TABLE DES MATIERES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABREVIATIONS

dB:	Décibels
HF	Haute fréquence
BF	Basse Fréquence
CAN:	Convertisseur Analogique Numérique
SNR :	Signal-to-noise ratio
C.D:	Compact Disc
ROT13:	rotate by 13
DES:	Data Encryptions Standard
NBS:	National Bureau of Standards
NSA:	National Security Agency
ANSI :	American National Standard Institute
ANSI X3.92:	Norme pour le DES
DEA:	Data Encryption Algorithm
GSM :	Global System for Mobile
MIT:	Massachusetts Institute of Technology
RC4 :	Rivest Cipher 4
RSA :	Rivest Shamir Adleman

INTRODUCTION

La part de plus en plus importante qu'occupent les médias dans notre société moderne nous prouve à quel point l'information est devenue une caractéristique de notre époque. La demande sans cesse croissante de nouveaux moyens de communication, dans des secteurs aussi variés que la télécommunication, la recherche spatiale, l'audio visuel ou l'informatique est à l'origine d'une discipline scientifique à part entière, la théorie de l'information.

De nos jours, la reproduction d'un produit numérique tel que l'image numérique, l'acoustique, la parole et le texte peut être facilement accomplie en employant des appareils enregistreurs. Cependant, l'inconvénient de cette amélioration technologique est la distribution illicite des copies, au coût très bas et en transformant la qualité. De plus, l'important développement des réseaux numériques pose un problème de protection de la propriété intellectuelle des documents, ce qui a motivé de nombreuses recherches sur la sécurisation des données par le moyen de la cryptographie.

Cette technique de sécurisation consiste à rendre un message clair inintelligible par celui qui ne possède pas une clef de déchiffrement. Le travail présenté dans ce rapport propose une nouvelle méthode de cryptage basée sur ***le signal Audio Numérique*** et utilisant ***les opérations du traitement de signal.***

Ce présent rapport est composé de quatre chapitres. Le premier chapitre, « les caractéristiques du son » est composé de la définition d'un son, sa propagation, sa perception humaine et ses caractéristiques. Le deuxième chapitre est « le traitement du signal », on verra quelques définitions, la classification des signaux et la notion de filtrage et de la modulation. Dans le troisième chapitre on peut voir quelques vocabulaires utilisés en cryptographie, les différents types de cryptanalyse et les deux grandes catégories de chiffrement. Et pour terminer, au dernier chapitre intitulé « La cryptographie et le traitement du son », se trouve le principe du codage et de décodage audio.

CHAPITRE 1 : Rappels sur la nature vibratoire du Son et le Traitement de signal

1.1. Qu'est-ce qu'un son ? [1]

Le son est une onde produite par la vibration d'un support fluide ou solide se propageant sous forme d'ondes longitudinales. Dans le cas le plus simple, cette onde est une simple sinusoïde, c'est-à-dire une vibration d'équation :

$$x(t) = A.\sin(2\pi f.t - \varphi)$$

A est appelé l'amplitude du son, f sa fréquence et φ le déphasage de la vibration par rapport à l'origine des temps.

Un tel son est appelé un son « pur ». Dans l'air, l'amplitude correspond aux variations de pression qui caractérisent l'onde.

Les sons les plus souvent rencontrés sont rarement purs. Ils sont la somme de plusieurs sons purs, c'est-à-dire de plusieurs sinusoïdes, plus couramment appelées « harmoniques ».

On dit qu'un son est « riche » quand il contient de nombreux harmoniques (comme la parole) et « pauvre » quand il n'a que peu d'harmoniques (comme le son d'une flûte).

1.2. La propagation du son [1]

Comme nous l'avons vu, le son est une onde, une vibration. Le son ne se propage pas dans le vide. Si une sonnerie est placée dans une cloche de verre et que le vide y est fait petit à petit, on remarquera que plus l'air se raréfie, plus le son s'atténuera jusqu'à son extinction totale.

Quand une source émet un son, la vibration se propage de particule en particule jusqu'à notre tympan qui vibre à son tour. Plus le milieu est dense plus le son se propage vite. Dans l'air le son se propage à environ 350 m/s, dans l'eau à environ 1500 m/s et à environ 5050 m/s dans l'acier. La vitesse de propagation du son dépend de la température, de la pression et surtout de la densité du milieu.

1.3. La perception humaine du son [1]

Une vibration mécanique de la matière et de l'air qui fait vibrer notre tympan ne constitue pas en elle-même le son. C'est dans notre cerveau que le son naît et se forme. Le son n'existe pas en dehors de notre cerveau.

Entre l'arrivée des signaux vibratoires aux oreilles et la sensation de son dans le cerveau a lieu le phénomène de traitement des signaux par le système nerveux. Cela signifie que la vibration physique de l'air ne parvient pas de façon brute au cerveau. Elle est transformée.

La gamme des vibrations perceptibles est tronquée, c'est-à-dire que nous n'entendons pas les sons ni trop bas (de fréquences faibles) ni trop hauts (de fréquences élevées) même si leurs vibrations parviennent à notre oreille. Le système nerveux ne peut traiter que des vibrations dont la fréquence est comprise entre 20 Hz et 20 kHz. Les sons de fréquences inférieures à 20 Hz sont appelés infrasons et ceux de fréquences supérieures à 20 kHz ultrasons.

Tout être vivant doté d'une ouïe ne peut percevoir qu'une partie du spectre sonore qui dépend de l'espèce concernée. Par exemple, le chat peut percevoir les sons de fréquence allant jusqu'à 25 kHz, le chien perçoit les sons allant jusqu'à 35 kHz, la chauve-souris et le dauphin les sons de fréquence jusqu'à 100 kHz .

En outre, l'ouïe est capable de traiter les signaux sonores de façon à n'en extraire que les informations nécessaires à notre perception de l'environnement. Par exemple, dans un environnement bruyant, un homme est capable d'extraire de façon automatique les sons qui ont un sens pour lui, comme les paroles de quelqu'un avec qui il parle. L'homme est également capable de reconnaître des formes sonores, tels que ceux produits par des instruments de musique.

1.1. Caractéristiques d'un son [1]

a. L'intensité

L'intensité d'un son dépend directement de son amplitude. Elle caractérise ce que l'on entend par un son fort (c'est-à-dire qui tend à assourdir) ou faible (c'est-à-dire qui est presque inaudible). L'intensité I en un point donné diminue en fonction de la distance r qui sépare ce point de la source. Elle est liée à la puissance P de l'émetteur par la formule :

$$I = \frac{P}{4\pi r^2}$$

L'intensité sonore exprime en effet la puissance de la vibration sonore reçue par unité de surface à l'endroit où l'on se trouve. Son unité est donc le W/m².

En acoustique, l'intensité est cependant exprimée en décibels pour les raisons citées ci-dessous :

- Ils permettent de travailler avec des valeurs facilement manipulables (ni « trop grandes », ni « trop petites »).
- L'oreille humaine perçoit l'intensité sonore de façon logarithmique.

Dans le standard international, on a pris comme intensité de référence I0 W/m² le seuil d'audibilité de l'oreille humaine pour un son de fréquence 1000 Hz. L'intensité acoustique (qui s'exprime en dB) est définie par :

$$L = 10 \log \frac{I}{I_0}$$

Le seuil d'audition de notre oreille se situe à 0 dB et le seuil de douleur à 120 dB. Le Tab. 1.1 nous montre l'échelle de bruit pour l'oreille humaine :

Tableau 1.1 : Echelle de bruit pour l'oreille humaine [2]

Classe du bruit	Intensité	Exemple
Sans danger pour l'audition	0	Silence total
	15	Bruissement des feuilles
	20	Chuchotement/Jardin paisible
	25	Conversation à voix basse
	30	Appartement dans une rue tranquille
	35	Bateau à voile/Tic-tac
	40	Rue résidentielle
	50	Bruit d'une voiture au ralenti
	60	Grand magasin/Sonnerie de téléphone
	70	Restaurant bruyant
	85	Radio volume à fond
Facteur de troubles auditifs	90	Rue au trafic intense
	95	Train passant à la gare
Pénible à entendre	100	Marteau piqueur/baladeur à fond
	105	Discothèque/Concert
	110	Atelier de chaudronnerie
Seuil de douleur	120	Moteur d'un Boeing 747
	130	Décollage d'un Boeing 747
Exige une protection auditive	140	Turbo réacteur
	150	Décollage d'une fusée

b. La hauteur

La hauteur d'un son est le paramètre qui permet de distinguer un son bas (ou grave) d'un son élevé (ou aigu). Elle dépend directement de la fréquence. Plus la fréquence augmente, plus le son est aigu et inversement, plus la fréquence diminue, plus le son est grave.

c. Le timbre

Le timbre est l'empreinte vocale qui permet de reconnaître la voix d'une personne, ou d'un instrument. Il est caractérisé par la fréquence des harmoniques, leur nombre, leur amplitude.

CHAPITRE 2 : Traitement du signal

2.1. Introduction

Le traitement du signal est une discipline indispensable de nos jours. Il a pour objet *l'élaboration* ou l'*interprétation* des signaux porteurs d'informations [3]. Son but est de réussir à extraire un maximum d'information utile sur un signal perturbé par du bruit [4] en s'appuyant sur les ressources de l'électroniques et de l'informatique.

2.2. Quelques définitions

a. Signal

Un signal est la représentation physique de l'information, qu'il convoie de sa source à son destinataire. La description mathématique des signaux est l'objectif de la théorie du signal. Elle offre les moyens d'analyser, de concevoir et de caractériser des systèmes de traitement de l'information.

b. Bruit

Un bruit correspond à tout phénomène perturbateur gênant la transmission ou l'interprétation d'un signal [4].

c. Système

Un système est un dispositif représenté par un modèle mathématique de type Entrée/Sortie (Fig.2.1) qui apporte une déformation au signal (Ex: modulateur, filtre, etc.).

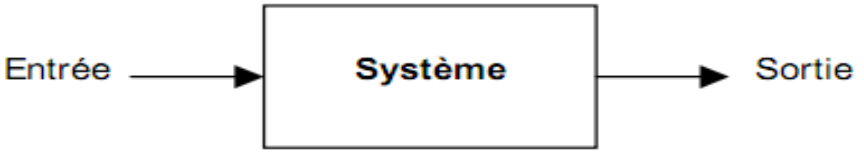


Figure 2.1 : Représentation synoptique d'un système

2.3. Classification des signaux

Les signaux sont classifiés suivant leurs propriétés

a. Classification Phénoménologique

On considère la nature de l'évolution du signal en fonction du temps. Il apparaît deux types de signaux :

- *Les signaux déterministes* (ou signaux certains)

  Leur évolution en fonction du temps peut être parfaitement modélisée par une fonction mathématique. On retrouve dans cette classe les signaux périodiques, les signaux transitoires, les signaux pseudo-aléatoires, etc.

- *Les signaux aléatoires*

  Leur comportement temporel est imprévisible. Il faut faire appel à leurs propriétés statistiques pour les décrire. Si leurs propriétés statistiques sont invariantes dans le temps, on dit qu'ils sont stationnaires.

b. Classification Energétique

On considère l'énergie des signaux :

- *Les signaux à énergie finie*

  Ce sont les signaux qui possèdent une puissance moyenne nulle et une énergie finie [5].

- *Les signaux puissance moyenne finie*

  Les signaux possèdent une énergie infinie et sont donc physiquement irréalisable [5].

