio, dans le but notamment d'améliorer la qualité, de les compresser, ou d'extraire de l'information.

Le traitement du signal est la discipline qui développe et étudie les techniques de traitement, d'analyse et d'interprétation des signaux. Parmi les types d'opérations possibles sur ces signaux, on peut dénoter le filtrage, la compression de données, la numérisation, le codage, le chiffrement et la transmission de données.

La science qui étudie les sons s'appelle l'acoustique. La psychoacoustique combine l'acoustique avec la physiologie et la psychologie, pour déterminer la manière dont les sons sont perçus et interprétés par le cerveau.

Dans ce chapitre, je vais présenter les notions de base de traitement de son.

## 3.2 Définition de son [11]

Le son est une onde produite par la vibration mécanique d'un support fluide ou solide et propagée grâce à l'élasticité du milieu environnant sous forme d'ondes longitudinales. Par extension physiologique, le son désigne la sensation auditive à laquelle cette vibration est susceptible de donner naissance.

Lorsqu'on jette une pierre dans l'eau, on peut facilement observer le phénomène de propagation des ondes à la surface:

*Figure 17 la propagation des ondes a la surface*

Lors de la diffusion d'un son dans un concert, c'est l'air qui permet sa transmission jusque nos oreilles. De même que l'exemple de l'eau illustrée ci-dessus, les molécules d'air transmettent 'énergie et son donc un support pour le son.

- **Emission, Propagation, Réception**

Pour qu'un son soit émis, une énergie doit avant tout mettre en mouvement un corps pour produire une vibration. Ainsi, le muscle du larynx, la chute d'un objet sur le sol, ou la tension électrique dans un haut-parleur, provoqueront l'énergie nécessaire pour produire cette vibration. Ensuite, pour que ce son puisse se propager, il faut un milieu élastique favorable à la transmission de la vibration. En créant des surpressions ou des dépressions, l'air permet la propagation de l'onde. Les matériaux solides ont aussi cette capacité de transmettre le son. Dans le vide par contre, aucun son ne peut se propager, car il n'y a aucun de support. Enfin, pour être perçue, il doit y avoir un récepteur sensible. Chez l'homme, l'oreille possède une membrane (le tympan) capable de transmettre les informations de vibration en signaux nerveux jusqu'au cerveau, grâce au nerf auditif. De même, le microphone possède également une membrane permettant de transformer les déplacements de l'air en signaux électriques.


*Figure 18 l'émission, la propagation et la réception du son*

## 3.3 Caractéristiques du son [12]

Comme tout phénomène vibratoire, le son peut être analysé comme un signal qui varie dans le temps. Les caractéristiques essentielles sont l'amplitude et la fréquence.

### 3.3.1 L'amplitude

La première caractéristique d'un son est son amplitude. Appelée aussi intensité ou volume sonore, c'est l'expression de la pression de l'air qui se mesure en décibels (dB). 0 dB correspond au minimum que l'oreille humaine puisse percevoir (seuil d'audibilité). Attention, une augmentation de 3db multiplie la puissance par deux!

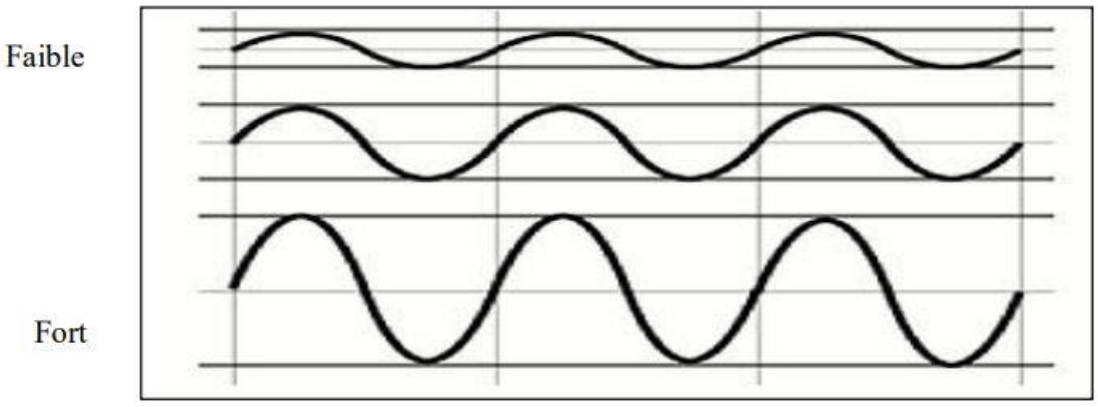


*Figure 19 L'évolution de l'amplitude sonore dans le temps.*

**Exemple concret:**

- De 0 à 10 dB : Seuil d'audibilité, Désert

- De 30 à 40 dB : forêt

- De 60 à 70 dB : sonnerie de téléphone

- De 80 à 90 dB : tondeuse à gazon, klaxon de voiture

- 120 dB : seuil de la douleur, avion au décollage

- 180 dB : décollage de la fusée Ariane, lancement d'une roquette

### 3.3.2 Fréquence

La fréquence, exprimée en Hertz (Hz), est le nombre de répétition d'une période par seconde. Plus elle est élevée et plus le son paraîtra « aiguë », à l'inverse, il paraîtra « grave ». En musique, la fréquence définit donc la hauteur d'un son, soit, la note. (Ex: la note « LA » correspond à 440Hz, soit 440 vibration en une seconde).

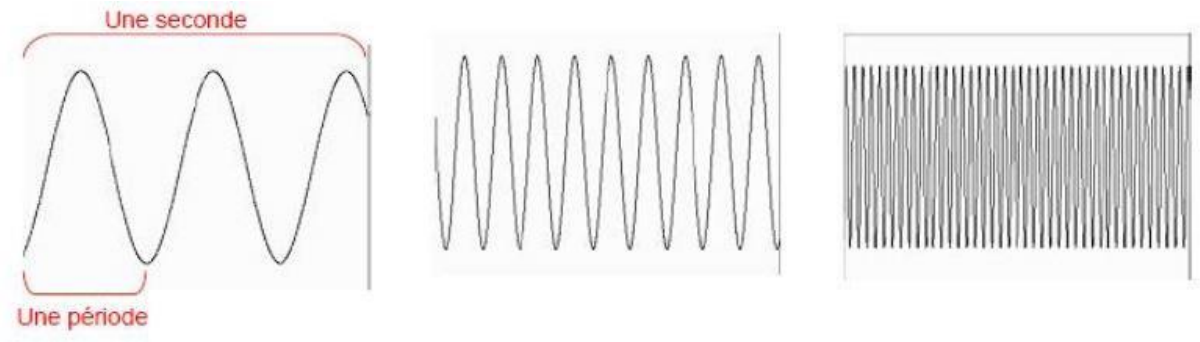


*Figure 20 les types de fréquence*

## 3.4 De l'analogique au numérique [13]

### 3.4.1 Le son analogique : un signal continu

Lorsqu'on capte un son à partir d'un microphone, ce dernier transforme l'énergie mécanique (la pression de l'air exercée sur sa membrane), en une variation de tension électrique continue. Ce signal électrique dit « analogique » pourra ensuite être amplifié, et envoyé vers un haut parleur dont la fonction est inverse: transformer à nouveau le signal électrique en une énergie mécanique (on peut observer le déplacement de la membrane d'un haut parleur en marche).

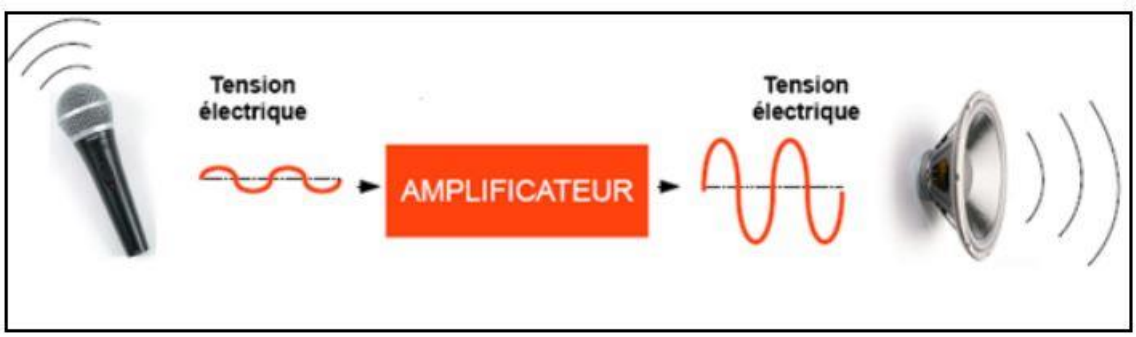


*Figure 21 L'exemple d'une chaîne analogique.*

Le son analogique est généralement fixé sur des supports comme les bandes magnétiques, disques vinyles etc. Le problème rencontré par ces supports réside dans l'usure physique des informations au cours de leur utilisation (lecture/écriture). A terme, le signal est affaibli et peut disparaitre.

### 3.4.2 Le son en numérique: un signal discontinu

Avec l'informatique, lorsque ce même signal électrique est capturé à partir du micro, il est converti en une suite de nombre, on parle alors de numérisation du signal. C'est la carte son qui s'en charge, elle contient des entrées (convertisseurs analogique vers numérique) et des sorties (convertisseurs numérique vers analogique).

La première phase appelée numérisation consiste donc à passer d'un signal continu (une variation de tension électrique) en une suite de valeurs mesurées à intervalles réguliers, donc discontinu.

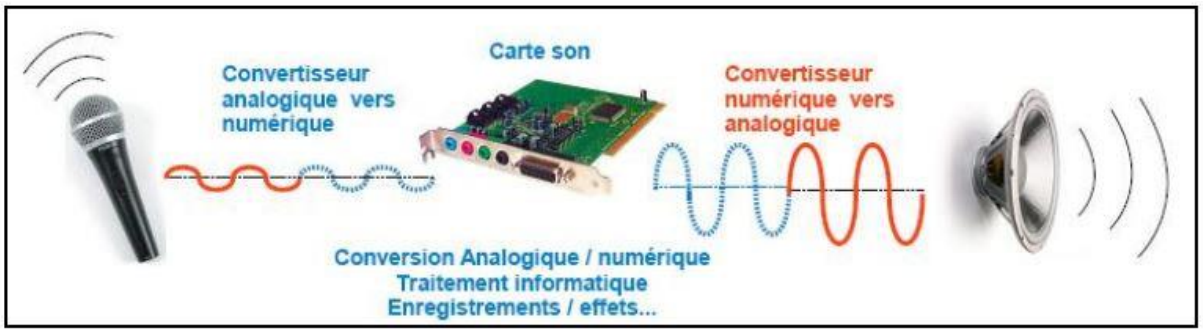


*Figure 22 Exemple d'une chaîne numérique*

L'avantage du numérique, est la possibilité de lire et de dupliquer autant de fois ce signal sans aucune détérioration, puisqu'il a été réduit en une suite de nombres stockée dans un fichier informatique! Cela dit, la compression audio comme le MP3 peut provoquer une perte volontaire du signal afin d'économiser de l'espace de stockage.

- **La fréquence d'échantillonnage**

Échantillonner un signal audio analogique revient à prélever ses valeurs de tension électrique un certain nombre de fois par seconde. La fréquence de ces prélèvements est appelée fréquence d'échantillonnage .La fréquence d'échantillonnage est fixée avant l'opération de numérisation et ne varie pas pendant la numérisation. Les fréquences d'échantillonnage couramment utilisées en audio sont 44100Hz et 48000Hz. Elles sont souvent imposées par des contraintes technologiques. Par exemple, la norme du disque compact audio (CD audio) impose une fréquence d'échantillonnage de 44100Hz.

L'échantillonnage est effectué par découpage temporel du signal audio analogique. Ce découpage temporel permet de reconstruire en données chiffrées la forme d'onde du signal numérisé. La numérisation ne repose que sur des séries de 0 et de 1 : il s'agit d'un codage binaire.