Formule de l'Energie et Puissance d'un signal x(t)

Energie du signal x(t) :

$$W_x = \int_{-\infty}^{+\infty} |x(t)|^2 \, dt$$

Puissance du signal x(t) :

$$P_x = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{T/2} |x(t)|^2 \, dt$$

c. Classification Morphologique

On distingue les signaux à variable continue des signaux à variable discrète ainsi que ceux dont l'amplitude est discrète ou continue.

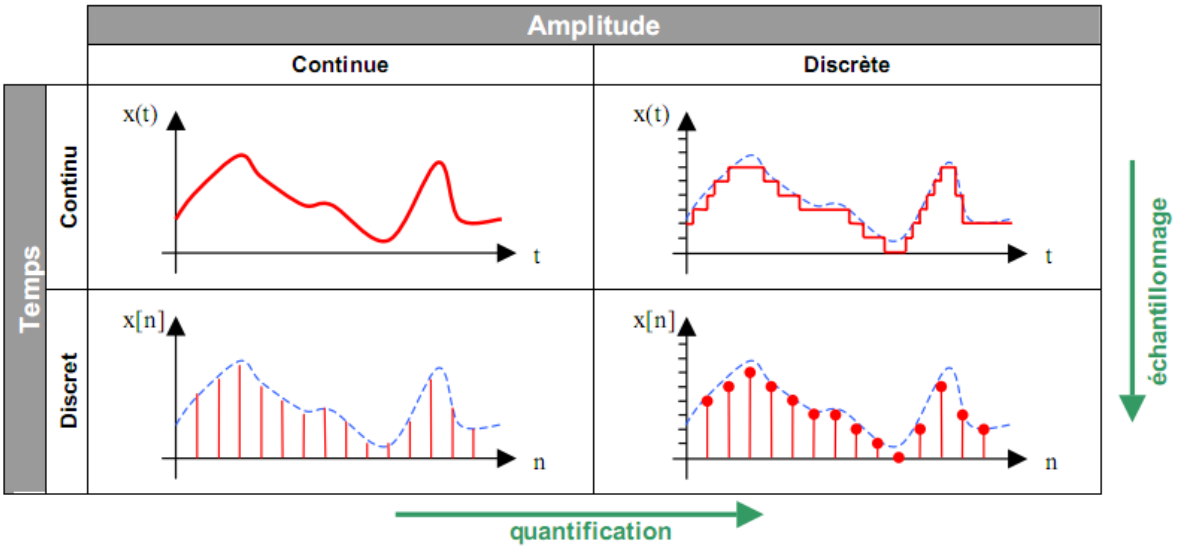


Figure 2.2 : Nature Morphologique des signaux

2.4. Notion de Filtrage

Le filtrage est une forme de traitement de signal qui modifie le spectre de fréquence et/ou la phase du signal présent en entrée du filtre et donc par conséquent sa forme temporelle. Il peut s 'agir soit :

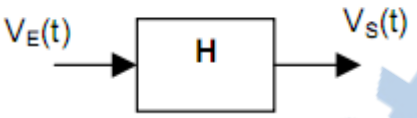
- d'éliminer ou d'affaiblir des fréquences parasites indésirables
- d'isoler dans un signal complexe la ou les bandes de fréquences utiles.

On classe les filtres en deux grandes familles :

- les filtres numériques : réalisés à partir de la structure intégrée micro programmable.

- les filtres analogiques : réalisés à partir de composants passifs (résistance, inductance, condensateur) ou actifs.

a. Fonction de Transfert



Le comportement d'un filtre est défini par l'étude fréquentielle de la fonction de transfert entre la tension de sortie et la tension d'entrée du filtre. On le caractérise par l'amplification et le déphasage qu'il apporte sur les différents harmoniques du signal d'entrée.

Ainsi, on obtient l'expression de la fonction de transfert :

Son module : sa fonction de transfert : son argument :

$$|\underline{H}|_{dB} = 20log\left|\frac{\underline{V_S}}{\underline{V_E}}\right| \qquad \underline{H}(j\omega) = \frac{\underline{V_S}(j\omega)}{\underline{V_E}(j\omega)} \qquad \varphi = Arg\,[\underline{H}(j\omega)]$$

Il faut remarquer que :

- Parfois, on préfère définir un filtre par rapport à l'atténuation qu'il amène sur la grandeur d'entrée :

$$\underline{A}(j\omega) = \frac{1}{\underline{H}(j\omega)}$$

- On définie aussi le temps de propagation τ de groupe plutôt que le déphasage. Il caractérise le retard apporté par le filtre sur les différents harmoniques du signal d'entrée :

$$\tau = \frac{d\varphi}{d\omega}$$

- H est la réponse impulsionnelle du filtre :

$$V_s(t) = V_E(t) \square h(t) \quad \text{et} \quad TF[V_s(t)] = V_E(f).h(f)$$

Autrement dit, le spectre du signal de sortie est égal au produit du spectre du signal d'entrée par la réponse en fréquence du filtre.

b. Filtre réel – Gabarit

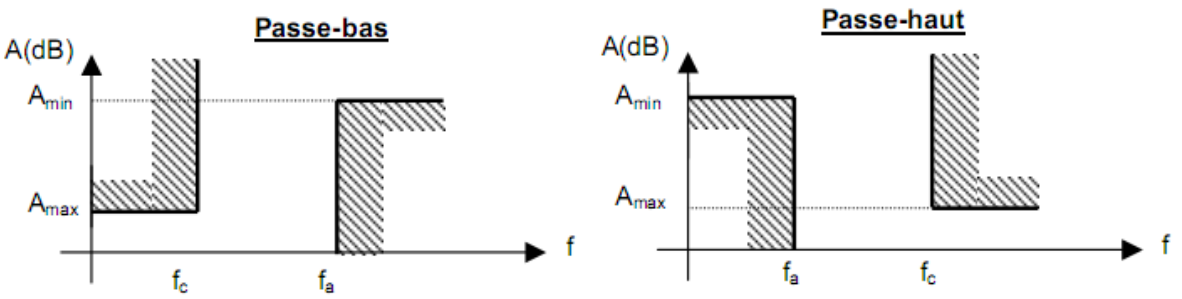
Un filtre idéal présente :

- un affaiblissement nul dans la bande de fréquence que l'on désire conserver (Bande passante)
- un affaiblissement infini dans la bande que l'on désire éliminer (Bande atténuée)

Il est impossible pratiquement de réaliser de tels filtres. Aussi se contente-t-on d'approcher cette réponse idéale en :

- conservant l'atténuation A inférieure à A_{max} dans la bande passante
- conservant l'atténuation supérieure à A_{min} dans la bande atténuée

Cela conduit ainsi à définir un gabarit [6] définissant des zones interdites et des zones dans lesquelles devra impérativement se situer les graphes représentant l'atténuation du filtre en fréquence. Suivant le type de réponse que l'on désire obtenir, on est amené à définir quatre familles de filtres :



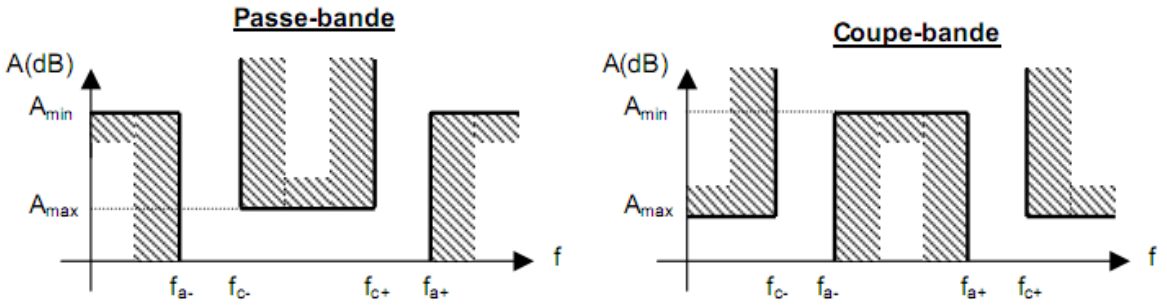


Figure 2.3 : Gabarit des filtres

Lorsque l'on veut dimensionner un filtre, on ne sait calculer analytiquement qu'un petit nombre de fonctions caractéristiques convenant à la réalisation d'un gabarit. Ces différentes fonctions fixeront les propriétés physiques du filtre (Butterworth, Tchebycheff, Bessel, Cauer).

2.5. Notion de Modulation

a. Principe

Le principe de modulation d'un signal est essentiellement utilisé pour la transmission des signaux. Il permet d'adapter le message à transmettre au canal de transmission [7].

Par exemple, en radio, le message transmis par voie hertzienne est un message audio dont le spectre sera compris dans la bande [20Hz, 20kHz]. La réception d'un tel signal nécessite des antennes dont les dimensions sont du même ordre de grandeur que la longueur d'onde du signal (en général de l'ordre de ½).

Ainsi, l'objectif est de se servir d'un signal de fréquence importante pour transmettre le message afin de réduire à des proportions raisonnable la taille des antennes. Ainsi, le but de la modulation est de translater le spectre d'un signal basses fréquences (BF) vers les hautes fréquences (HF).

La radio, la télévision, les lignes téléphoniques utilisent le procédé de modulation. Le signal HF utilisé pour transporter le message est appelé la porteuse. Le message, dont on

se sert pour moduler une des caractéristiques de la porteuse, est appelé le modulant. Si la porteuse est de forme sinusoïdale, elle possède comme expression :

$$S_P(t) = U_p \cos(\omega_p t + \varphi) \; avec \; \omega_p \; \square \; 0$$

Pour transporter le message, on ne peut jouer que sur deux paramètres :

- l'amplitude U_p : on effectue alors *une modulation d'amplitude*
- la phase φ : on effectue alors *une modulation angulaire (phase ou fréquence).*

En ce qui concerne la démodulation, elle est seulement l'inverse de la modulation. Elle consiste à reconstruire le signal modulant à partir du signal modulé. La qualité d'une modulation est déterminée par la facilité à récupérer le signal modulant et par son immunité aux bruits.

b. Modulation d'Amplitude

Le principe consiste à moduler l'amplitude de la porteuse $S_p(t)$ par le signal message m(t) :

$$S_m(t) = m(t).U_p cos\,\omega_p\, t$$

Dans le cas où le message a une forme sinusoïdale :

$$S_m(t) = U_m cos\,\omega_m\, t.U_p cos\,\omega_p\, t$$

$$S_m(t) = \frac{U_m U_p}{2}\{cos\,|(\omega_m - \omega_p)t| + cos\,|(\omega_m + \omega_p)t|\}$$

Son amplitude sera comprise entre :

$$+U_m.U_p \qquad et \qquad -U_m.U_p$$

Le spectre du signal modulé est:

$$S_m(f) = \frac{U_m U_p}{4}|\delta(f - f_m + f_p) + \delta(f - f_m - f_p) + \delta(f + f_m - f_p) + \delta(f + f_m + f_p)|$$

Procédure de la modulation

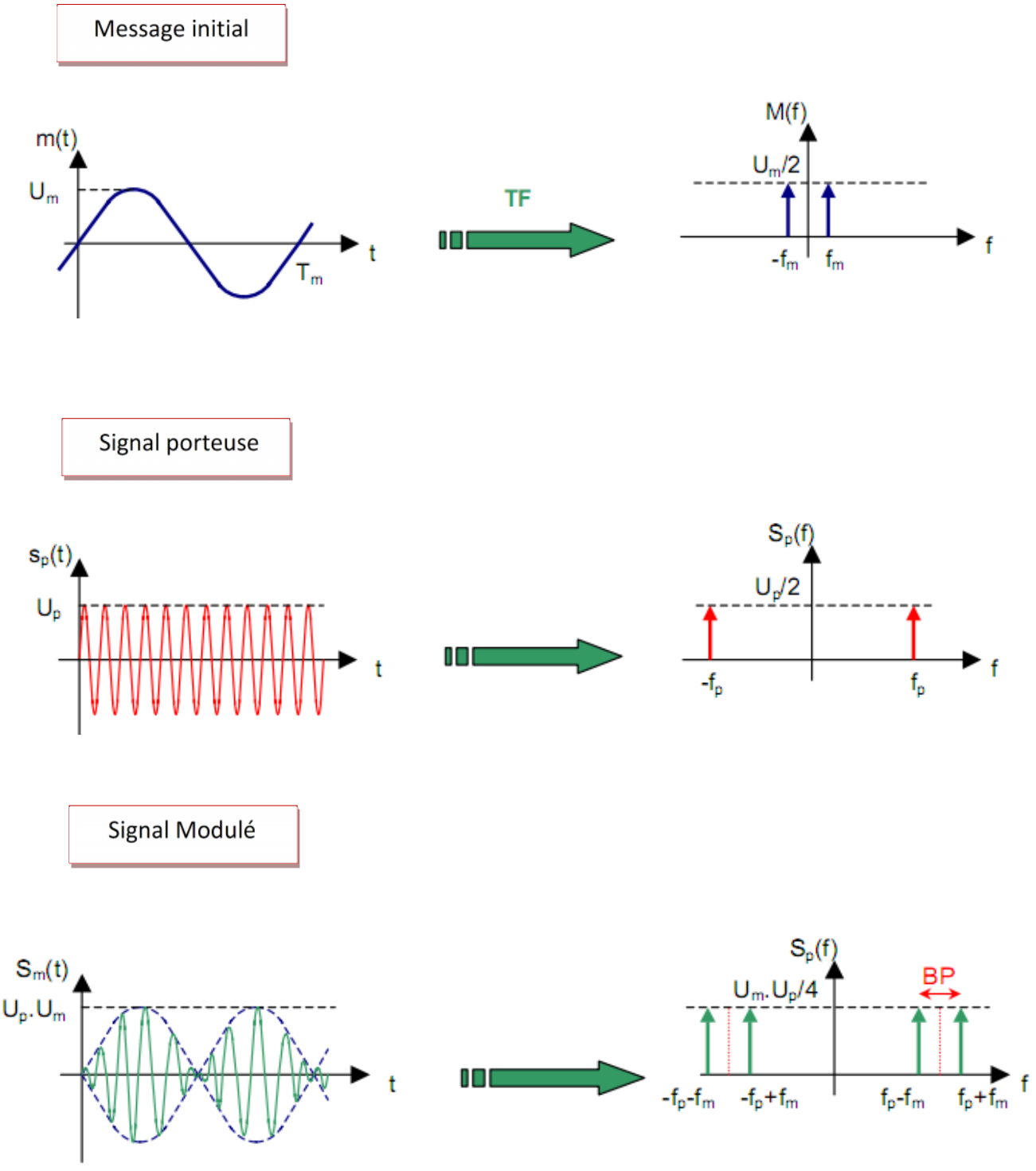


Figure 2.4 : Processus de la modulation d'un signal

La modulation d'amplitude réalise donc une transposition en fréquence du signal message. Elle est réalisée à partir d'une simple multiplication. A noter que si l'on veut transmettre un signal de fréquence f_m, la bande passante nécessaire est de deux fois f_m.

La récupération du message par démodulation implique de réaliser l'opération inverse. Il faut donc multiplier le signal modulé par la porteuse pour refaire une transposition en fréquence puis isoler le message par filtrage.

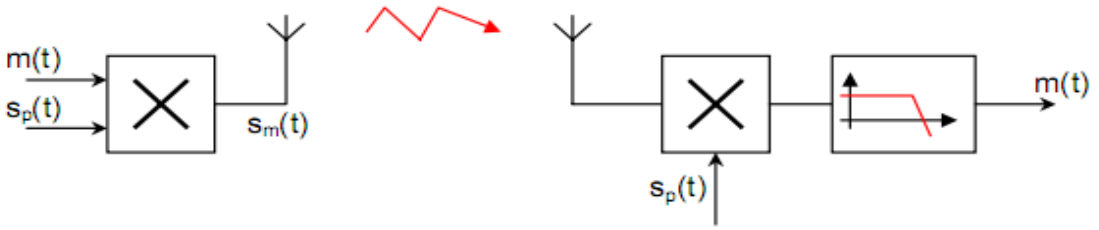


Figure 2.5 : Reconstitution du message initial

Mais fabriquer *une porteuse de fréquence* strictement identique est très difficile. Une solution consiste à transmettre la porteuse avec le message pour pouvoir facilement la reconstruire à la réception.

On l'appelle *la modulation avec porteuse* et l'expression du signal modulé devient :

$$s_m(t) = [k.m(t) + 1]U_p cos\omega_p t$$

(avec K est le taux de modulation)

C'est ce principe qui est retenu en radiodiffusion.

CHAPITRE 3 : La Cryptographie

3.1. Introduction

La ***Cryptologie*** est une science mathématique qui comporte deux branches : la cryptographie et la cryptanalyse.

Le mot **cryptographie** vient du grec « **kruptos** » (qui signifie "caché") et « **graphein** » (pour "écrire").

Elle se définit comme l'art de transformer un message clair en un message inintelligible. Tandis que la cryptanalyse est un art d'analyser un message chiffré afin de le déchiffrer.

3.2. Vocabulaires

a. Le chiffrement [8]

Le **chiffrement** est en cryptographie le procédé grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (de)chiffrement.

b. Le déchiffrement [8]

C'est l'action de déchiffrer qui consiste à retrouver le texte original (aussi appelé texte clair) d'un message chiffré dont on possède la clé de chiffrement.

c. Crypter

C'est le synonyme du mot chiffrer.

d. Décrypter [8]

C'est l'action de retrouver un message clair correspondant à un message chiffré sans posséder la clé de déchiffrement (terme que ne possèdent pas les anglophones, qui eux « cassent » des codes secrets).

e. Cryptolecte [8]

C'est un jargon réservé à un groupe restreint de personnes désirant dissimuler leur communication**.**

f. Cryptogramme

Le terme est parfois utilisé en cryptologie comme un synonyme de texte chiffré ou de « message chiffré ».

g. Clés [9]

C'est une valeur utilisée dans un algorithme de cryptographie afin de générer un texte chiffré ou de le déchiffrer. Les clés sont en réalité des nombres extrêmement important (mesure en bits).

h. Stéganographie [10]

La stéganographie est une forme de cryptographie qui consiste à camoufler un message dans un texte, une image, ou n'importe quel support.

3.3. Les différents types de cryptanalyse [11]

Un attaquant est donc une personne qui tente de décrypter des messages, c'est-à-dire de retrouver des claires à partir de chiffrés sans connaître la clé. On réserve généralement le verbe « déchiffrer » à l'action du destinataire légitime qui effectue l'opération inverse du chiffrement.

La cryptanalyse d'un système cryptographique peut être :

- **Une cryptanalyse partielle** : l'attaquant découvre alors le texte clair correspondant à un ou plusieurs messages chiffrés interceptés.
- **Une cryptanalyse totale** : l'attaquant découvre un moyen de déchiffrer tous les messages, aussi bien ceux qu'il a interceptés que ceux à venir, par exemple en découvrant la clé utilisée.

Selon les moyens dont dispose l'attaquant, on distingue plusieurs types d'attaques.

Par ordre de moyens croissants, on a :

- **Attaque à messages chiffrés** (seulement) : L'attaquant a seulement la possibilité d'intercepter un ou plusieurs messages chiffrés.

- **Attaque à messages clairs** : L'attaquant dispose d'un ou plusieurs messages clairs avec les messages chiffrés correspondants.

- **Attaque à messages clairs choisis** : L'attaquant a la possibilité d'obtenir la version chiffrée de messages clairs de son choix. On distingue alors deux sous-types d'attaque, suivant que l'attaquant est contraint de choisir les clairs en une seule fois, ou au contraire peut faire évoluer ses choix au fur et à mesure des résultats obtenus. Dans le deuxième cas, on parle d'attaque adaptive à messages clairs choisis.

- **Attaque à messages chiffrés choisis** : L'attaquant a temporairement l'opportunité de déchiffrer les messages de son choix (en ayant accès par exemple à une machine déchiffrant). Il tente alors d'en profiter pour obtenir des informations lui permettant de décrypter ensuite d'autres messages par ses propres moyens. Comme dans le point précédent, on peut distinguer deux sous-types : attaque adaptive ou non.

3.4. Les deux grandes catégories de Chiffrement

a. Les chiffrements symétriques

i) Introduction [8]

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie à clé publique), est la plus ancienne forme de chiffrement. On a des traces de son utilisation par les Égyptiens vers 2000 avant Jésus Christ. Plus proche de nous, on peut citer le chiffre de Jules César, dont le ROT13 est une variante.

ii) Définition

Le chiffrement est symétrique quand il utilise la même clé pour le chiffrement et le déchiffrement.

iii) Les chiffrements symétriques par blocs

iii.1. Le chiffrement à clé secrète classique

La transposition [10]

Le chiffrement par transposition est une méthode qui consiste à réarranger les données à chiffrer de façon à les rendre incompréhensibles. Par exemple en réordonnant géométriquement les données pour les rendre visuellement inexploitables.

Exemple : « Le rouleau assyrien »

Figure 3.1: Le rouleau assyrien

La technique de chiffrement assyrienne est vraisemblablement la première preuve de l'utilisation de moyens de chiffrement en Grèce dès 600 avant Jésus Christ, afin de dissimuler des messages écrits sur des bandes de papyrus.

Lors de l'écriture du message la feuille est enroulée autour d'un cylindre d'un certain diamètre. Pendant le transport le message n'est plus enroulé autour du rouleau et est donc illisible. Le destinataire doit enrouler la feuille autour d'un cylindre de diamètre identique à celui qui a servi à coder. Cette technique consiste à faire des anagrammes (changer l'ordre des lettres), on dit que c'est une technique de transposition.

La substitution [10]

Le chiffrement par substitution consiste à remplacer un ou plusieurs caractères par un ou plusieurs autres caractères.

Il y a plusieurs moyens de chiffrement par substitution :

La substitution monoalphabétique : qui consiste à substituer chaque lettre du message par une autre lettre de l'alphabet.

Exemple : Jules César

Il suffit de décaler vers la droite ou gauche d'un certains nombre les lettres du message à coder.

Tableau 3.1 : Table de César

Normal	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
Décalé	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

La substitution polyalphabétique : on utilise plusieurs tables de substitution monoalphabétique, et la table utilisée dépend de la position de lettre dans le texte.

Exemple : on prend les 3 tables de correspondance suivantes :

```
Texte en clair:        abcdefghijklmnopqrstuvwxyz

Table 1:               nopqrstuvwxyzabcdefghijklm
Table 2:               azertyuiopqsdfghjklmwxcvbn
Table 3:               mlkjhgfdsqytrezauiopnbvcxw
```

Maintenant, imaginons que l'on veuille crypter le mot « ***electronique*** » par exemple, on change de table toutes les lettres et l'on boucle donc tous les 3 caractères (car nous n'avons ici que 3 tables):

e :	r (par la table 1)	**o** :	b (par la table 1)
l :	s (par la table 2)	**n** :	f (par la table 2)
e :	h (par la table 3)	**i** :	s (par la table 3)
c :	p (par la table 1)	**q** :	d (par la table 1)
t :	m (par la table 2)	**u** :	h (par la table 2)
r :	i (par la table 3)	**e** :	h (par la table 3)

On trouve : « ***rshpmibfsdhh*** ». On se rend compte tout de suite que ce chiffrement est plus difficile à « casser » que la substitution monoalphabétique. Car à n lettres différentes (si nous avons n tables) peuvent correspondre une seule et même lettre (la méthode utilisant les fréquences tombe à l'eau).