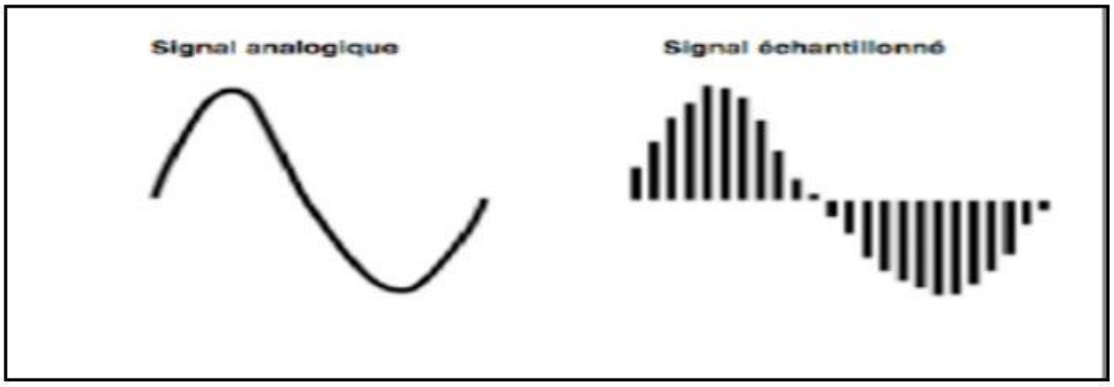


*Figure 23 Echantillonnage d'un signal audio*

### ❖ La quantification

Alors que l'échantillonnage opère un découpage temporel, l'opération de quantification crée une échelle de valeurs discrètes permettant d'attribuer à chaque échantillon une valeur d'amplitude. La quantification s'exprime en « bit » (un acronyme de binary digit). Les valeurs couramment utilisées en audio sont 16bit et 24bit.

L'amplitude de chaque échantillon doit impérativement prendre l'une des valeurs définies par l'échelle de quantification. Si la valeur d'amplitude de l'échantillon se situe entre deux paliers de l'échelle de quantification, elle est approximée au palier le plus proche. Cette approximation induit une erreur que l'on nomme « erreur de quantification ».

Par suite, plus le nombre de bits est élevé, plus le nombre de paliers est important et l'erreur de quantification faible. Autrement dit, les petites variations d'amplitude du signal échantillonné sont d'autant mieux approximées que la résolution de la quantification est élevée.

La fidélité de la forme d'onde numérisée à la forme d'onde du signal analogique dépend donc de la résolution (exprimée en bit) et de la fréquence d'échantillonnage (exprimée en kHz).

De même que pour la fréquence d'échantillonnage, le choix de la résolution de la quantification est soumis à des contraintes techniques.

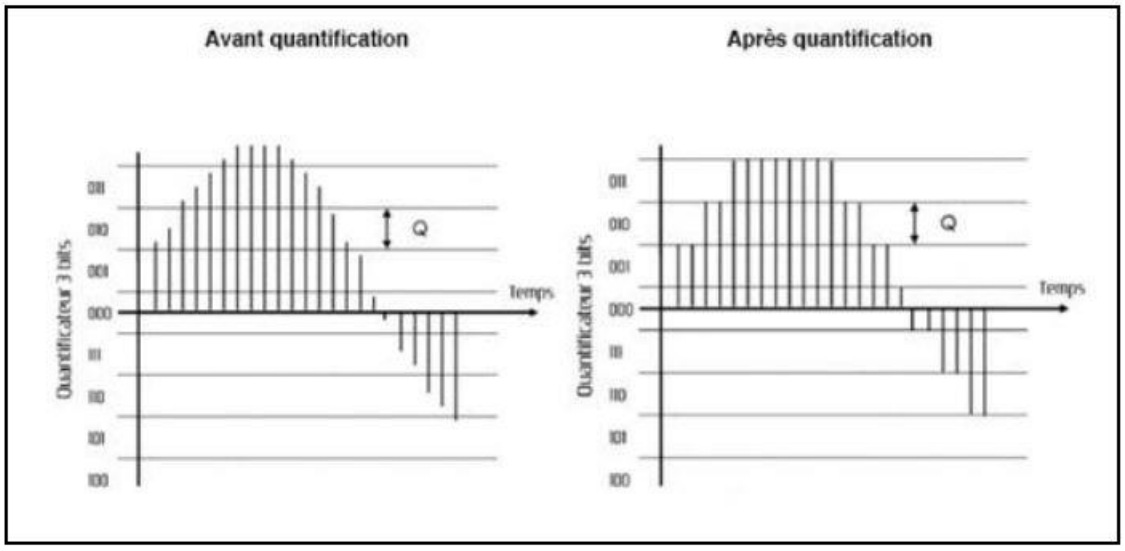


*Figure 24 signal échantillonné avant et après quantification*

- La compression du signal audio numérisé

Un signal audio numérisé est stocké sur des disques durs, des disques compacts, des DVD… La nature de l'information qu'ils contiennent rend ces fichiers relativement volumineux. L'intérêt de la compression de stockage limitée (ex : baladeur mp3).

Les techniques de réduction de débit sont déjà très largement employées dans les domaines du cinéma et de la radio, via le câble, le satellite.

✓ Les algorithmes de compression

Un algorithme est l'énoncé d'une suite d'opérations permettant de donner la réponse à un problème.

Dans le cas de la compression, l'algorithme a pour fonction de réduire la taille d'un fichier selon un certain nombre de contraintes que le programmeur spécifie. Par exemple, une des contraintes peut être de conserver toutes les fréquences inférieures à 20kHz afin de limiter les pertes de qualité sonore dans la zone audible du spectre.

Lors de l'étape de compression et de décompression d'un flux audio ou vidéo, on utilisera des algorithmes spécifiques rassemblés sous le terme commun de « CoDec ».

Un codec est constitué de deux éléments :

• le CODeur contient un algorithme destiné à coder l'information. Dans le cas de la compression ce sera pour effectuer une réduction du poids des données ;

• le DECodeur contient un algorithme destiné à décoder l'information. Dans le cas de la compression ce sera pour reconstruire un signal audionumérique.

- ✓ Le taux de compression

Compresser revient à réduire le débit du flux audio et/ou vidéo. Les algorithmes sont adaptés en fonction des applications (diffusion internet, télévision, cinéma) pour répondre aux besoins de chacun des médias. La réduction de débit (ou compression) s'exprime généralement sous la forme d'un taux dit « taux de compression ». Le taux de compression peut s'énoncer comme suit :

- soit comme le rapport entre le volume initial des données et le volume après réduction. Si le volume de données est deux fois plus faible après réduction (passant de 10Mo à 5Mo par exemple), on écrira qu'il s'agit d'un taux de 2:1 ;

- soit en pourcentage du volume après réduction par rapport au volume initial. Si le volume de données est deux fois plus faible après réduction, on écrira qu'il s'agit d'un taux de 50%. Il existe par ailleurs deux types de compressions : la compression « destructive » et la compression« non destructive ».

## 3.5 Format de fichier audio [14]

Un format de fichier audio est un format de données utilisé en informatique pour stocker des sons, (de la musique, des voix, etc.) sous forme numérique. De nombreux standards existent; certains s'appliquent à la production, au stockage et à la diffusion, d'autres (ceux qui utilisent des algorithmes de compression de données ou de débit), sont destinés, en principe, uniquement à la diffusion. Actuellement, le format le plus utilisé est de loin le mp3, suivi du wma, et de l'aac.

### 3.5.1 Caractéristique des formats audio [15]

Les formats audio varient selon :

1. Le nombre de canaux sonores encodés.

2. Le nombre d'échantillons par seconde avec lequel on découpera numériquement, pour chaque canal, une onde sonore ou un signal électrique.

3. La résolution donnée à chaque échantillon et la grandeur physique qu'on lui donne.

4. l'application d'une compression ou non.

Chaque format audio présente aussi des caractéristiques découlant de l'algorithme de compression/décompression, ou codec (ou « codage-décodage » - COde-DECode en anglais), qu'il utilise ou non. Après la numérisation du son, le format utilisé est inscrit dans l'extension du fichier de données qui en stocke la transcription. Chaque format se caractérise aussi par sa propension à inclure et gérer des Métadonnées.

Dans un format donné, les fichiers peuvent être déclinés en plusieurs échelles de quantification (8, 16 ou 24 bits) avec différentes fréquences d'échantillonnage (p. ex. 22.05, 44.1, 48, 88.2 ; 96, 176.4, 192, kilohertz) appliqués à un certain nombre de voies (monophonique, stéréophonique).

Le nombre de canaux sonores peuvent être réels et séparés, ou mélangés discrètement aux signaux principaux; ils seront décodés et restitués par la suite à l'aide d'algorithmes spécifiques.

## 3.5.2 Types de formats

### *3.5.2.1 Les formats audio compressés avec perte*

La compression audio avec perte (lossy) se base sur des algorithmes spécialisés pour déterminer quelles transformations simplifient la représentation du son tout en étant perçue quasiment de la même manière par l'oreille humaine. Elle diminue la taille du fichier en éliminant les nuances perçues comme les moins utiles. L'élimination est définitive, créer un fichier dans un format de haute qualité à partir d'un fichier compressé avec perte ne sert strictement à rien.

Le format le plus connu est le MPEG-1/2 Audio Layer 3, dont le suffixe est .mp3. Ce format propose une qualité sonore très correcte pour un débit de 128 kbit/s. C'est ce format qui a été massivement utilisé pour transférer les musiques via internet dès la fin des années 1990. Rapidement, des baladeurs avec une mémoire réenregistrable et capables de lire directement ce format sont apparus.

Dans la décennie 2000, de nouveaux formats ont été proposés. Vu les progrès des algorithmes, ils surpassent largement le MP3 en termes de qualité à débit égal, et peuvent atteindre des qualités supérieures. De plus, certains sont moins contraignants que le MP3 quant aux droits d'utilisation (le Ogg est un format libre).

Mais le MP3 reste le plus utilisé, car l'arrivée en continu de nouveaux formats, apportant un avantage assez faible par rapport aux précédents, ne permet pas de mettre en place un standard meilleur que le MP3 et lisible par tous les baladeurs. En particulier, le fait que les iPod d'Apple ne lisent que le MP3 et l'AAC freine assez fortement les initiatives dans ce domaine.

Pour un même format de compression, il n'y a pas de manière unique de coder, car chaque algorithme cherche la meilleure manière de représenter le son d'origine suivant le langage de compression. En particulier, les codecs de MP3 ont réalisé des progrès très importants depuis le début de l'utilisation de ce format.

Elle permet typiquement un gain d'un facteur 10 de taille du fichier. Cela a rendu possible non seulement le stockage d'un temps d'écoute formidable sur les supports informatiques, mais aussi leur échange par Internet, souvent illégalement.

- AC3

Officialisée en 1992, la compression AC3 permet d'utiliser jusqu'à 6 canaux sonores indépendants avec un taux d'échantillonnage de 32, 44,1 ou 48 kHz et avec un taux de transfert allant de 32 à 640 kbit/s. Le Dolby Digital utilise ce principe de codage, c'est pourquoi on le désigne souvent sous ce nom. Format très courant dans les DVD.

- MP3

MP3 est l'abréviation de MPEG-1/2 Audio Layer 3. Cet algorithme de compression prend naissance en 1987. L'ISO en fera un standard dans les années 92-93. La couche (Layer) III est la couche la plus complexe. Elle est dédiée à des applications nécessitant des débits faibles (128 kbit/s) d'où une adhésion très rapide du monde Internet à ce format de compression. Les taux de compression (ratio) sont d'ordinaire de 1 pour 10 (1:10) (1:4 à 1:12). Très rapide à l'encodage. Des royalties importantes sont à payer pour exploiter la licence MP3.

Utiliser l'encodeur MP3 LAME dernière version, encodé à 130 kbit/s (V5) permet d'obtenir une qualité comparable au AAC (Advanced Audio Coding) encodé à 48 kbit/s.

Le suffixe des fichiers créés est .mp3

Type de compression : constant ou variable (VBR).

- mp3PRO

Le format mp3PRO, fruit de la collaboration entre Thomson Multimédia et l'Institut Fraunhofer, combine l'algorithme MP3 et un système améliorant la qualité des fichiers comprimés appelé (en)SBR pour Spectral Bandwidth Replication. Ce format a été publié à la fin de 2001; un fichier MP3pro 64 kbit/s a une qualité équivalente à celle d'un MP3 à 128 kbit/s. Le suffixe des fichiers créés est .mp3

- Ogg Vorbis

Le format Ogg Vorbis est un format libre, fruit de la fondation Xiph.org. Vorbis se différencie des MP3, WMA et autre AAC par son algorithme. Il segmente les sources audio en paquets successifs, l'algorithme de compression agissant dans un premier temps sur chaque paquet indépendamment des autres. Cela lui permet d'avoir très peu de faiblesses sur certaines fréquences et de conserver la même qualité quel que soit le type de musique.

Le suffixe des fichiers créés est .ogg ou parfois .oga.

Par abus de langage, on appelle 'fichier Ogg' des fichiers musicaux compressés par l'algorithme Vorbis. Ceci peut être particulièrement dérangeant à l'ère des baladeurs numériques supportant audio et vidéo. En fait, Ogg est un conteneur qui peut contenir des pistes sonores (Vorbis), audio sans perte (FLAC), audio parlées (Speex) et vidéo (Theora). Un 'fichier Ogg' peut donc contenir l'un ou l'autre (ou une combinaison) de pistes. Pour être plus clair, nous devrions parler de fichier Ogg Vorbis lorsque nous mentionnons un fichier. Ogg qui ne contient qu'une piste sonore au format Vorbis.

- WMA

Le format WMA (Windows Media Audio), créé par Microsoft à partir des recommandations MPEG-4 en 1999, est utilisé par le logiciel Windows Media Player. Ce format est lié à une gestion pointue des droits d'auteurs (Gestion numérique des droits, en anglais Digital Right Management ou DRM) qui permet de définir par exemple une durée de vie limitée pour les fichiers ou d'interdire les possibilités de gravure.

Il existe plusieurs versions du codec (wma7.1, wma9, wma pro).

Le suffixe des fichiers créés est .wma

- AU

Le format AU est assez bien répandu grâce à Unix et Linux. La fréquence d'échantillonnage est comprise entre 1 kHz et 200 kHz. Mais les applications de rendu audio ne lisent principalement que trois fréquences d'échantillonnage : 8012.821 (codec entré), 22050 et 44100 hertz.

Le suffixe des fichiers créés est .au

Les résolutions 8, 16, 20, 24 et 32 bits (flottant) sont acceptées.

#### *3.5.2.2 Les formats audio compressés sans perte*

La compression sans perte (lossless) signifie qu'on utilise un algorithme tel qu'on peut toujours retrouver les données d'origine. Dans l'absolu, il existe toujours un fichier d'origine tel que l'algorithme ne ferait pas gagner d'espace disque.

Typiquement, la compression sans perte permet de diviser la taille des fichiers par deux ou trois. Elle est relativement peu utilisée, car ce gain est très faible en comparaison de ceux permis par la compression avec perte (ce qui est un gros handicap pour les échanges de fichiers), et assez gourmande en temps de calcul. Aucun standard n'a donc suffisamment convaincu pour devenir universellement lisible.

- ATRAC

L'ATRAC (Adaptive Transform Acoustic Coding) est une technique de compression audio avec et sans pertes développée par Sony en 1992. Ce format a subi plusieurs évolutions : ATRAC3, ATRAC3plus (familièrement écrit ATRAC3+) et ATRAC Advanced Lossless se sont succédé respectivement en 1999, 2002 et 2006.

- FLAC

Le format FLAC (Free Lossless Audio Codec), est un format libre de compression audio sans perte. Maintenu par la fondation Xiph.org, il est apprécié pour conserver la qualité des fichiers sonores originaux en alternative aux formats de compression avec perte type MP3.

#### *3.5.2.3 Les formats audio sans compression*

Il existe un format audio non compressé, PCM, qui est généralement stocké sous forme de WAV sur Windows ou sous .Aiff sur Mac OS. WAV et AIFF sont des formats de fichiers flexibles conçus pour stocker plus ou moins n'importe quelle combinaison de taux d'échantillonnage ou de bitrates (bit rate). Ce sont les formats de fichier appropriés pour le stockage et la réalisation d'enregistrements originaux.

- RAW

RAW (Real Audio Wrapper) est un format audio utilisé pour représenter les données de son en modulation d'impulsion codée sans en-tête ni métadonnées.

- WAV

Le format WAV (ou WAVE),(WAVEform audio format) est une extension de fichiers audio, il s'agit d'un conteneur capable de recevoir des formats variés. Il est basé sur le format de fichier RIFF, lequel est semblable au format IFF.

Mono ou stéréo, il a été mis au point par Microsoft et IBM.

Le suffixe des fichiers créés est .wav

- BWF

Le BWF (Broadcast Wave Format) est un format audio standard créé par l'European Broadcasting Union en tant que successeur du WAV. Le BWF permet de stocker des

métadonnées dans le fichier. Voir European Broadcasting Union : Spécification du Broadcast Wave Format (EBU Technical document 3285, juillet 1997). Il s'agit du format d'enregistrement usuel utilisé dans de nombreuses stations de travail audio professionnel de la télévision et du cinéma. Les Fichiers BWF incluent une référence standardisée Timestamp qui permet et facilite la synchronisation avec un élément d'image distincte.

L'AIFF est un format de stockage de sons sur les ordinateurs de Apple. C'est l'équivalent du format WAV dans le monde Windows.

Les résolutions 8, 16, 20, 24 et 32 bits (à virgule flottante) sont acceptées.

Le suffixe des fichiers créés est .aif

- CAF

Le CAF (Core audio format) a été développé par Apple pour s'affranchir des limitations de conteneur audio plus ancien comme le AIFF ou le WAV. Il est compatible avec le système Mac OS X d'Apple depuis la version 10.3 et est lisible par Quicktime 7.

- CDA

Le CDA (Compact Disc Audio), est un format Microsoft spécifique à Windows, des pistes des CD audio, telles qu'elles apparaissent lorsqu'elles sont insérées dans le lecteur CD-ROM. Les CD audio du commerce répondent à la norme professionnelle "Red Book". La technique d'échantillonnage du son utilisée pour les disques compacts est la modulation d'impulsion codée (en anglais PCM, pour Pulse Coded Modulation).

Le suffixe des fichiers créés est .cda

## 3.6 Conclusion

Depuis la découverte de la synthèse numérique des sons, et avec l'arrivée d'ordinateurs personnels équipés en standard d'une carte son, il est devenu à la portée de tous d'enregistrer et de traiter les sons. De nombreux professionnels se tournent vers des solutions numériques, de moins en moins onéreuses, qui offrent, avec la progression de la capacité des ordinateurs, une foule de possibilités. Dans mon projet de fin d’étude, je suis intéressés par le cryptage des flux audio des vidéos avec un format supporté par la bibliothèque Ffmpeg

# Chapitre 4 :

# Application au cryptage/décryptage du flux vidéo

## 4.1 Introduction :

On va présenter dans ce chapitre, les résultats obtenus de l'implémentation de différents algorithmes de chiffrement Appliqués aux flux audio de différentes vidéos.

Les algorithmes principale de comparaison dans cette partie sont blowfish et 3-way .pour mieux analyser les résultats on a ajouté deux algorithmes simples ou-exclusif et un chiffrement par substitution simple.

Les résultats obtenus permettent de savoir la vitesse de chiffrement et déchiffrement de chaque algorithme ainsi que la qualité de chiffrement en variant les différents paramètres de l'audio.

## 4.2 Présentation de l'environnement et du matériel et outils utilisés:

**Configuration du matériel :**

```
CPU: Dual Core Intel Core i3-3217U (-MT MCP-)
speed/min/max: 798/800/1800 MHz Kernel: 5.13.0-44-generic x86_64 Up: 13m
Mem: 1236.8/3811.6 MiB (32.4%) Storage: 465.76 GiB (19.2% used) Procs: 233
Shell: bash 5.0.17 inxi: 3.0.38
```

*Figure 25 Configuration du matériel*

**Environnement :**
On a developpé notre application dans un environnement linux avec la distribution ubuntu 20.04. On a utilisé le compilateur gcc sous linux pour l'implémentation des algorithmes.

**Spek – Analyseur de spectre acoustique [16]**
aide à analyser vos fichiers audio en affichant leur spectrogramme. Spek est un logiciel gratuit disponible pour Unix, Windows et Mac OS X.

**Bibliotheque Ffmpeg [17]**
FFmpeg est un programme informatique capable d'enregistrer, de convertir et de diffuser de la vidéo et de l'audio numériques dans une variété de formats. Le programme est un outil en ligne de commande composé d'un groupe de bureaux gratuits et open source. Il comprend une bibliothèque appelée LAVC, qui est une bibliothèque de codecs audio et vidéo utilisée par de nombreux projets, ainsi que la bibliothèque libavformat, qui combine et décode les conteneurs audio et vidéo numériques. Le nom du projet vient des caractères "MPEG", un groupe qui établit des normes pour un format vidéo populaire, ainsi que des lettres "FF", qui est une abréviation de "avance rapide".

Le projet a été lancé par Fabrice Bellard (utilisant Gerard Lantau comme pseudonyme), et le projet est maintenant maintenu par Michael Niedermeier. Un certain nombre de développeurs du projet font également partie du projet mplayer et FFMPEG est hébergé sur le serveur de ce même projet.

e programme a été développé sous Linux, mais il peut être traduit sous la plupart des systèmes tels que Mac OS X, Microsoft Windows et Amiga OS. Il prend également en charge la plupart des plates-formes informatiques et des architectures de microprocesseurs telles que x86 (c'est-à-dire-32 et x86-64), PowerPC, la famille de processeurs ERM, DEC Alpha, Spark et MIPS.

La version 0.5 est sortie il y a un certain temps, bien que les développeurs aient toujours conseillé d'utiliser la construction normale à partir du code source trouvé dans le système de contrôle de révision Sub Virgin du projet, car les développeurs essaient de créer et de maintenir un sous-dossier stable. Le programme est publié sous les termes de la licence publique générale GNU et de la licence publique générale limitée GNU (selon les sous-bibliothèques utilisées), le programme est donc gratuit.

Il y a deux encodeurs vidéo et un conteneur numérique vidéo qui ont été inventés dans ce projet lors de son développement. Les deux codecs sont "FFV1" et "Snow codec" qui est la version 1.0 et est toujours en cours de développement, et le contenu numérique est "NUT" et est actuellement en développement intensif.

**Les composants :**

Le projet comprend plusieurs volets, à savoir :

**ffmpeg** est un outil en ligne de commande pour convertir un format vidéo en un autre. Il peut également récupérer et encoder une vidéo à partir d'une carte TV pendant la diffusion.

**ffserver** est un serveur de diffusion en direct utilisé pour diffuser des vidéos en direct, et il peut également usurper l'heure de diffusion en direct pendant un certain temps, le serveur utilise HTTP et le protocole de flux d'informations en temps réel.

**ffplay** est un simple lecteur multimédia basé sur SDL et des bibliothèques de projets.

**libavcodec** est une bibliothèque qui contient tous les encodeurs et décodeurs dont ffmpeg a besoin. La plupart des codecs sont développés à partir de zéro pour garantir des performances optimales et un code réutilisable.

**libavformat** est une bibliothèque qui contient des assembleurs et des diviseurs utilisés dans les conteneurs numériques pour la vidéo et l'audio.

**libavutil** est une bibliothèque d'aide qui contient des plugins pour diverses parties du projet, y compris adler32, test d'itération cyclique, md5, sha1, compression ouverte à partir du format lzo, encodeur/décodeur pour encoder/décoder en base64, encodeur/décodeur pour encoder/décoder en rc4 et Encodage/décodage AES.

**libpostproc** est une bibliothèque d'actions de post-traitement vidéo.

**libswscale** est une bibliothèque qui contient des actions pour ajuster la taille de l'image dans une vidéo.

**libavfilter** est une alternative à la bibliothèque vhook qui permet l'édition et l'inspection vidéo entre l'encodeur et l'encodeur.

**Liste des formats conteneurs audio/vidéo supportés**

AVI

MPEG

ASF

MOV

OGG

Matroska (dont WebM)

WAVE

**Protocoles**

Protocole de transfert hypertexte

RTP

RTSP

TCP

UDP

gopher

**Projets utilisant FFmpeg**

Ce programme est utilisé par de nombreux projets open source tels que VLC, MPlayer, Handbrake, Google Chrome et bien d'autres.

**Frameworks multimédia utilisant FFmpeg**

Spectacle direct / VFW

ffdshow

Quick Time

Perian

Banderole J

J-Streamer

**Statut des codes juridiques**

Le projet comprend plus de 100 encodeurs, la plupart d'entre eux ne sont pas stockés sous forme de données compressées. Les titulaires de brevets peuvent revendiquer au moins tous les codecs qui compriment les informations comme étant leur invention. De telles revendications peuvent être efficaces dans des pays tels que les États-Unis qui ont mis en œuvre des brevets logiciels, mais sont inefficaces dans d'autres pays qui ne les ont pas encore adoptés. De plus, un certain nombre de ces codecs n'ont été émis que dans des conditions empêchant la rétro-ingénierie,

même si c'est à des fins de compatibilité entre les systèmes. Cependant, ces conditions sont rejetées dans de nombreux pays, comme un certain nombre de pays de l'Union européenne.