La substitution homophonique : qui permet de faire correspondre les lettres du message en clair à un ensemble possible d'autres caractères.

La substitution de polygramme : qui consiste à remplacer un groupe de caractères dans le message par un autre groupe de caractères.

iii.2. Le système DES

Historique [12]

Le 15 mai 1973 le **NBS** a lancé un appel pour la création d'un algorithme de chiffrement.

Fin 1974, IBM propose « Lucifer », qui, grâce à la NSA, est modifié le 23 novembre 1976 pour donner le DES. Le DES a finalement été approuvé en 1978 par le NBS. Le DES fut normalisé par l'ANSI sous le nom de ANSI X3.92, plus connu sous la dénomination DEA.

Principe du DES [9]

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de « 1 » dans l'octet à qui il appartient. La clé possède une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme.

L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). La combinaison entre substitutions et permutations est appelée code produit.

La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k1 à k16. Etant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 256 (soit 7,2*1016) clés différentes.

L'algorithme du DES [9]

Comme le paragraphe précédent a mentionné, le DES manipule un en clair par bloc de 64 bits. Ce bloc de texte subit en premier lieu une permutation initiale. Ensuite le bloc est coupé en deux parties : la partie droite et la partie gauche de longueur de 32 bits chacun. Après cela il y a 16 rondes opérations identiques, appelée « fonction f » (Fig. 3.2), qui consistent à combiner les données avec la clé. Après la 16eme ronde, les deux parties sont rassemblées et une permutation finale termine l'algorithme.

A chaque ronde, les bits de la clé sont décalés et 48 bits sont sélectionnés par une permutation compressive. La partie droite des données est étendue à 48 bits par une permutation expansive (notée P.E) puis elle est combinée avec 48 bits de la clé décalée par un « xor ». Le résultat est soumis à une opération de substitution (notée S) qui les ramène à 32 bits et de nouveau il subit une simple permutation (notée P). La fonction f est constituée de ces 4 opérations. La sortie de la fonction f est alors combinée avec la partie gauche par un « xor ». Le résultat devient la nouvelle moitié droite, l'ancienne moitié droite devient la nouvelle moitié gauche. Ces opérations sont répétées 16 fois le DES à 16 rondes.

Les parties gauche et droite du DES est généralisées par la formule suivante :

$$\begin{cases} G_i = D_{i-1} \\ D_i = G_{i-1} \oplus f(D_{i-1}, k_i) \end{cases}$$

Avec G_i et D_i sont les résultats de la i^{ème} itération respectivement de la partie gauche et celle de la droite.

Et k_i est la clé de 48 bits pour i^{ème} ronde.

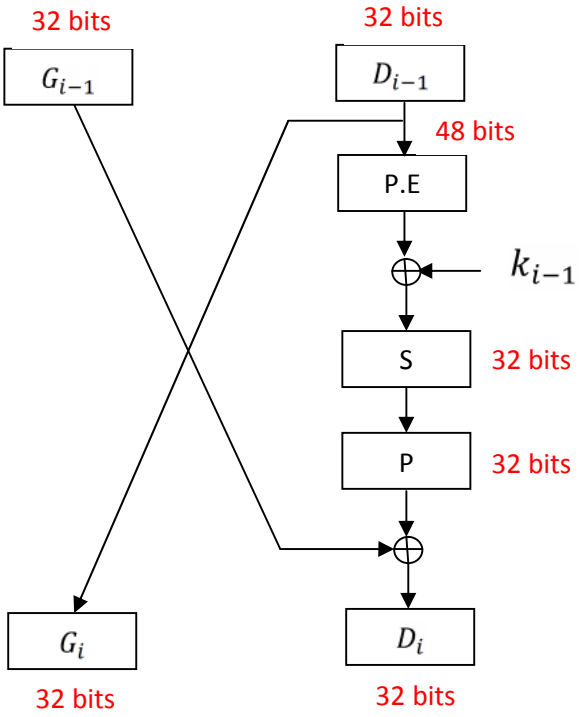


Figure 3.2: Ronde du DES

La permutation initiale et finale [9]

C'est une permutation bit à bit qui transpose le bloc de 64 bits d'entrée avant la 1ère ronde. Cette permutation est difficile à réaliser en logiciel de nombreuse réalisation logiciel du DES n'inclut pas les permutations.

Tandis que la permutation finale est l'inverse de la permutation initiale.

Le plan de la génération de clé [9]

Après que la clé de 56 bits est extraite, une clé de 48 bits est engendrée pour chaque ronde de DES (Fig. 3.3).

- la clé de 56 bits est divisée en deux moitié (28 bits chacune).

- les moitiés sont décalées vers la gauche d'une ou deux positions en fonction de la ronde (Tab. 3.2). Les décalages ont pour effets de différencier les sous-ensembles de bit utilisé dans chacune de sous clé.

- 48 bits parmi les 56 sont sélectionnés. Cette opération est appelée permutation compressive car elle combine une permutation de bit avec une sélection d'un sous-ensemble de bit.

Tableau 3.2 : Nombre de décalage de clé en fonction de ronde

Ronde	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Nombre de décalage	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

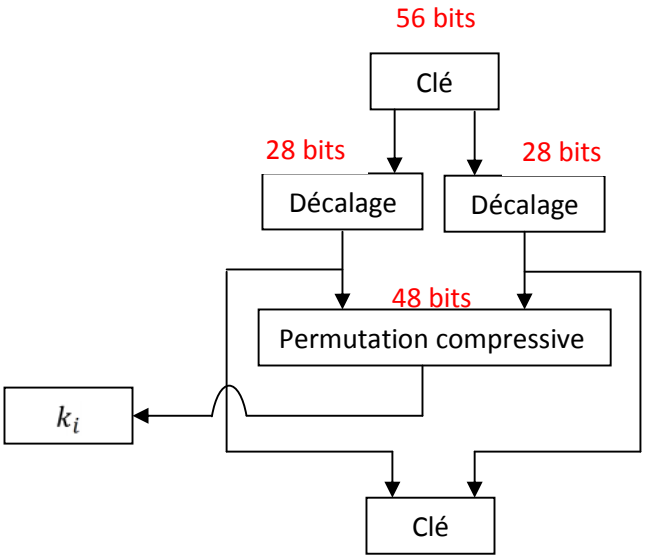


Figure 3.3: Algorithme de la clé

La permutation expansive [9]

C'est une opération qui étend la moitié droite de la donnée de 32 bits à 48 bits. Elle change l'ordre des bits et répète certain bits.

iv) Les chiffrements symétriques en continus

Le chiffrement en continu est un chiffrement qui travaille bit par bit ou octet par octet. En anglais, c'est « Stream cipher » ou chiffrement par flot. Quelquefois, on l'appelle « State cipher » chiffrement dépendant d'un état interne [13].

C'est la combinaison d'un texte en clair en ou exclusif avec un flot de clés obtenu par un générateur de nombres pseudo aléatoires. La même clé ne doit jamais être utilisée deux fois. C'est une solution rapide en chiffrement, et plus facile à implanter en matériel (solution appréciée des électroniciens).

iv.1. A5/1

A5/1 est un algorithme de chiffrement par flot utilisé dans le cadre des communications GSM. Il génère une suite pseudo-aléatoire avec laquelle on effectue un XOR avec les données. L'algorithme A5 utilise une clé de 64 bits mais son implémentation dans le GSM n'utilise que 54 bits effectifs (10 bits sont mis à zéro). En 2000, on comptait environ 130 millions d'utilisateurs du GSM basé sur A5/1.

iv.2. RC4

RC4 a été conçu par Ronald Rivest de RSA Security en 1987. Officiellement nommé Rivest Cipher 4.

L'algorithme est utilisé dans la spécification de téléphone modulaire. Les raisons de son succès sont liées à sa grande simplicité et à sa vitesse de chiffrement. Les implémentations matérielles ou logicielles sont faciles à mettre en œuvre.

La longueur de la clé varie de 1 à 256 bits. En pratique, elle est souvent choisie de taille égale à 5 octets (pour 40 bits) ou 16 octets (pour 128 bits).

b. Les chiffrements asymétriques

i) Historique [8]

Le concept de cryptographie à clé publique, autre nom de la cryptographie asymétrique, est dû à Whitfield Diffie et à Martin Hellman. Il fut présenté pour la première fois à la National Computer Conference en 1976, puis publié quelques mois plus tard dans New Directions in Cryptography.

Dans leur article de 1976, W. Diffie et M. Hellman n'avaient pas pu donner l'exemple d'un système à clé publique, n'en ayant pas trouvé. Il fallut attendre 1978 pour avoir un premier exemple, dans l'article A Method for Obtaining Digital Signatures and Public-key Cryptosystems de Ronald Rivest, Adi Shamir et Leonard Adleman, le RSA, abréviation tirée des trois noms de ses auteurs. C'est du moins la version académique. Les trois hommes fondèrent aussi la société RSA Security.

ii) Définition [8]

La **cryptographie asymétrique** permet à tous d'envoyer un message chiffré à une personne de sorte à que celle-ci seule puisse le décoder, sans qu'elle n'ait besoin de divulguer la clé privée servant à déchiffrer**.**

iii) Principe [8]

La **cryptographie asymétrique** est fondée sur l'existence de fonctions à sens unique, une fois la fonction appliquée à un message, il est extrêmement difficile de retrouver le message original.

En réalité, on utilise en cryptographie asymétrique des fonctions à sens unique et à brèche secrète. Une telle fonction est difficile à inverser, à moins de posséder une information particulière, tenue secrète, nommée clé privée.

À partir d'une telle fonction, voici comment se déroulent les choses : Alice souhaite pouvoir recevoir des messages chiffrés de n'importe qui.

1. Alice génère deux clés. La clé publique verte qu'elle envoie à Bob et la clé privée rouge qu'elle conserve précieusement sans la divulguer à quiconque (Fig. 3.4).

2. Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffre.

3. Alice déchiffre le message grâce à sa clé privée (Fig. 3.5).

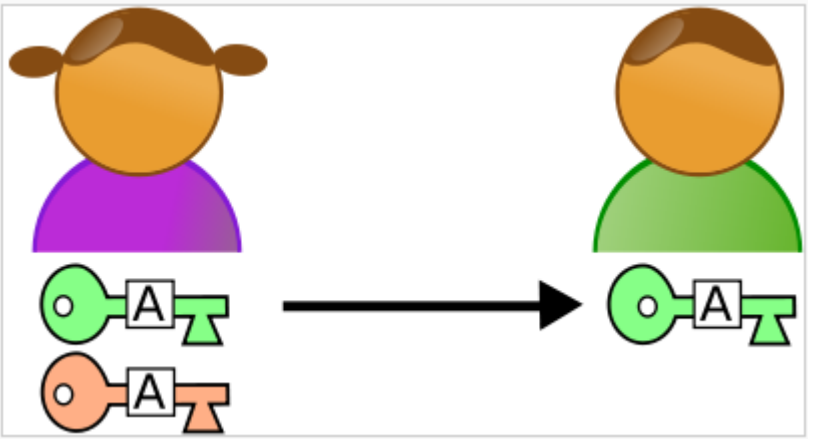


Figure 3.4: 1ère étape du principe d'authentification

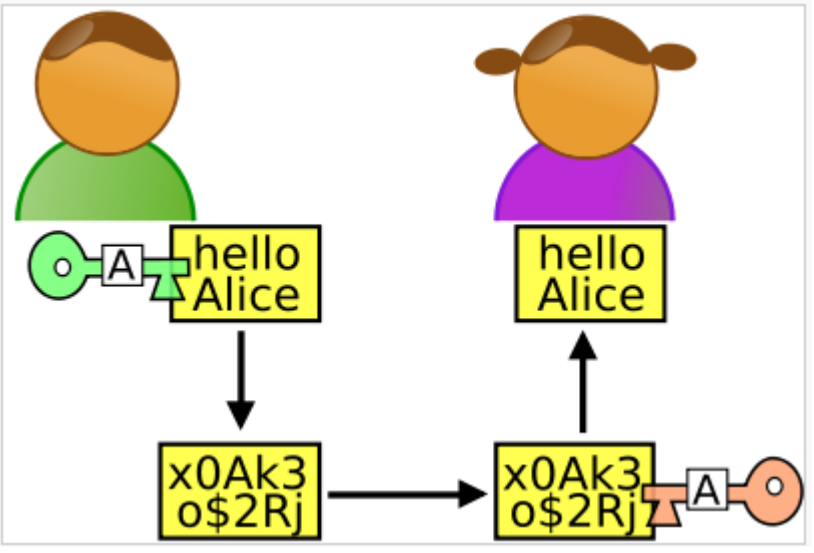


Figure 3.5: 2e et 3e étape du principe d'authentification

iv) ***RSA*** [8]

Rivest Shamir Adleman ou RSA est un algorithme asymétrique de cryptographie à clé publique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été décrit en 1977 par Ron Rivest, Adi Shamir et Len Adleman, d'où le sigle RSA. RSA a été breveté par le MIT en 1983 aux États-Unis. Le brevet a expiré le 21 septembre 2000.

En 2008, c'est le système à clef publique le plus utilisé (carte bancaire française, de nombreux sites web commerciaux…)**.**

Voici la fonction de chiffrement notée E (partie publique) [13] :

La clé publique comporte deux entiers: $k = (e, n)$.Le chiffrement est effectué par bloc de M. On élève M à la puissance e modulo n:

$$E_k(M) = M^e (mod\, n)$$

Et la fonction de déchiffrement notée D (partie secrète) :

La clé secrète est un couple d'entiers: $k' = (d, n)$.On procède à un déchiffrement d'un bloc chiffré C sur b bits. Et on élève C à la puissance d modulo n: $D_{k'}(C) = C^d (mod\, n)$

Remarque: Les entiers n, e, d doivent être choisis selon des règles précises.

D'après les paragraphes précédents, RSA a besoin de deux clés [15] : la clé publique et la clé privée.

Et pour la détermination de la clé publique, c'est-à-dire la valeur (***e***, ***n***), il faut :

- Choisir deux entiers premiers p et q (différents, grands et aléatoires).

- Calculer $n = p \square q$.

- Calculer $z = (p - 1)(q - 1)$.

- Choisir un entier ***e*** premier avec ***z*** (***1<e<z***, ***e*** et ***z*** n'ont pas de diviseurs communs).

La sécurité de RSA repose sur la difficulté de factoriser un entier n en deux entiers premiers p et q, n (grand) peut avoir les valeurs suivantes : 320 bits, 512 bits, 1024 bits …. La taille de n conditionne la vitesse de chiffrement et de déchiffrement.

Et pour la détermination de la clé privée, c'est-à-dire le couple de valeurs (d, n), il faut :

- Choisir un entier d tel que :

$e^d = 1 (mod\ z)$, d est un inverse de e dans l'arithmétique modulo z
(soit encore $e^d = k(p-1)(q-1) + 1$).

Remarque :

La contrainte de RSA est que les blocs à chiffrer M sont des entiers inférieurs à l'entier n

- M plus petit que n => les calculs sont conduits modulo n.

- Exemple : si on choisit n sur $d+1$ bits, on chiffre des messages M de d bits (taille inférieure) alors les messages chiffrés sont sur $d+1$ bits (restes modulo n).

- Autre aspect: utilisation d'une méthode de bourrage des messages en clair courts pour ne pas chiffrer de trop petites valeurs.

CHAPITRE 4 : La cryptographie et le traitement du son

4.1. Principe du codage audio

a. Synoptique du cryptage

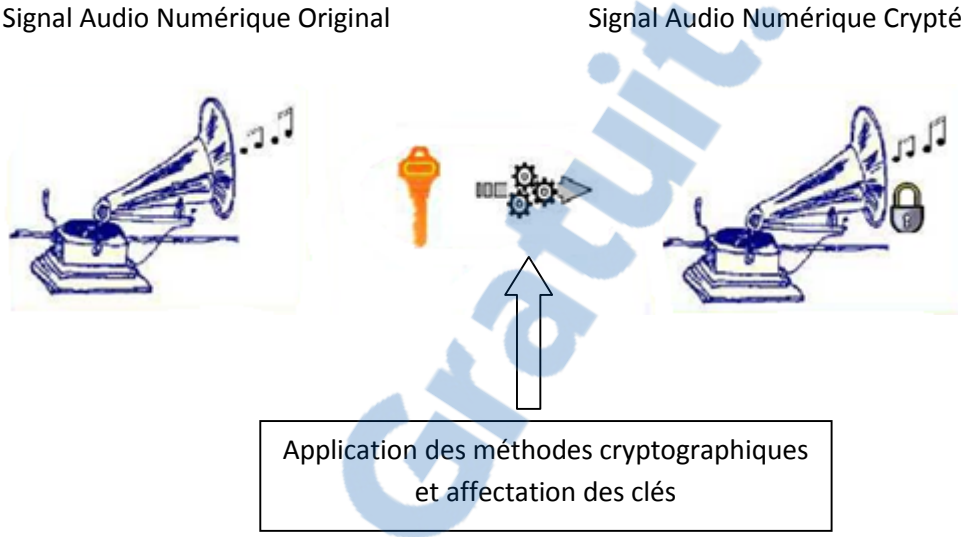


Figure 4.1 : Chaîne du cryptage Audio Numérique

b. Principes

i) Choix de la méthode de cryptage

Malgré les divers types de méthodes cryptographiques utilisés dans le domaine de la cryptographie pour le chiffrement ou le déchiffrement des informations [15], la méthode de cryptage utilisée dans le domaine Audio Numérique représentée dans cet ouvrage est classée à part. En effet, ici il n'est pas nécessaire d'utiliser les méthodes de chiffrement par bloc, par chaîne ou autre [15], car de la Transformée de Fourier apportée par la théorie du Traitement numérique de signal [14] on peut visualiser le spectre d'un Signal Audio, avec des notions complémentaires de programmation quelques que soient les langages que vous connaissez.

Ainsi, on peut baser notre recherche de la méthode de cryptage audio [4] en étudiant directement le spectre du signal. D'où la méthode qu'on a choisie ici consiste en *une inversion de spectre* du signal audio par le principe de *Modulation d'Amplitude* au tour de 12.8khz.

ii) Clé utilisée pour le chiffrement

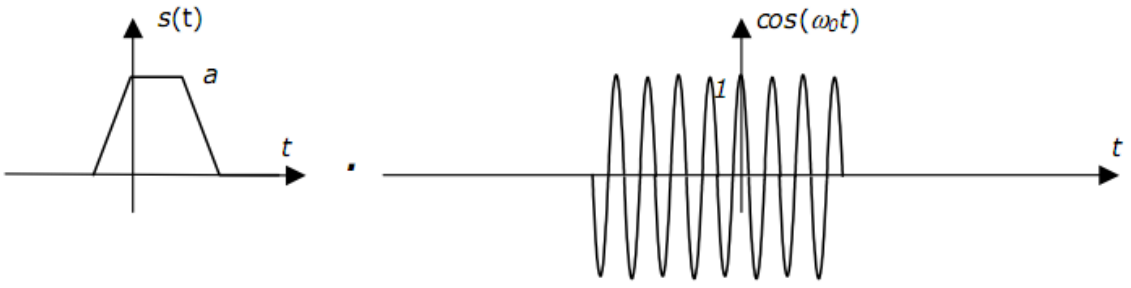
Après le choix de la méthode du cryptage, il est nécessaire de spécifier la clef de chiffrement. Pour en savoir de plus, intéressons nous à l'étude approfondie de la *Modulation d'Amplitude*.

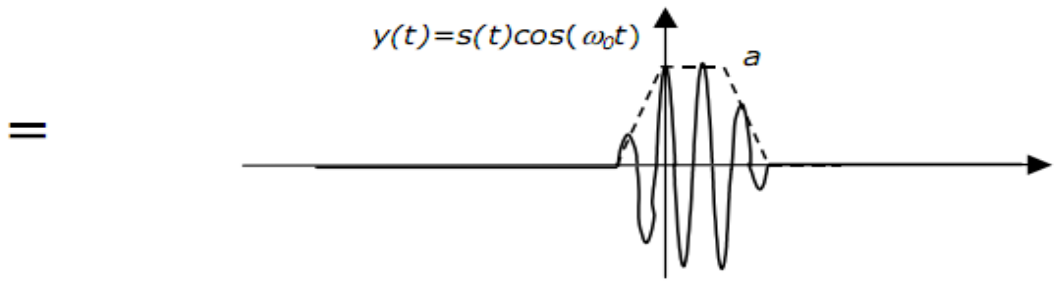
Rappelons par un exemple théorique ce qu'est un signal modulé en Amplitude. Soit s(t) un signal réel, de spectre limité par f_{bb} et $f_{bh,}$ sans composante continue, et $\cos(\omega_0 t)$ une onde périodique réelle de pulsation fondamentale ω_0 ($\omega_0 = 2\pi f_0$).

Le spectre du signal s(t)cos ($\omega_0 t$) résulte de la translation, sur l'axe des pulsations, de $\pm\omega_0$ du spectre de s(t) (Fig. 4.2).

Analyse temporel

Signal s(t) multiplié par le signal cos ($\omega_0 t$)





Analyse fréquentiel

Convolution de S(f) avec TF [cos (ω_0t)]

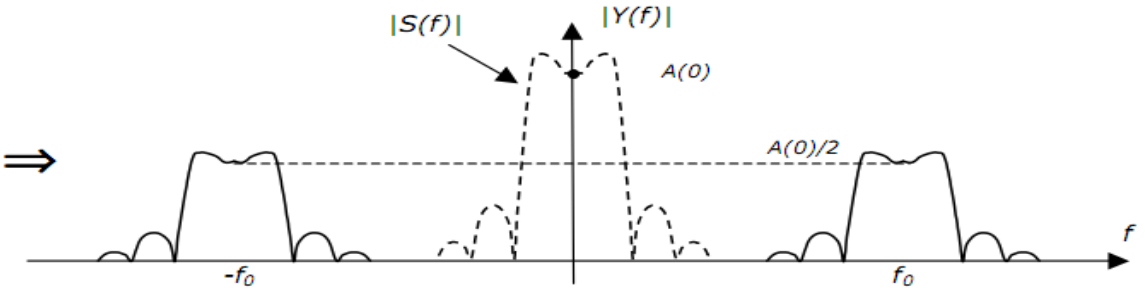


Figure 4.2 : Modulation d'amplitude

En effet le développement en séries de Fourier de cos (ω_0t) comprend deux termes d'amplitude ½ (Fig. 4.3):

$$\cos(\omega_0 t) \overset{F}{\Leftrightarrow} \frac{1}{2}[\delta(f - f_0) + \delta(f + f_0)]$$

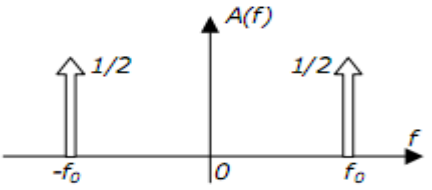


Figure 4.3 : Transformé de Fourier d'un cosinus

Le produit s(t).cos (ω_0t) correspond à la convolution des transformés de Fourier de s(t) et cos (ω_0t) [3], et que la convolution d'un signal par une impulsion de Dirac correspond au déplacement de ce signal au droit de l'impulsion, et à une multiplication par son poids (Fig. 4.2).