La plupart des distributions Linux contiennent un ffmpeg raccourci qui contient un certain nombre de codecs pour éviter les complications juridiques, mais le reste des codecs peut être trouvé dans des référentiels non officiels.

## 4.3 Processus de chiffrement/déchiffrement :

1_ Vidéo in

2_ extraction de l'audio utilisant ffmpeg (désignation du format, frequence,bitrate..etc)

3_ lecture des échantillons audio sur 16 bit

4_ chiffrement des échantillons

5_ecriture du fichier chiffré

6_ audio chiffré

7_ fusion de l'audio et la vidéo

8_ Vidéo out

## Vidéos utilisé dans cette étude :

Les vidéos utilisées sont tous de format mp4

Pour une meilleur étude ces vidéos comportent des flux audio tel que : la voie, le son, la voie et le son :

| Video | v1 | v2 | v3 | v4 | v5 | V6 |
|---|---|---|---|---|---|---|
| Audio | A1 | A2 | A3 | A4 | A5 | A6 |
| Taille | 471 Ko | 0.908Ko | 1.55 Mo | 1.61 Mo | 1.64 Mo | 2.89 Mo |

*Tableau 6 les tailles des fichiers audios des videos utilisés*

**Analyse des spectres audio :**

Comparaison entre spectre d'audio clair et celui des audios cryptés :