Ainsi, la clef du chiffrement utilisée pour le cryptage audio est un signal de type « bcos(2π12800t + Φ) » dont le fonctionnement est décrit ci après avec la méthode de la Modulation d'Amplitude .

Le principe de la Modulation d'Amplitude pour le cryptage audio consiste ici à multiplier le signal non codé en bande de base par un signal de type « bcos(2π12800t + Φ) ».

Dans l'exemple théorique donnée à la section précédente, les spectres translatés ne se recouvrent pas car on a supposé que $f_0 > f_{bh.}$ Cette condition n'est visiblement pas vérifiée dans le cas du codage utilisé pour l'Audio Numérique. En effet le spectre d'un signal audible s'étend jusqu'à 20 kHz. Pour qu'il n'y ait pas de recouvrement des 2 spectres translatés, on procède d'abord à un filtrage passe bas (dont la fréquence de coupure est choisie précisément à 12.8 kHz) du signal non codé en bande de base. On procède ensuite à la modulation.

iii) Visualisation spectrale du mécanisme

Ici nous allons appliquer la méthode de la Modulation d'Amplitude pour le cryptage d'un signal réel s(t) qui sera filtré puis modulé.

Processus du cryptage vu spectral

Spectre du signal original s(t)

Spectre du signal s(t) filtré

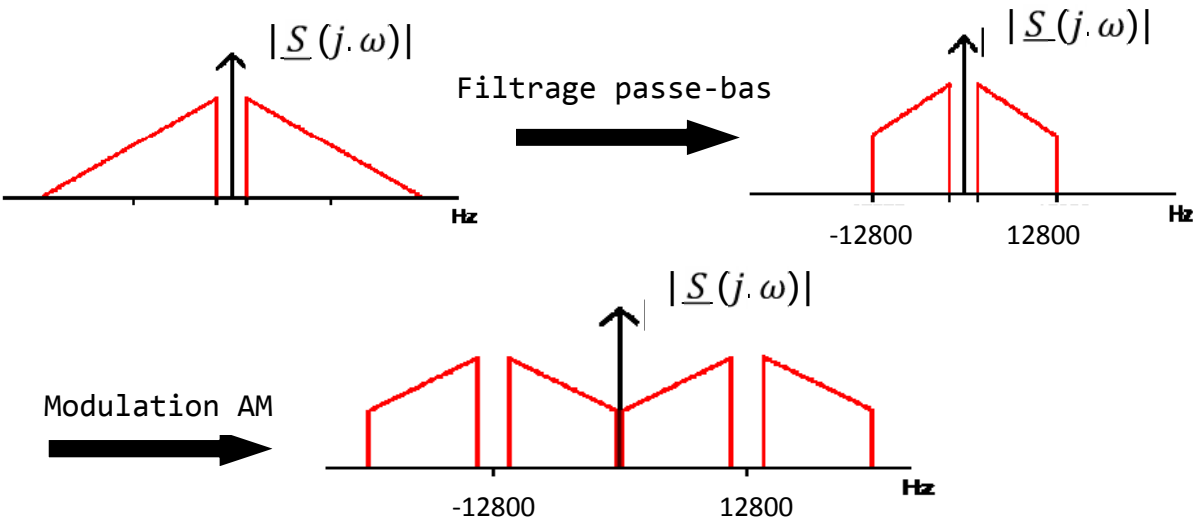


Figure 4.4 : Processus de cryptage d'un signal s(t) par Modulation d'Amplitude

iv) Résultat du cryptage avec un Audio Numérique

Le résultat qu'on devrait avoir pour le cryptage Audio est le même que ce obtenu avec le cryptage d'un signal réel quelconque étudié ci-dessus car le signal Audio Numérique est un signal réel.

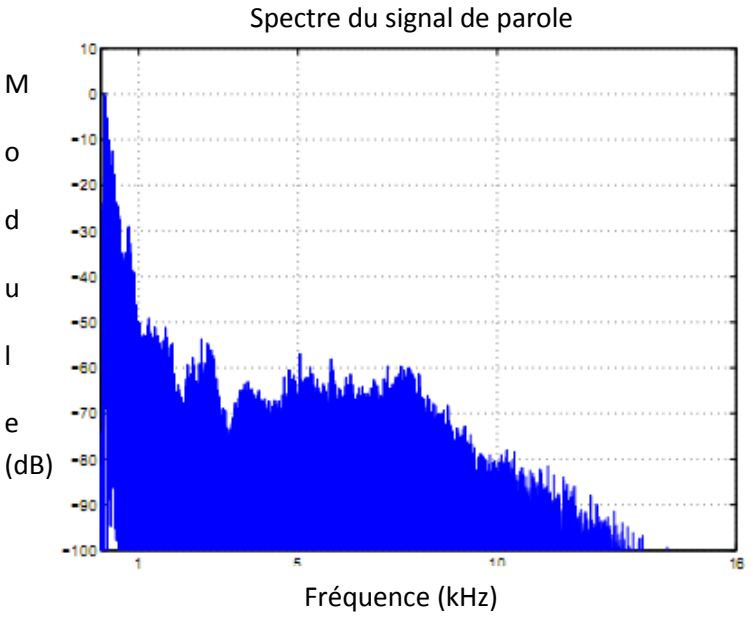


Figure 4.5 : Spectre d'un des extraits Audio

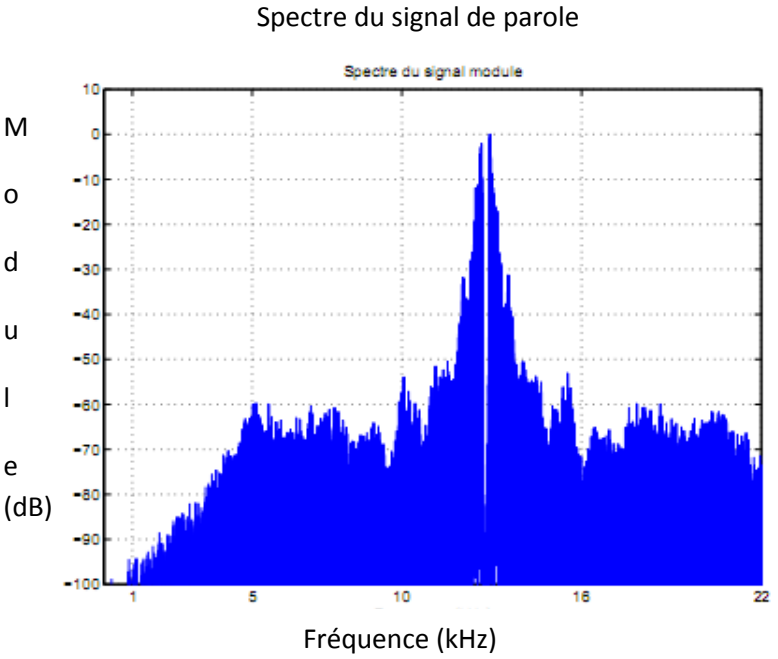


Figure 4.6 : Spectre de l'extrait Modulé

4.2. Principe du décodage audio

a. Synoptique du décryptage

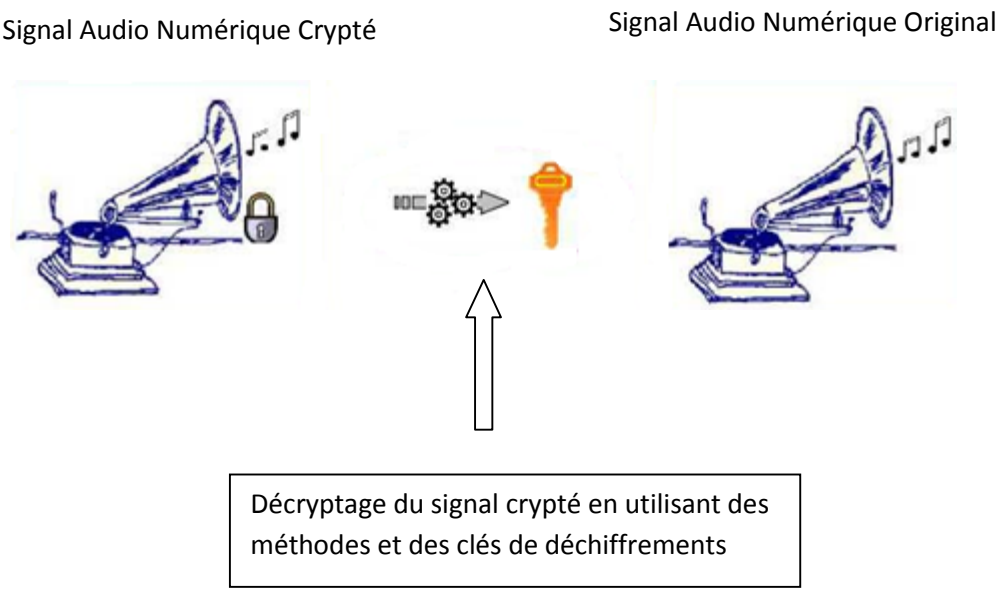


Figure 4.7 : Chaîne du décryptage Audio Numérique

b. Principes

i) Méthode de décryptage

Ici le décryptage consiste à démoduler le signal crypté pour retrouver le signal initial. La modulation est alors appliquée une nouvelle fois pour inverser le spectre, mais auparavant on doit filtrer passe-bas le signal ainsi obtenu pour ne conserver que la partie nécessaire du spectre comme on peut le voir sur le spectre du signal modulé de la Fig. 4.6.

Après avoir démodulé le signal, on doit appliquer un nouveau filtrage passe-bas [4] pour ne conserver que la partie du spectre de fréquence inferieure à la fréquence de modulation de 12800Hz.

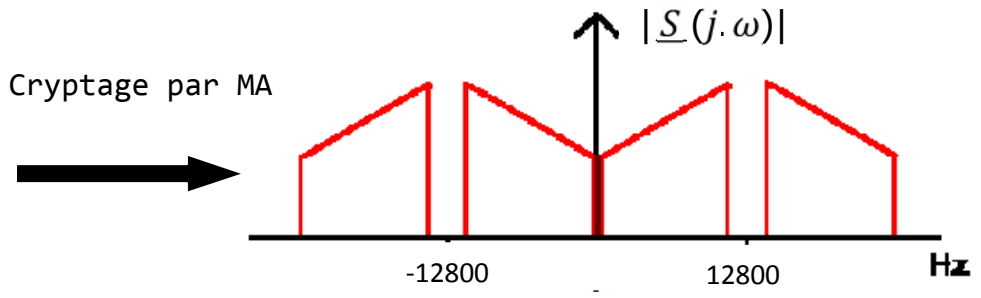
ii) Clé de déchiffrement

Comme la méthode de déchiffrement utilisée est la Modulation d' Amplitude, alors la clef du décryptage [16] est la même que celle utilisée pour le chiffrement. Le signal crypté qui est réel, est ainsi multiplié par un signal sinusoïdal de fréquence 12800Hz.