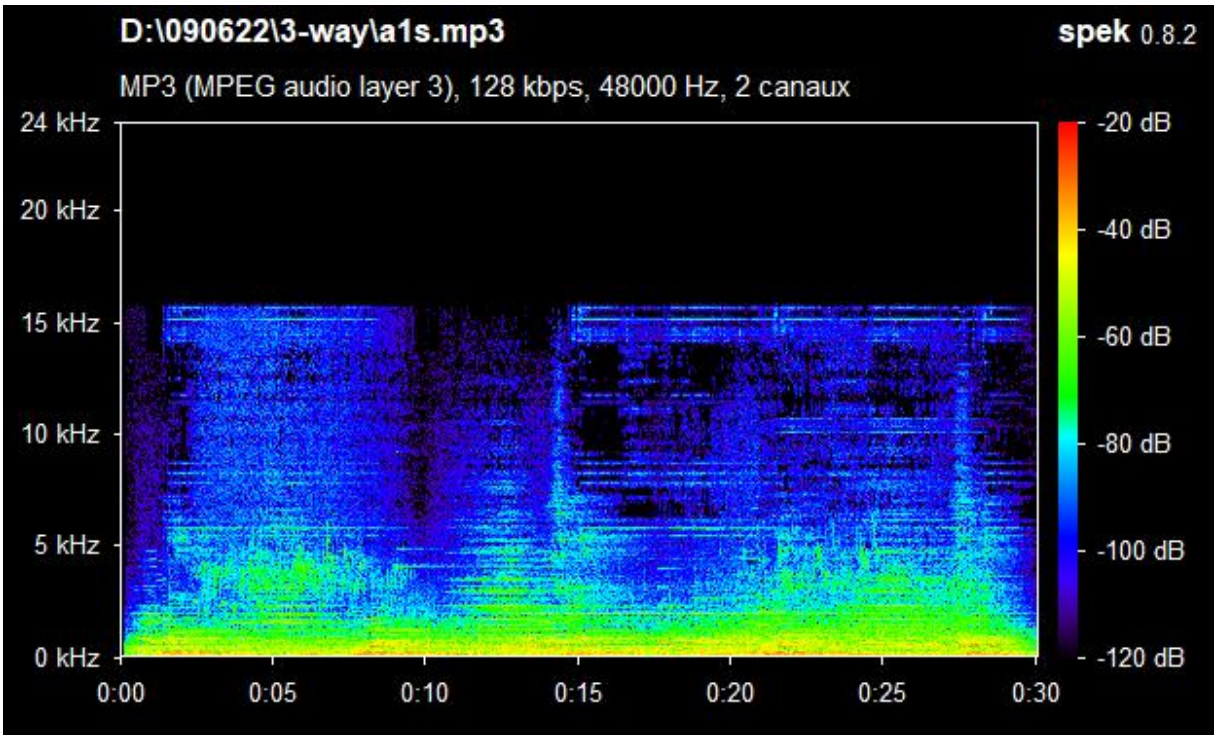


*Figure 26 spectre audio clair*

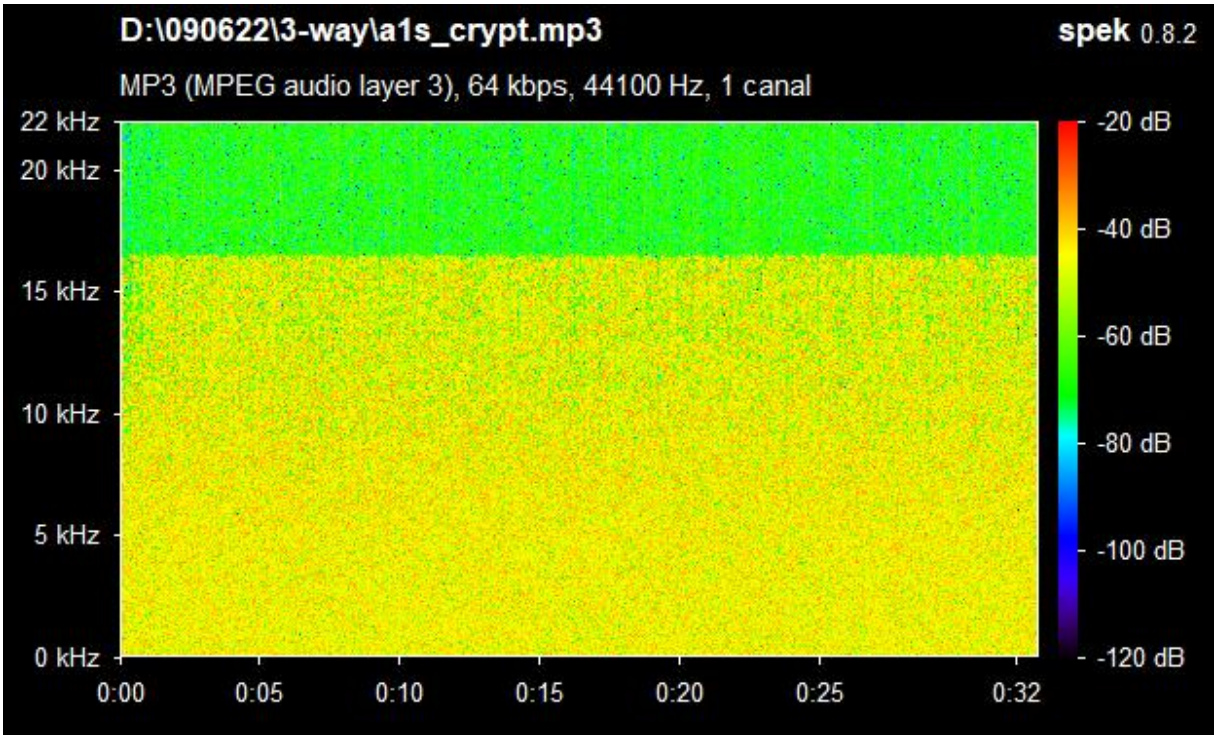


*Figure 27 spectre audio crypté par 3-way*

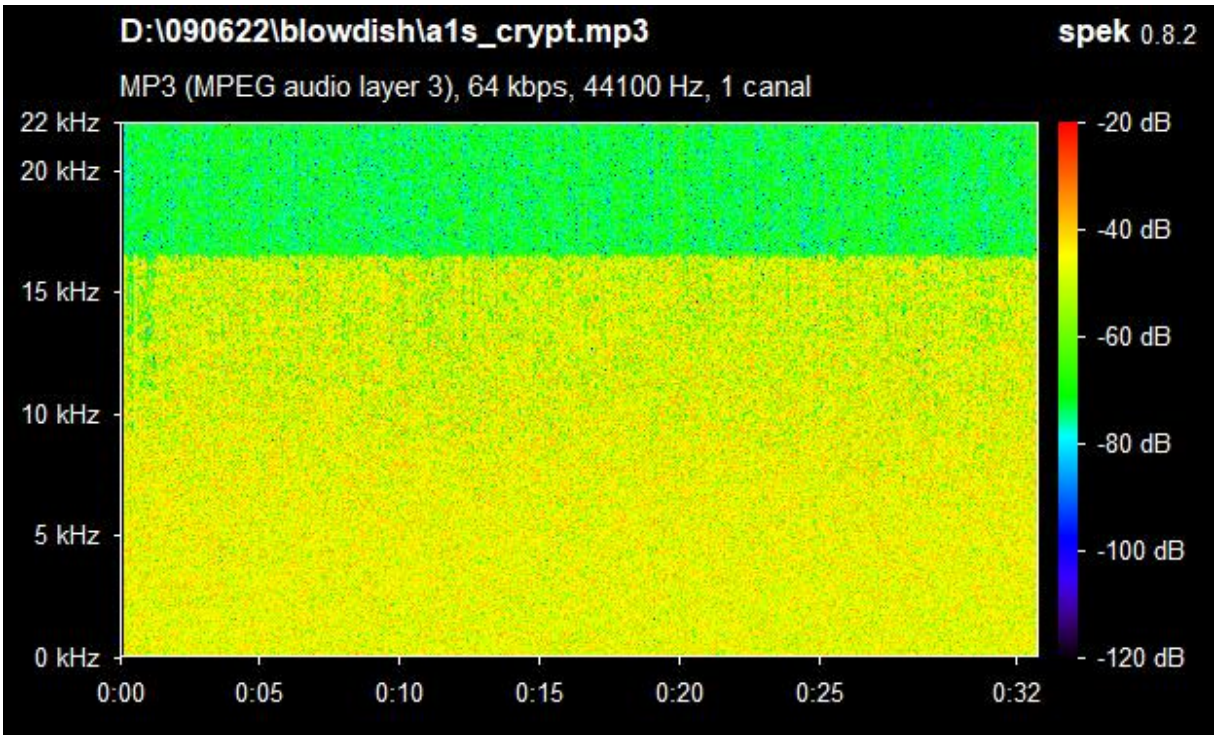


*Figure 28 spectre audio crypté par blowfish*

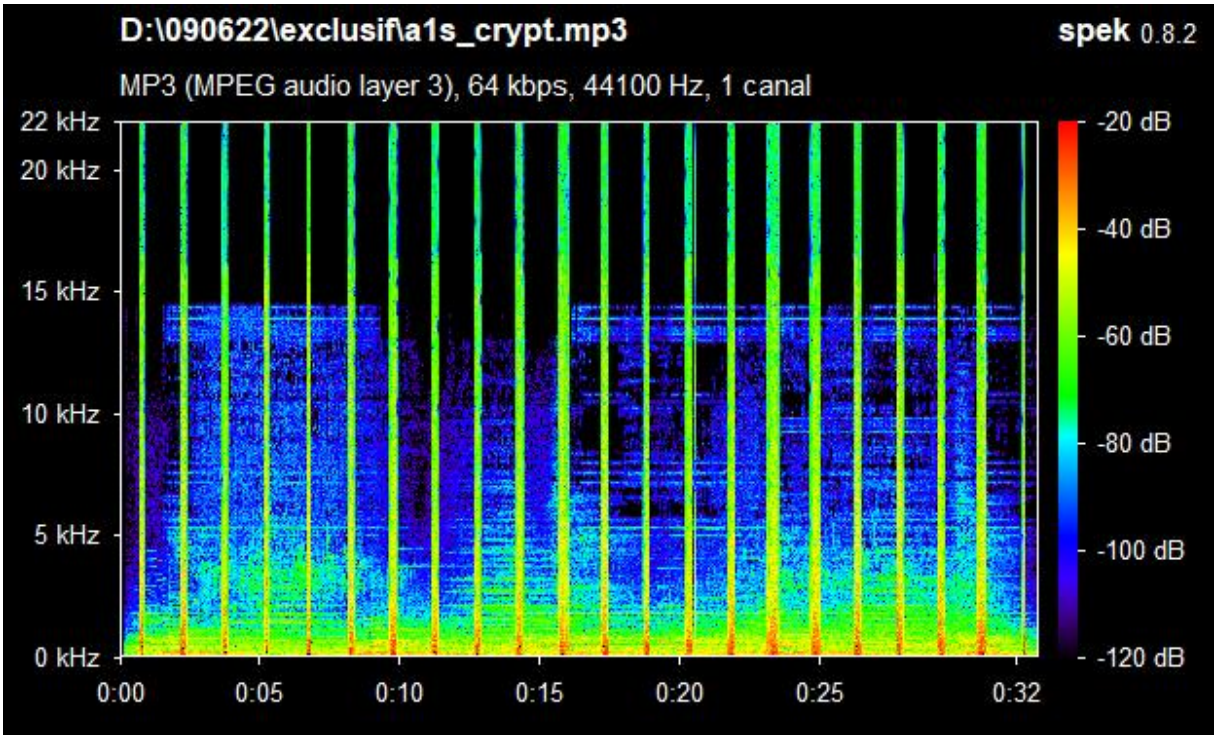


*Figure 29 spectre audio crypté par substitution simple*

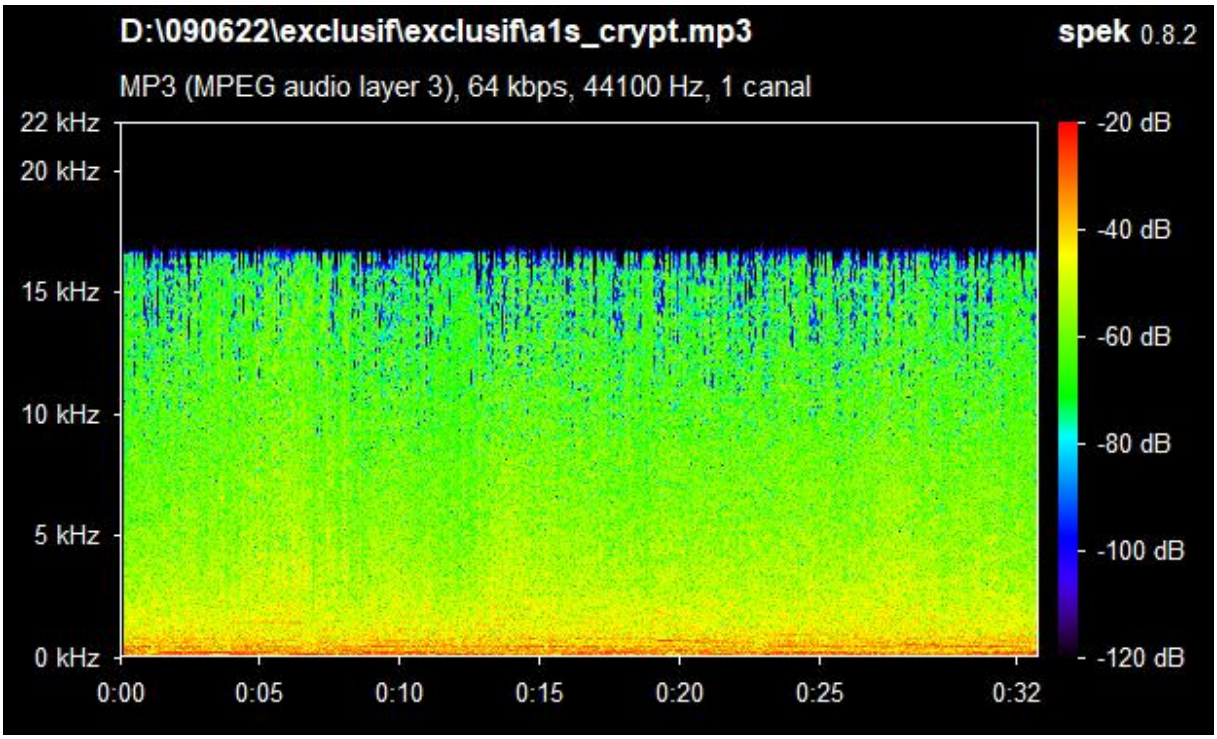


*Figure 30 spectre audio crypté par ou-exclusif*

**Temps de chiffrement :**

| audios \algorithmes | Dacalge simple | Ou-exclusif | 3-way | blowfish |
|---|---|---|---|---|
| A1 0.471 | 0.143198 | 0.160599 | 1.782092 | 565.997762 |
| A2 0.908 | 0.318152 | 0.317248 | 3.363021 | 1083.057306 |
| A3 1.55 | 0.464848 | 0.549225 | 6.501789 | 1501.682531 |
| A4 1.61 | 0.486795 | 0.595259 | 6.535476 | 1753.816119 |
| A5 1.64 | 0.509687 | 0.568268 | 6.621354 | 1947.306009 |
| A6 2.89 | 1.168506 | 0.869012 | 10.927795 | 3538.687074 |

*Tableau 7 résultats temps de chiffrement*

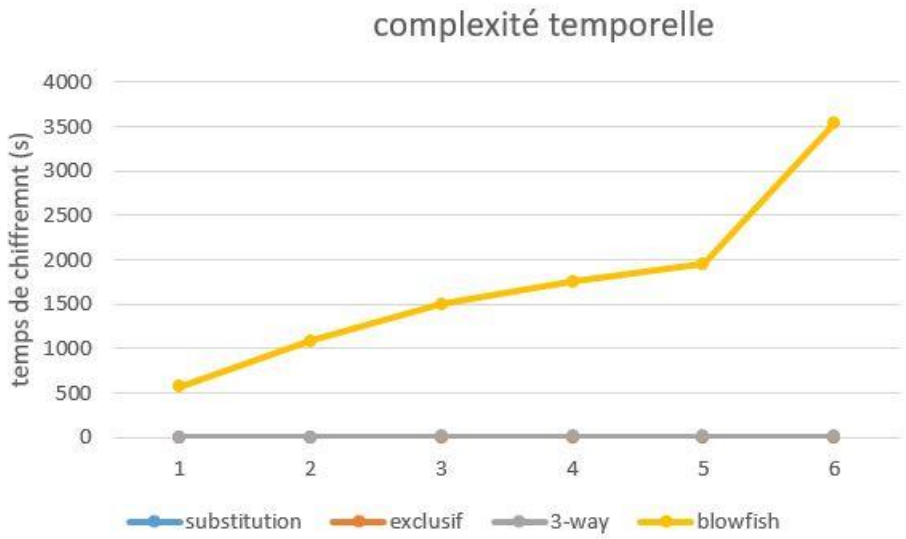


*Figure 31 comparaison de temps de cryptage entre les 4 algorithme*

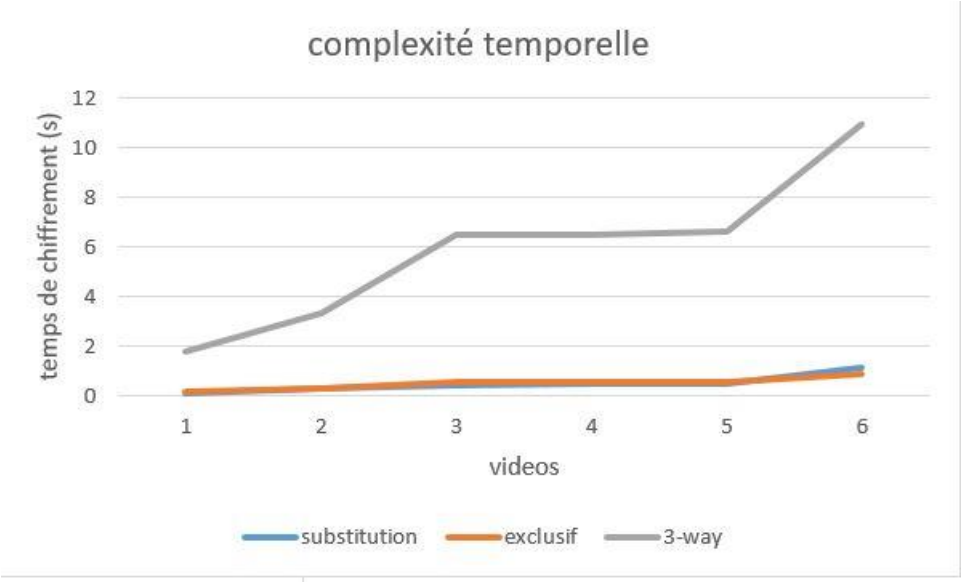


*Figure 32 comparaison de temps de cryptage sans blowfish*

**Analyse des resultats :**

_le premier graphe montre la grande différence de complexité en temps entre le blowfish et les 3 autre algorithmes

_pour le deuxième graphe le 3-way a de plus grande complexité par rapport au ou-exclusif et la substitution qui ont presque la même complexité.

_la complexité temporelle varie proportionnellement à la taille du fichier audio à crypter.

_la vitesse de chiffrement est indépendant de bitrate, format et extension des fichiers audio.

## Dechiffrement :

Les résultats de déchiffrement sont les même que le chiffrement

## Qualité de chiffrement :

L'analyse du spectre audio clair et chiffré nous permet de savoir la qualité chiffrement de chaque algorithme

Pour cela j'ai choisi 3 vidéos ont de contenu audio différents (son,parole,son et parole) :

**Vidéos contenant juste le son :**

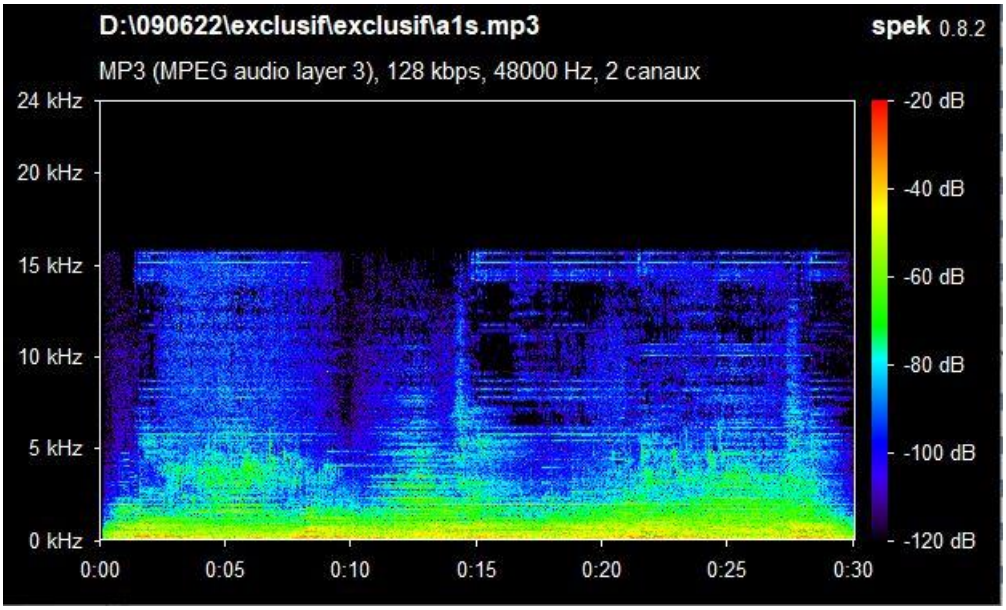


*Figure 33 spectre audio clair comportant juste le son*

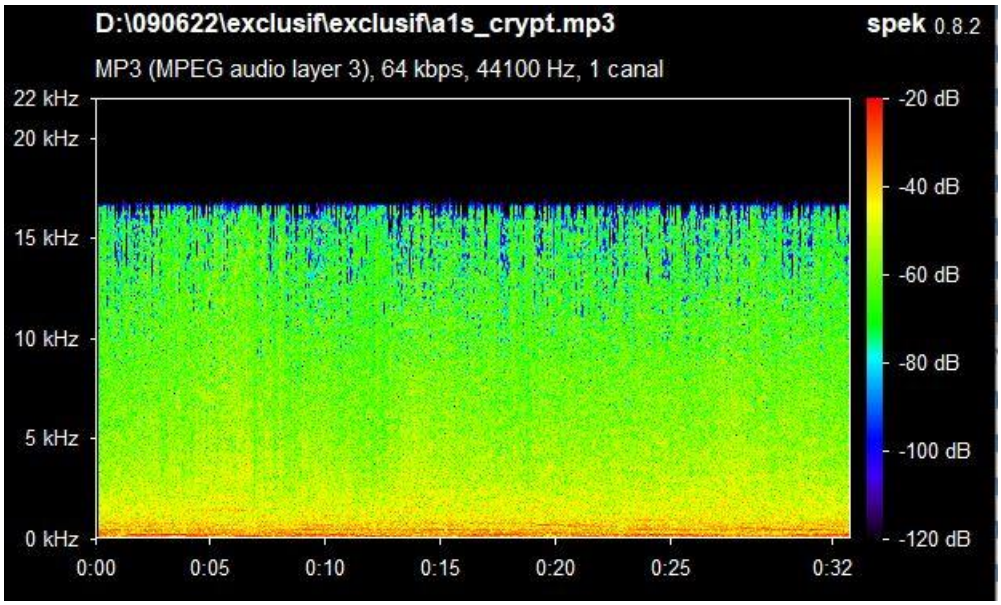


*Figure 34 spectre audio chiffré par ou-exclusif comportant juste le son*

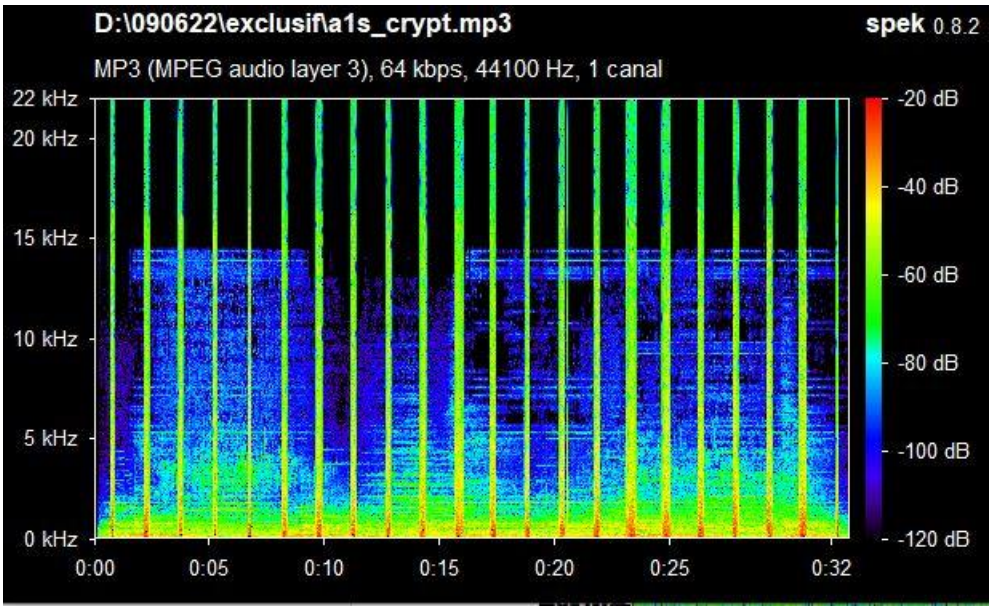


*Figure 35 spectre audio chiffré par la substitution simple comportant juste le son*

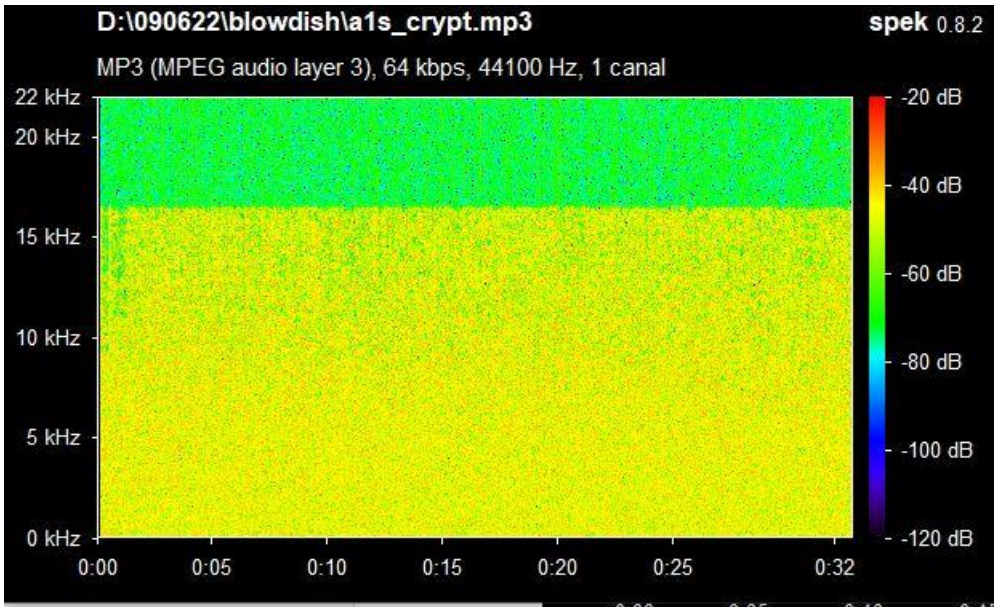


*Figure 36 spectre audio chiffré par blowfish comportant juste le son*

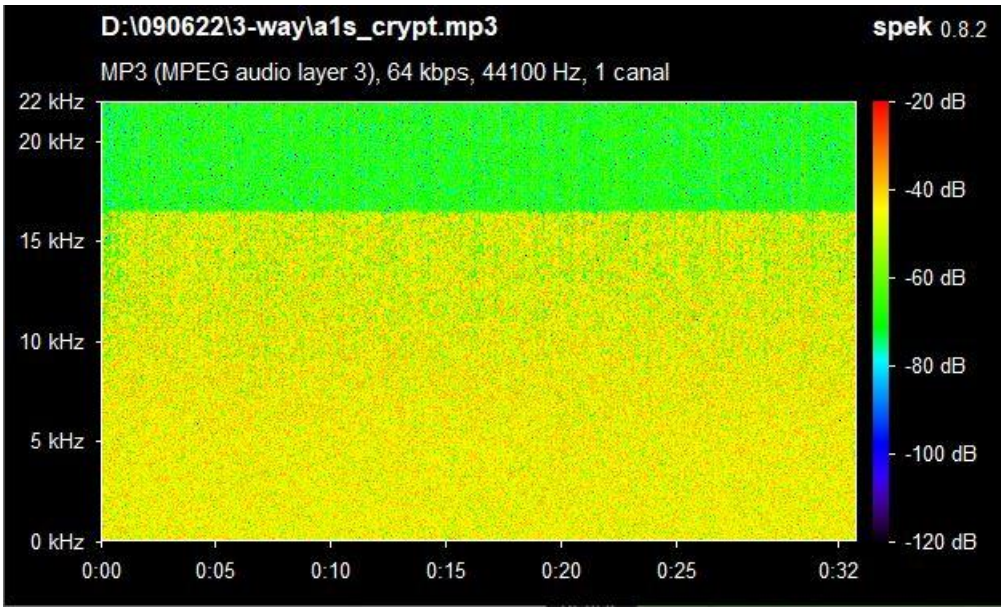


*Figure 37 spectre audio chiffré par 3-way comportant juste le son*

Vidéos comportant juste la parole :

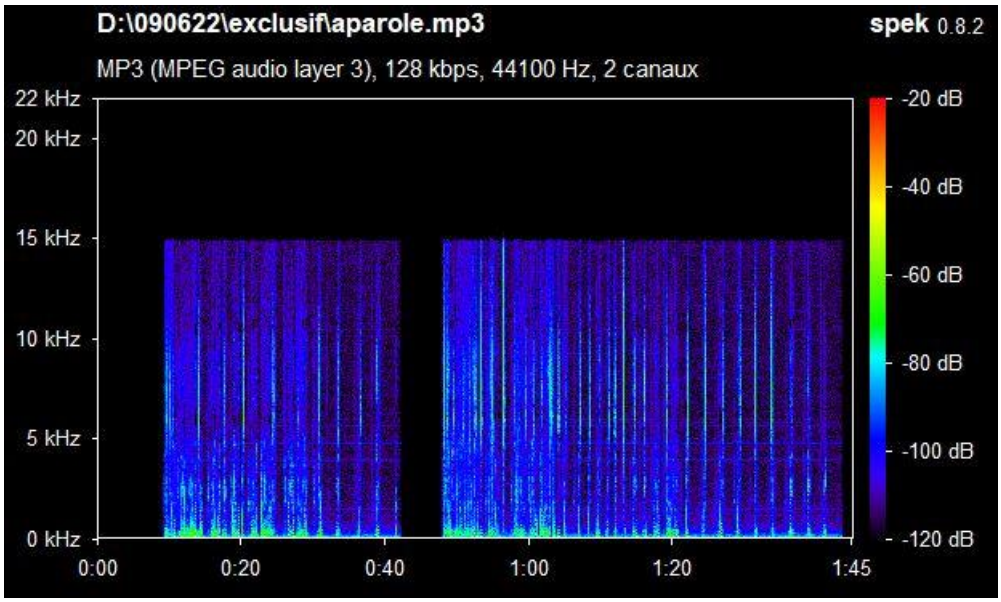


*Figure 38 spectre audio clair contenant juste la parole*

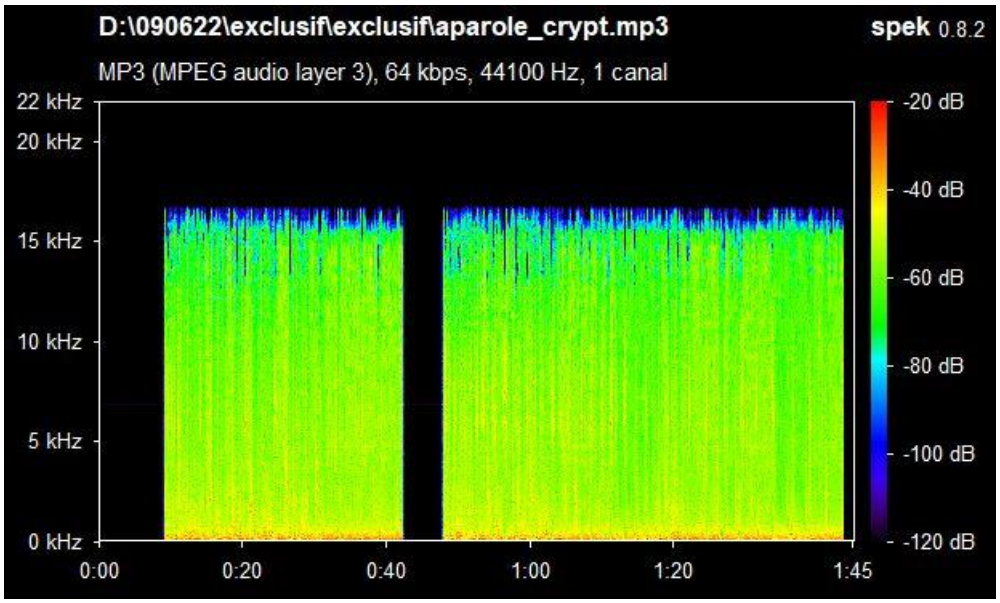


*Figure 39 spectre audio chiffré par ou-exclusif contenant juste la parole*

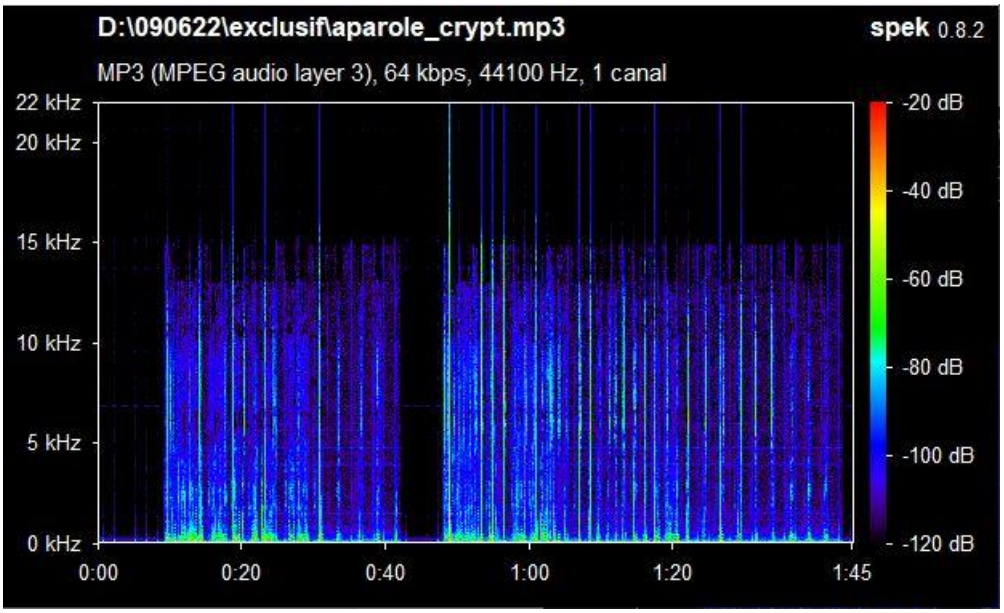


*Figure 40 spectre audio chiffré par la substitution simple contenant juste la parole*