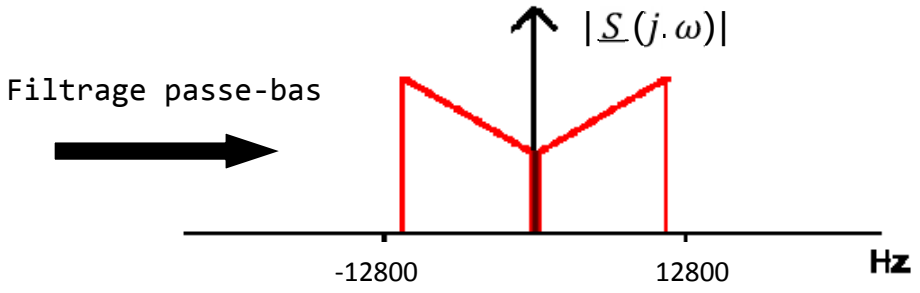
iii) Spectral du résultat

Voyons d'abord le principe de ce décryptage avec un signal réel crypté quelconque s(t) avant de l'appliquer au signal Audio Numérique.

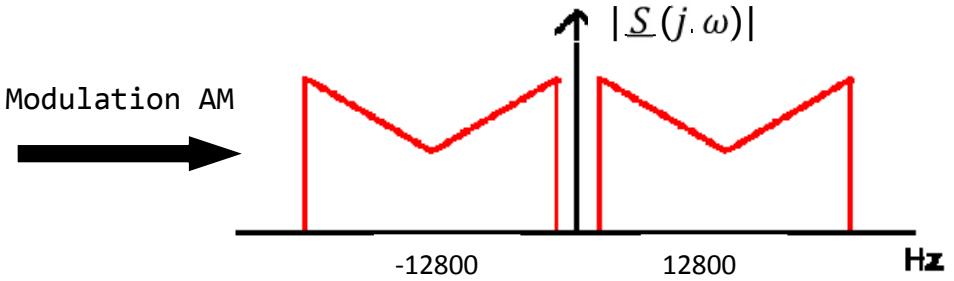
Spectre du signal s(t) Crypté



Spectre du signal s(t) Filtré



Spectre du signal s(t) Modulé en Amplitude



Spectre du signal s(t) Filtré après Modulation

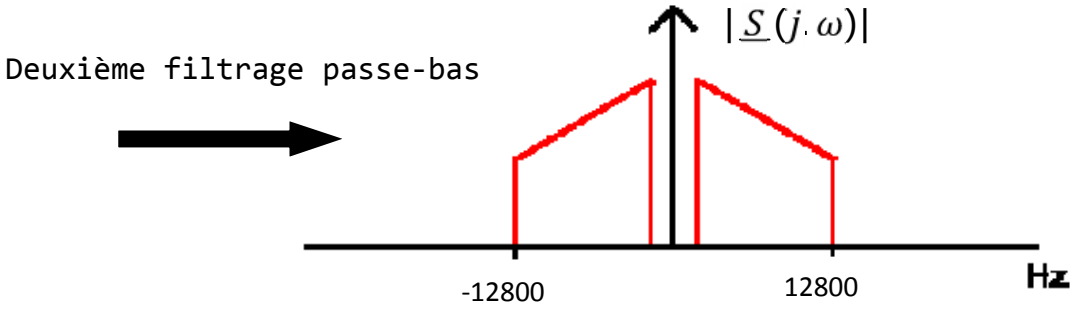


Figure 4.8 : Processus de décryptage d'un signal crypté s(t)

Cette méthode appliquée au décodage d'un signal Audio Numérique nous donne le résultat spectral ci-dessous.

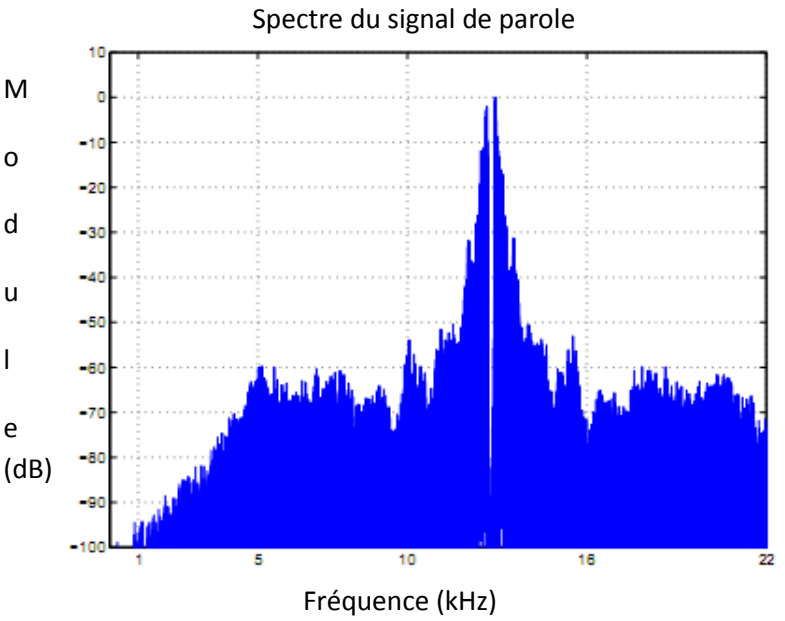


Figure 4.9 : Spectre d'un extrait audio crypté

Apres le filtrage passe-bas, une Modulation d'Amplitude et un deuxième filtrage passe-bas [4], on obtient le signal Audio Numérique original présenté par la figure 4.10.

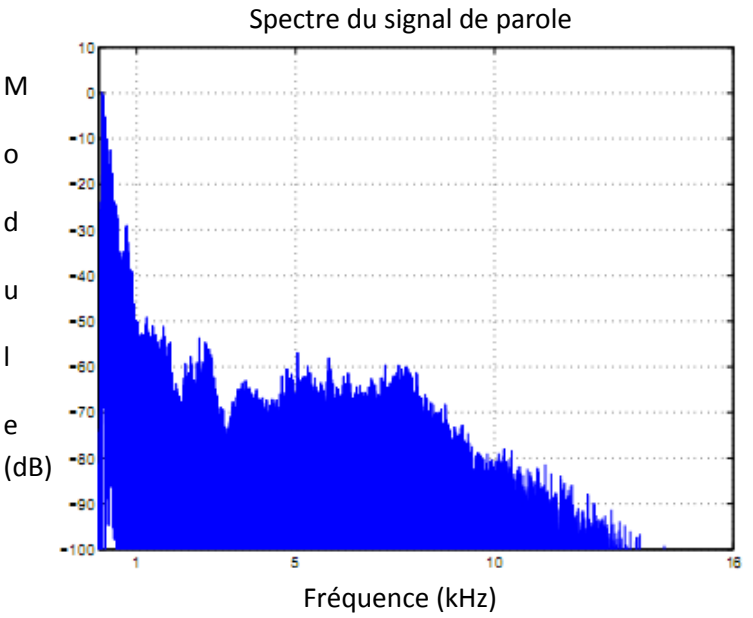


Figure 4.10 : Spectre de l'extrait du signal Audio Numérique original

CONCLUSION

La cryptographie est un domaine le plus connu actuellement surtout dans les pays développés. Elle permet de cacher des données confidentielles à une certaine personne. On l'utilise surtout dans le domaine de l'informatique et de la télécommunication. On peut la recourir aussi dans le traitement d'un son numérique. A part les différents types du système cryptographique, une autre manière de crypter un son numérique est la modulation et la démodulation d'amplitude qui est plus facile à réaliser.

Pour bien préserver la confidentialité des données, on peut envisager de combiner la méthode de la modulation d'amplitude et l'une des méthodes propre à la cryptographie telle que le DES, RSA, etc. Mais cette combinaison exige une profonde connaissance à la programmation que ce soit le langage ou l'algorithme. Et ceci augmente la difficulté de déchiffrer les données sans la clé de déchiffrement.

ANNEXE

ANNEXE : OUTILS DE TRAITEMENT DU SIGNAL

1. Des signaux particuliers

Afin de simplifier les opérations, ainsi que les formules obtenues, certains signaux fréquemment rencontrés en traitement du signal disposent d'une modélisation propre.

a. Fonction signe

Représentation mathématique :

$$sgn(t) = \begin{cases} -1 & pour \quad t < 0 \\ +1 & pour \quad t > 0 \end{cases}$$

Courbe correspondante :

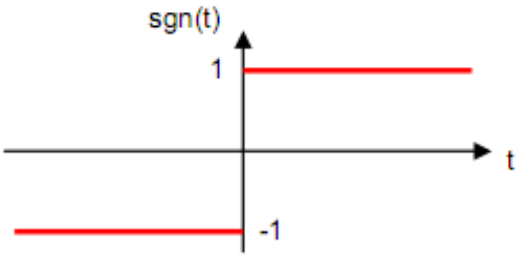


Figure A.1 : Modélisation de la fonction *signe*

Par convention, on admet pour valeur à l'origine : sgn (t) = 0 pour t=0.

b. Fonction Echelon

Représentation mathématique :

$$u(t) = \begin{cases} 0 & pour \quad t < 0 \\ 1 & pour \quad t > 0 \end{cases}$$

Courbe correspondante :

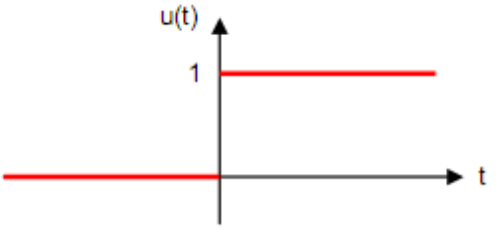


Figure A.2 : Modélisation de la fonction *Echelon*

Par convention, on admet pour valeur à l'origine : u (t) = ½ pour t=0.

Dans certains, il sera préférable de lui donner la valeur 1.

c. Fonction Rampe

Représentation mathématique :

$$r(t) = t.u(t)$$

$$= \int_{-\infty}^{t} u(\tau)d\tau$$

Courbe correspondante :

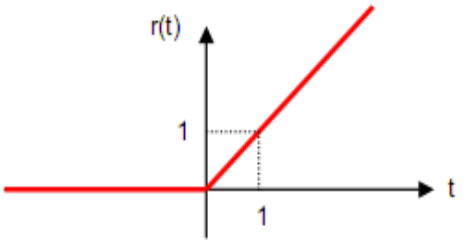


Figure A.3 : Modélisation de la fonction *Rampe*

d. Fonction rectangulaire

Représentation mathématique :

$$rect\left(\frac{t}{T}\right) = \begin{cases} 1 \ pour & \left|\frac{t}{T}\right| < \frac{1}{2} \\ 0 \ pour & \left|\frac{t}{T}\right| > \frac{1}{2} \end{cases}$$

Courbe correspondante :

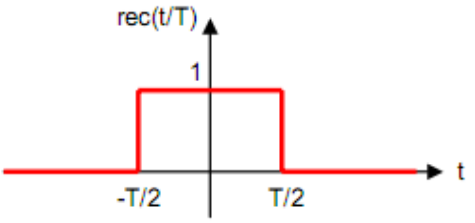


Figure A.4 : Modélisation de la fonction *Rectangulaire*

On l'appelle aussi fonction porte. Elle sert de fonction de fenêtrage élémentaire.

e. Impulsion de Dirac

L'impulsion de Dirac correspond à une fonction porte dont la largeur T tendrait vers 0 et dont l'aire est égale à 1.

Représentation mathématique :

$$\delta(t) = \begin{cases} \infty & pour \quad t = 0 \\ 0 & pour \quad t \neq 0 \end{cases}$$

Courbe correspondante

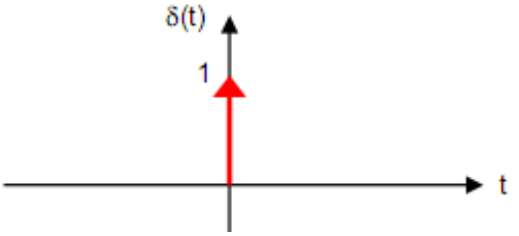


Figure A.5 : Modélisation de l'*Impulsion de Dirac*

δ(t) ne peut être représentée graphiquement. On la schématise par le symbole $\uparrow^{1}$, Le 1 marqué sur la flèche pleine représente l'aire de cette impulsion (et non la hauteur de l'impulsion).

Quelques propriétés

Intégrale

$$\int_{-\infty}^{+\infty} \delta(t)\, dt = 1$$

$$\int_{-\infty}^{+\infty} x(t).\delta(t)\, dt = x(0)$$

$$\int_{-\infty}^{+\infty} x(t).\delta(t - t_0)\, dt = x(t_0)$$

Produit

$$x(t).\delta(t) = x(0).\delta(t) = x(0)$$

$$x(t).\delta(t - t_0) = x(t_0).\delta(t - t_0) = x(t_0)$$

Identité

$$x(t) \square \delta(t) = x(t)$$

Translation

$$x(t) \square \delta(t - t_0) = x(t - t_0)$$

$$x(t - t_1) \square \delta(t - t_0) = x(t - t_1 - t_0)$$

Changement de variable

$\delta(a.t) = |a|^{-1}\,\delta(t)$ avec en particulier $\delta(\omega) = \frac{1}{2\pi f}\,\delta(t)$

f. Peigne de Dirac

On appelle peigne de Dirac une succession périodique d'impulsions de Dirac.

Représentation mathématique :

$$\delta_T(t) = \sum_{k=-\infty}^{+\infty} \delta(t - kT)$$

⟶ *T est la période du peigne*

Courbe correspondante :

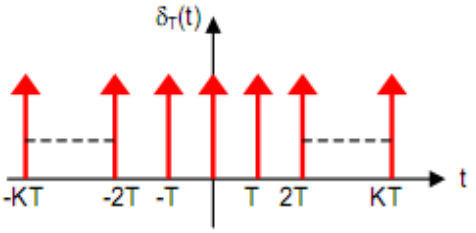


Figure A.6 : Modélisation d'une *Peigne de Dirac*

Cette suite est parfois appelée ***train d'impulsions***.

C'est un signal utilisé principalement en échantillonnage.

g. Fonction sinus cardinal

Représentation mathématique :

$$sinc\,(t) = \frac{sin\,(\pi t)}{\pi t}$$

Courbe correspondante :

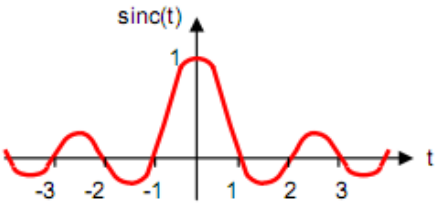


Figure A.7 : Modélisation de la fonction *sinus cardinal*

Cette fonction joue un rôle très important en traitement du signal.

Quelques propriétés sur le calcul d'intégral

$$\int_{-\infty}^{+\infty} sinc(t)\,dt = 1$$

$$\int_{-\infty}^{+\infty} sinc^2(t)\,dt = 1$$

2. Représentation fréquentielle

On a pour habitude de décrire les signaux en fonction de la variable temporelle t car notre perception des phénomènes physiques nous y incite. En électronique, la connaissance des propriétés spectrales d'un signal est primordiale.

Ainsi, on utilise souvent une représentation en fonction de la fréquence pour caractériser un signal ou un système. Les outils de traitement des signaux nous aident dans cette tâche.

3. Série de Fourier

a. Définition

La décomposition en série de Fourier [16] permet de décomposer un signal en somme de sinusoïdes. On utilise principalement les séries de Fourier dans le cas des signaux périodiques. Elles permettent ainsi de passer facilement du domaine temporel au domaine fréquentiel. Pour pouvoir être décomposable, un signal doit être à variations bornées (Dirichlet).

Pour tout signal s(t) réel où $s(t) = s(t+T_0)$, on peut écrire :

$$s(t) = S_0 + \sum_{n=1}^{\infty}[A_n\ cos(n\omega_0 t) + B_n\ sin(n\omega_0 t)] \qquad \text{Où} \qquad \omega_0 = \frac{2\pi}{T_0}$$

Avec

$$S_0 = \frac{1}{T_0} \int_{(T_0)} s(t)dt$$

$$A_n = \frac{2}{T_0} \int_{(T_0)} s(t)\cos(n\omega_0 t)dt \qquad (A.1)$$

$$B_n = \frac{2}{T_0} \int_{(T_0)} s(t)sin(n\omega_0 t)dt \qquad (A.2)$$

On rappelle que :

- Le signal de pulsation ω_0 est le fondamental.
- Les signaux de pulsation $n.\omega_0$ sont les harmoniques de rang n.
- La valeur de S_0 représente la valeur moyenne de s(t).

L'écriture précédentes des séries de Fourier présente en fait peu d'intérêt physique, en effet si la fonction f(t) subit une simple translation suivant l'axe des temps alors les coefficients A_n et B_n seront modifiés. En conséquence, on cherche une nouvelle écriture des

séries de Fourier dans laquelle la puissance est conservée après une translation suivant l'axe des temps et où cette translation apparaîtra sous la forme d'un déphasage.

Cette nouvelle écriture s'obtient en remplaçant ***les équations*** **(A.1)** et **(A.2)** par :

$$\begin{cases} A_n = C_n \sin \Phi_n \\ B_n = C_n \cos \Phi_n \end{cases}$$

b. Développement en termes complexe

En introduisant la notation complexe de $\cos(n\omega_0 t)$ et $\sin(n\omega_0 t)$, il est possible d'obtenir une écriture complexe de la série de Fourier.

On pose :

$$cos(n\omega_0 t) = \frac{e^{jn\omega_0 t} + e^{-jn\omega_0 t}}{2}$$

$$\sin(n\omega_0 t) = \frac{e^{jn\omega_0 t} - e^{-jn\omega_0 t}}{2j}$$

On obtient alors :

$$s(t) = \sum_{-\infty}^{+\infty} S_n e^{jn\omega_0 t}$$

Avec

$$S_n = \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} s(t) e^{-jn\omega_0 t}$$

Les coefficients complexes S_n sont reliés aux coefficients A_n et B_n par les relations suivantes :

$$\begin{cases} S_n = \dfrac{A_n - jB_n}{2} \\ S_{-n} = \dfrac{A_n + jB_n}{2} \end{cases} \quad \forall n > 0$$

c. Propriétés

Si s(t) est paire ⟶ $B_n = 0$ et $S_n = S_{-n}$

Si s(t) est impaire ⟶ $A_n = 0$ et $S_n = -S_{-n}$

4. Transformée de Fourier

C'est une généralisation de la décomposition de série de Fourier à tous les signaux déterministes. Elle permet d'obtenir une représentation en fréquence (représentation spectrale) de ces signaux. Elle exprime la répartition fréquentielle de l'amplitude, de la phase et de l'énergie (ou de la puissance) des signaux considérés.

a. Définition

Soit s(t) un signal déterministe. Sa transformée de Fourier est une fonction, généralement complexe, de la variable f et définie par :

$$S(f) = TF[s(t)] = \int_{-\infty}^{+\infty} s(t)e^{-j2\pi ft}dt$$

Si cette transformée existe, la transformée de Fourier inverse est donnée par :

$$s(t) = TF^{-1}[S(f)] = \int_{-\infty}^{+\infty} S(f)e^{j2\pi ft}df$$

On rappelle que le module de la transformée de Fourier de s est appelé spectre de s.

b. Propriétés

Tableau A.1 : Propriétés de la Transformée de Fourier

	S(t)	S(F)
Linéarité	$\alpha.s(t) + \beta.r(t)$	$\alpha.S(f) + \beta.R(f)$
Transition	$s(t - t_0)$	$e^{-2j\pi f t_0}S(f)$
	$e^{2j\pi f_0 t}s(t)$	$S(f - f_0)$
Conjugaison	$s^{\square}(t)$	$S^{\square}(-f)$
Dérivation	$\frac{d^n s(t)}{dt^n}$	$(j2\pi f)^n S(f)$
Dilatation	$s(at)\ avec\ a \neq 0$	$\frac{1}{\lvert a\rvert}S(\frac{f}{a})$
Convolution	$s(t) \square r(t)$	$S(f).R(f)$
	$s(t).r(t)$	$S(f).R(f)$
Dualité	$s(t)$	$S(-f)$

REFERENCES

[1] Zo Manankasina et Jessy Edouard, Livre de mémoire de fin d'étude intitulé : « Réalisation d'une suite complète d'acquisition, de génération et de traitement du son »

[2] http://www.techniquesduson.com/acoustique1.pdf

[3] http://lpce.cnrs-orleans.fr/~ddwit/enseignement/cours-signaux.pdf

[4] bruit.pdf (voir CD)

[5] E341, Cours Théorie du signal, 3ème Année, Département Electronique, ESPA, 2008,

[6] http://fr.wikipedia.org/wiki/Filtre_(%C3%A9lectronique)

[7] http://translate.google.mg/translate?hl=fr&langpair=en|fr&u=http://library.thinkquest.org/27887/gather/fundamentals/bandwidth.shtml

[8] www.esiee.fr%2F~francaio%2Fenseignement%2Fversion_pdf%2FV_theorie.pdf&rct=j&q=V_theorie.pdf

[9] Cours signaux et bruit, 2ème Année, Département Electronique, ESPA, 2006

[8] http://fr.wikipedia.org/wiki/Cryptographie.html

[9] E530, Cours Cryptographie, 5ème Année, Département Electronique, ESPA, 2009

[10] http://nicolastorres.free.fr/cryptoquantique/?part=1&spart=2.html

[11] http://sciences.ows.ch/informatique/Cryptographie.pdf

[12] http://www.commentcamarche.net/contents/crypto/des.php3

[13] http://deptinfo.cnam.fr/Enseignement/CycleProbatoire/SECURITE/cours_cryptographie.pdf

[14] http://www-prima.imag.fr/jlc/Courses/2000/ENSI2.TS/ENSI2.TS.S2.pdf

[15] http://www.hsc.fr/ressources/cours/crypto/crypto.pdf

Auteur : TOLOTRA Ambroise Vincent

Titre **: La cryptographie appliquée au traitement du son**

Nombre de pages : 40

Nombre de figures : 20

Nombre de tableaux : 2

RESUME

On peut appliquer à un son audio numérique le principe du cryptage et de décryptage. Ceci demande une bonne connaissance dans les domaines du traitement du signal et de la cryptographie. Il est important de savoir quelques paramètres lui caractérisant. Etant donné qu'un son numérique est aussi un donnée qu'on peut envoyer ou à transférer. Pour envoyer une donnée confidentielle, il est nécessaire de recourir à la cryptographie. Elle permet de transformer un message clair en un message inintelligible. Elle est caractérisée par les deux grandes catégories de chiffrement : celui de chiffrement symétrique utilisant une clé unique et celui de chiffrement asymétrique qui, par contre, utilise deux clés distinctes pour le chiffrement et le déchiffrement. On peut associer le traitement du son et celle de la cryptographie. Ici dans ce rapport, une autre manière de crypter un son numérique est élaborée, il s'agit du principe de modulation d'amplitude.

Mots clés : traitement, son, signal, modulation, cryptographie

Rapporteur : Monsieur ANDRIAMANANTSOA Guy Danielson

Adresse de l'auteur : *Lot 3/V1 Tanambao Mananjary 317*