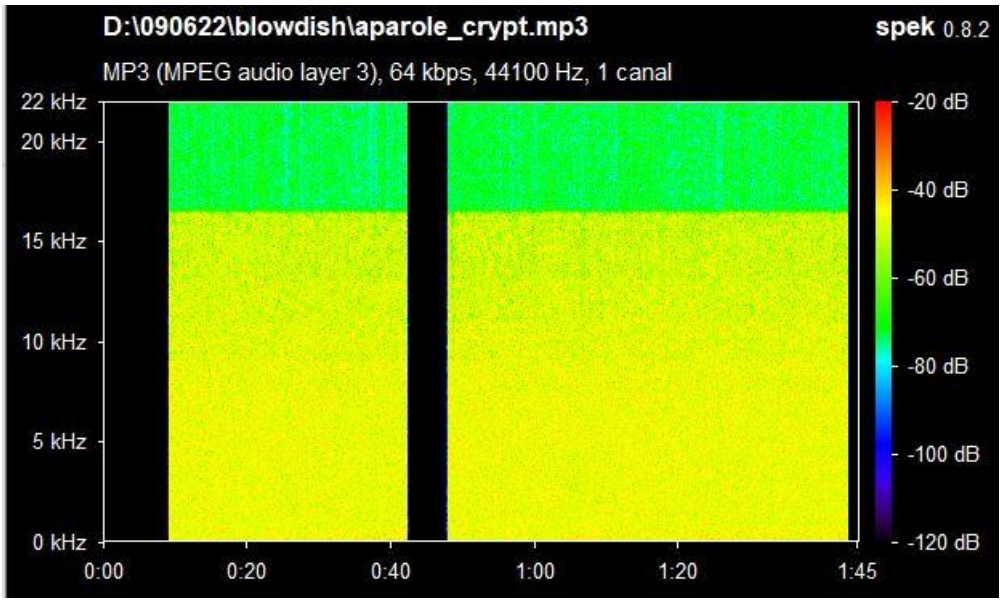


*Figure 41 spectre audio chiffré par blowfish contenant juste la parole*

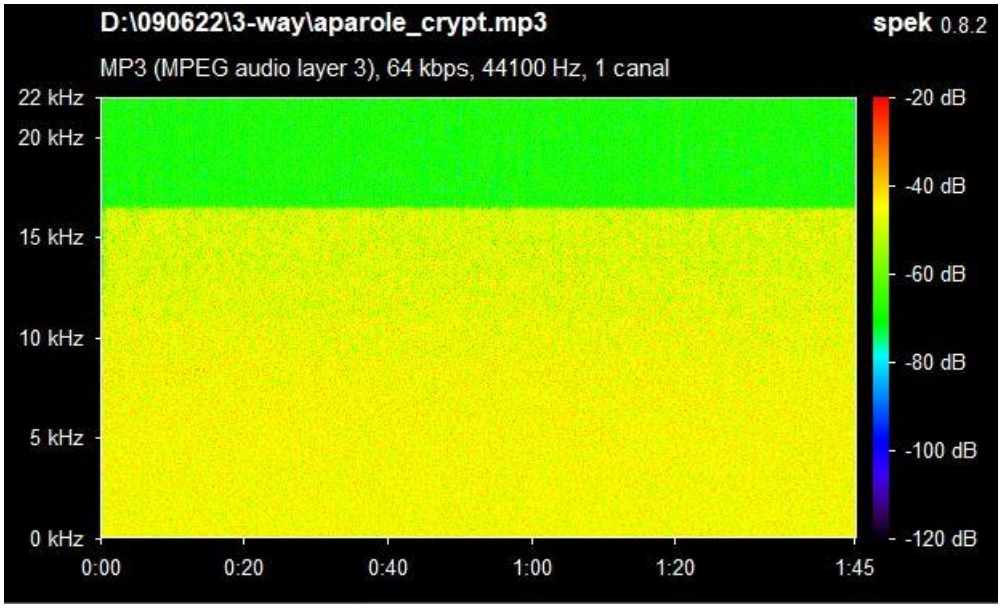


*Figure 42 spectre audio chiffré par 3-way contenant juste la parole*

**Son et parole :**

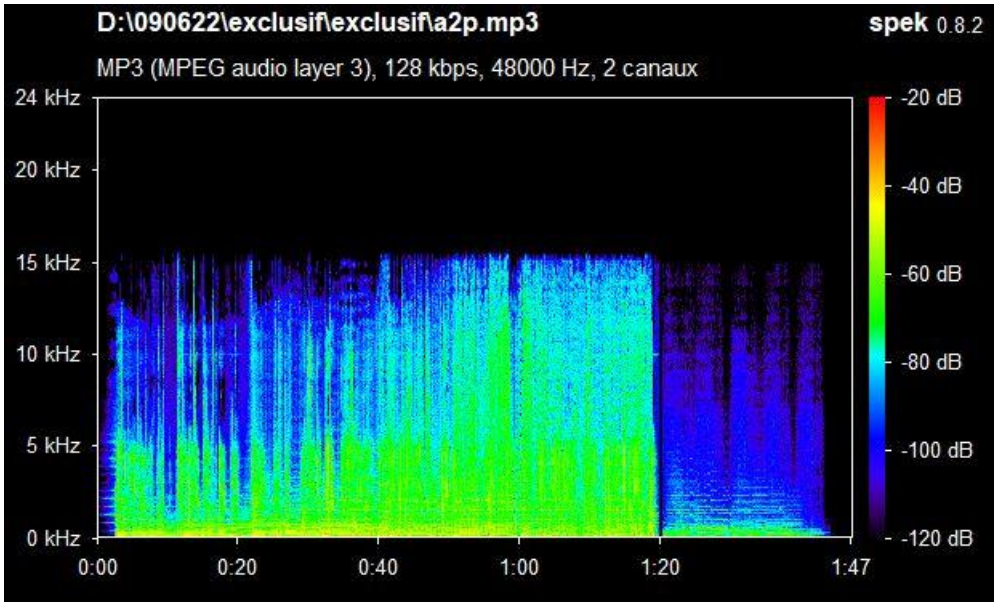


*Figure 43 spectre audio clair contenant le son et la parole*

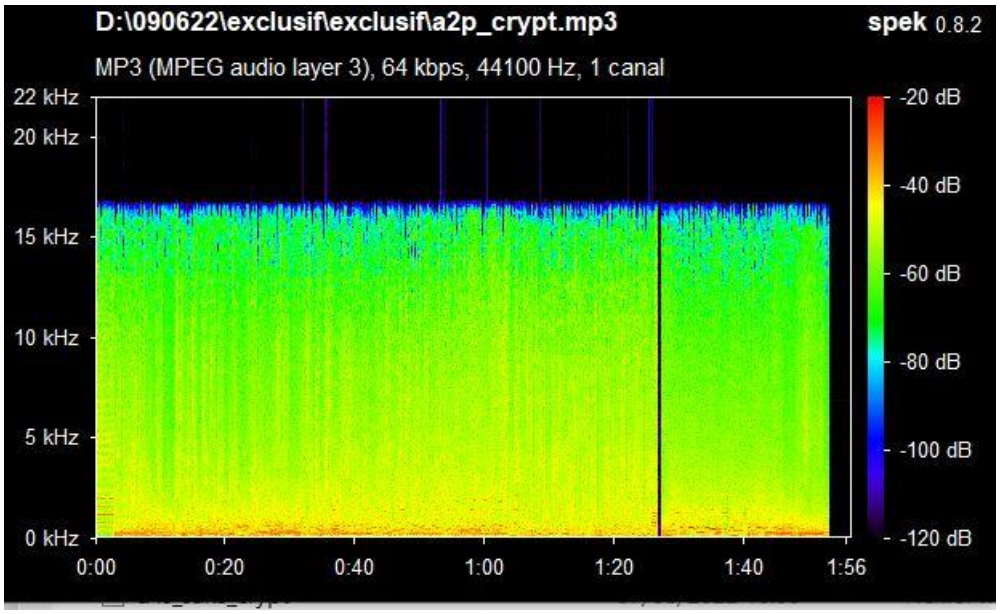


*Figure 44 spectre audio chiffré par ou-exclusif contenant le son et la parole*

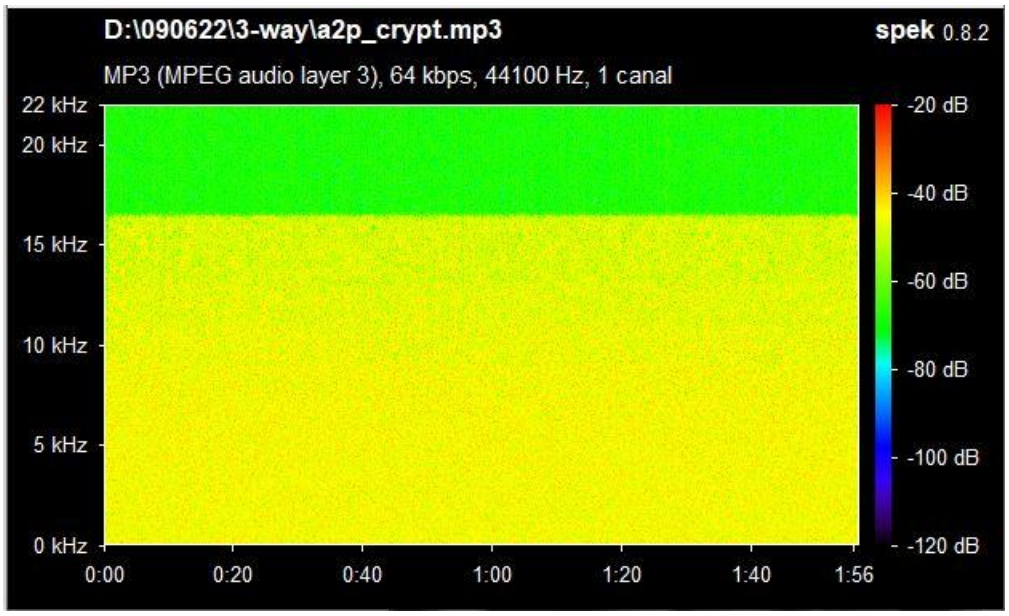


*Figure 45 spectre audio chiffré par 3-way contenant le son et la parole*

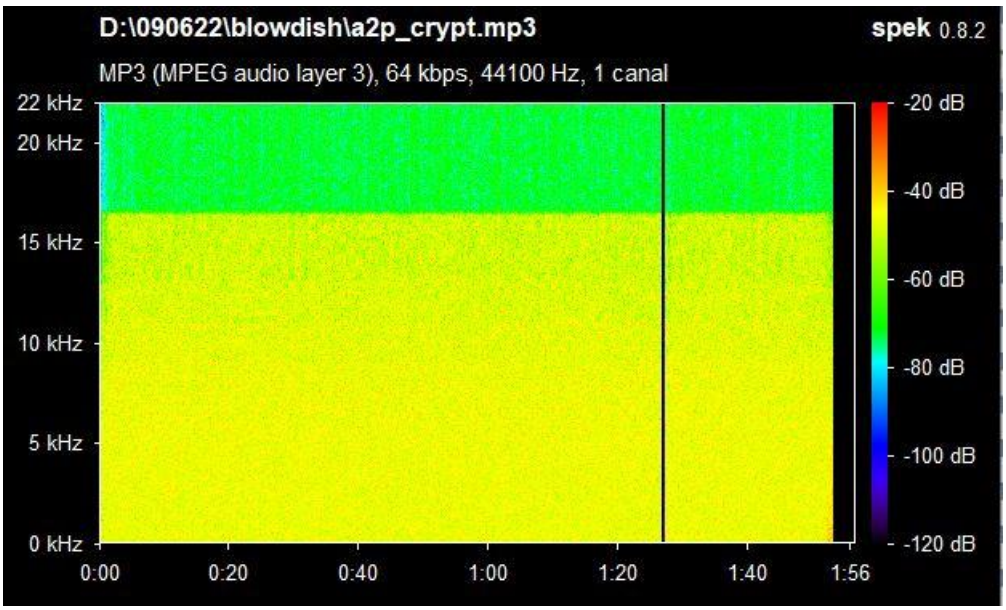


*Figure 46 spectre audio chiffré par blowfish contenant le son et la parole*

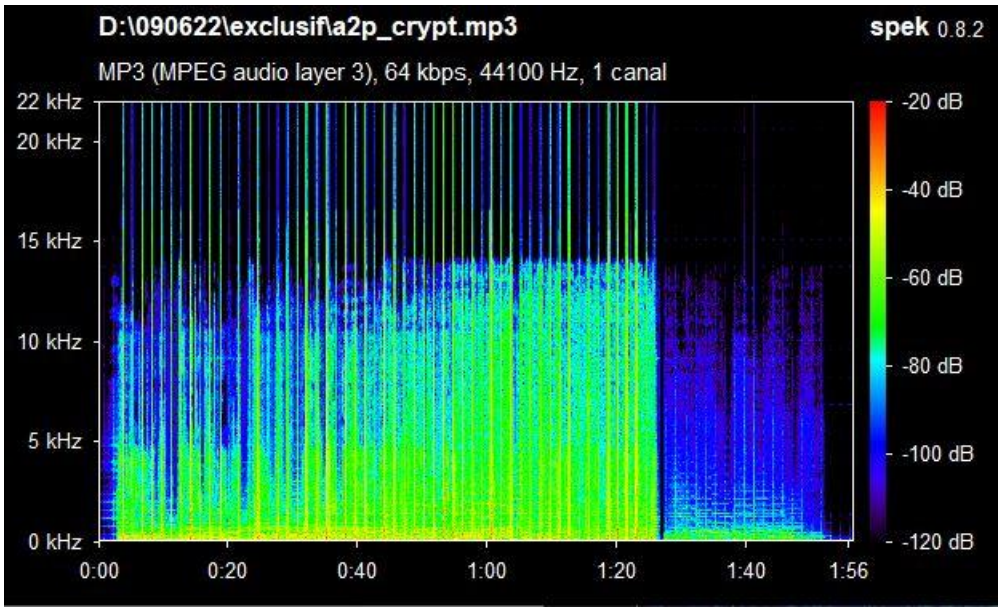


*Figure 47 spectre audio chiffré par la substitution simple contenant le son et la parole*

**Tableau comprative de qualité de chiffrement :**

Entre 80 et 100 meilleur

Entre 50 et 80 bonne

Entre 30 et 50 moyenne

Entre 10 et 30 mauvaise

| | **substitution** | **Ou-exclusif** | **3-way** | **Blowfish** |
|---|---|---|---|---|
| **Video1 (son)** | **20** mauvaise | **30** mauvaise | **100 meilleur** | **100 meilleur** |
| **Video2 (parole et son)** | **10** mauvaise | **25** mauvaise | **100 Meilleur** | **80 meilleur** |
| **Video3 (parole)** | **10** mauvaise | **20** mauvaise | **100 Meilleur** | **80 meilleur** |

*Tableau 8 qualité de chiffrement*

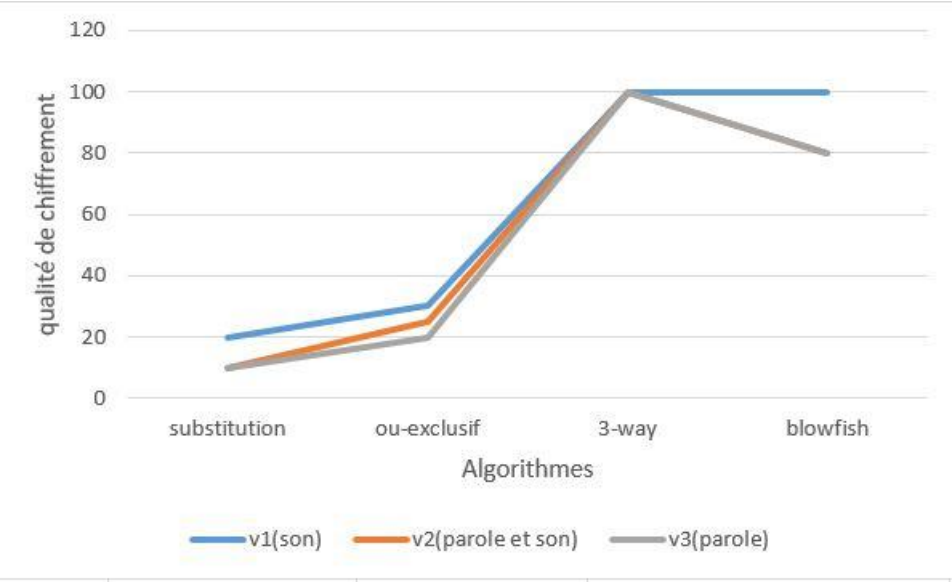


*Figure 48 qualité de chiffrement en fonction des contenu audio*

**Analyse des résultats :**

_la substitution et le ou-exclusif sont des simples algorithmes n'ont pas de grandes complexité mais ont de mauvaise qualité.

_le 3-way a de meilleur qualité quel que soit le contenu du vidéo

_le son est plus simple à chiffrer par rapport à la parole

_la parole pose un problème de chiffrement sauf pour 3-way

## 4.4 Conclusion :

L'analyse des résultats obtenus durant l'application de chiffrement par des diffèrent algorithmes permet de choisir la meilleur performance dans un tel domaine.

Les deux algorithmes blowfish et 3-way sont très performant en terme de qualité de chiffrement tandis que le ou-exclusif et la substitution simple sont de mauvaise qualité.

Vue que 3-way est de meilleur qualité de chiffrement que blowfish en un temps incomparable, on peut le considérer comme l'algorithme optimale pour ce domaine .

# CONCLUSION GENERALE

# Conclusion générale

Depuis que l'homme a été créé, il vit parmi ses semblable et communique avec eux et donc ressent parfois le besoin de dissimiler des informations secrètes en les rendant illisibles car le maintien du secret est une nécessité qui offre parfois la sécurité et donc la cryptographie a toujours été parmi nous.

La cryptographie est la « «science du secret », regroupe deux branches : d'une part, la cryptographie, qui permet de coder des messages, et d'autre part, la cryptanalyse, qui permet de les décoder.

La cryptographie informatique professionnelle est un phénomène récent, rendu indispensable du fait que les informations sont accessibles pratiquement à tous par des réseaux publics.

La cryptographie moderne est orientée vers la manipulation des chiffres et utilise avec abondance des résultats de l'arithmétique, établit souvent il y a longtemps et dont l'utilité pratique n'avait pas été prouvé.

L'informatique par la puissance de calcul qu'elle offre est un outil essentiel de la cryptographie moderne.

J' étais intéressé dans mon projet de fin d'étude par la cryptographie de flux audio d'une vidéo en utilisant l'algorithme a chiffrement itératif 3-way et l'algorithme blowfish en plus de deux algorithmes courant simple le ou-exclusif et la substitution.

La performance des algorithmes de chiffrements dépend de plusieurs paramètres donc l'étude de ces dépendances est important pour obtenir les meilleurs resultat

# Références


[1] : Terminologie, cryptologie.free.fr, Disponible sur :

http://cryptologie.free.fr/crypto/terminologie.html#debut

[2] ; Introduction à la cryptographie, web.maths.unsw.edu.au, Disponible sur :

https://web.maths.unsw.edu.au/~lafaye/CCM/crypto/crypto.htmt

[3] : concepts_de_base.html igm.univ-mlv.fr, Disponible sur :

http://igm.univ-mlv.fr/~dr/XPOSE2007/vma_PKI/concepts_de_base.html

[4] : Cryptographie et codes secrets, www.bibmath.net, Disponible sur :

https://www.bibmath.net/crypto/index.php?action=affiche&quoi=substi/defsub

[5] : Chiffre de Vigenère - Définition et Explications, www.techno-science.net, Disponible sur : https://www.techno-science.net/definition/6140.html

[6] : http://x.heurtebise.free.fr/Enseignements/ATER/S4/Crypto/PDF/Crypto_CM_chap1.pdf

[7] : Blowfish Algorithm with Examples, www.geeksforgeeks.org, Disponible sur : https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/

[8] : Blowfish, www.techtarget.com, Disponible sur :

https://www.techtarget.com/searchsecurity/definition/Blowfish

[9] : 03fr-rist14-2.pdf www.webreview.dz , Disponible sur :

http://www.webreview.dz/IMG/pdf/03fr-rist14-2.pdf 3-way

[10] : https://en.wikipedia.org/wiki/3-Way

[11] : http://univ.ency-education.com/uploads/1/3/1/0/13102001/phys27-son.pdf

[12] : Son (physique) - Définition et Explications, www.techno-science.net, Disponible sur :

https://www.techno-science.net/definition/1236.html

[13] : Principe du passage de l'analogie, culturesciencesphysique.ens-lyon.fr, Disponible sur :

http://culturesciencesphysique.ens-lyon.fr/ressource/principe-numerisation.xml

[14] : 10 formats de fichiers audio communs, recoverit.wondershare.fr, Disponible sur :

https://recoverit.wondershare.fr/audio-recovery/top-10-common-audio-file-formats.html

[15] : Format de fichiers audio / Format audio, www.traitement-signal.com, Disponible sur :

http://www.traitement-signal.com/format_de_fichiers_audio.php#:~:text=Caract%C3%A9ristiques%20des%20formats%20audio&text=Dans%20un%20format%20donn%C3%A9%2C%20les,176.4%2C%20192%2C%20kilohertz)

[16] : http://spek.cc/ visité le 02/06/2022.

[17] : ar.wikipedia.org, Wikipédia, Disponible sur :

https://ar.wikipedia.org/wiki/%D8%A5%D9%81_%D8%A5%D9%81_%D8%A5%D9%85_%D8%A8%D9%8A_%D8%A5%D9%8A_%D8%AC%D9%8A

# Résumé

**Resumé**

De nos jours, la croissance de la quantité d'informations transitant les réseaux internationaux impose de les crypter pour assurer la confidentialité et la sécurité. C'est peut-être le problème le plus important d'Internet. En clair, le cryptage permet d'éviter l'interception, la lecture ou la modification d'un message en clair, ainsi que la fabrication d'un message falsifié.

Le transfert des données audiovisuelles comme les vidéos qui contient des données audio représentées par le son ,la parole ou les deux en même temps .le système de communication comme Internet a besoin d'être sécurisé et protégé contre les utilisateurs non autorisés à faire des modifications dans un contenu sur lequel ils n'ont pas de privilèges . C'est dans ce cadre que se situe mon travail qui consiste à implémenter les différents algorithmes de cryptographie pour chiffrer le flux audio d'un fichier vidéo. Mon travail se termine par une étude comparative sur les performances de chaque algorithme dans ce domaine de multimédia dont la qualité et la complexité temporelle de chiffrement.

**ملخص**

في الوقت الحاضر ، يتطلب النمو في كمية المعلومات التي تمر عبر الشبكات الدولية التشفير لضمان السرية والأمان. ربما تكون هذه هي المشكلة الأكثر أهمية للإنترنت. من الواضح أن التشفير يجعل من الممكن تجنب اعتراض رسالة أو قراءتها أو تعديلها بشكل واضح ، فضلاً عن إنتاج رسالة مزيفة.

نقل البيانات السمعية والبصرية مثل مقاطع الفيديو التي تحتوي على بيانات صوتية ممثلة بالصوت أو الكلام أو كليهما في نفس الوقت. يحتاج نظام الاتصال مثل الإنترنت إلى أن يكون آمنًا ومحميًا ضد المستخدمين غير المصرح لهم لإجراء تعديلات على المحتوى الذي لا يتمتع بامتيازات. . في هذا السياق يقع عملنا ، والذي يتمثل في تنفيذ خوارزميات التشفير المختلفة لتشفير دفق الصوت لملف فيديو. ينتهي عملنا بدراسة مقارنة حول أداء كل خوارزمية في مجال الوسائط المتعددة هذا ، بما في ذلك جودة التشفير وتعقيد الوقت.

**abstract**

Nowadays, the growth in the amount of information passing through international networks requires encryption to ensure confidentiality and security. This is perhaps the most important problem of the Internet. Clearly, encryption makes it possible to avoid the interception, reading or modification of a message in plain text, as well as the production of a falsified message.

The transfer of audiovisual data such as videos which contains audio data represented by sound, speech or both at the same time. The communication system such as the Internet needs to be secure and protected against unauthorized users to make modifications in content over which they have no privileges. It is in this context that my work is located, which consists in implementing the different cryptography algorithms to encrypt the audio stream of a video file. My work ends with a comparative study on the performance of each algorithm in this multimedia field, including encryption quality and time complexity.with a comparative study on the performance of each algorithm in this multimedia field, including encryption quality and time complexity.