N° d'ordre : 470/RS/TCO Année universitaire : 2017 / 2018

UNIVERSITÉ D'ANTANANARIVO

INSTITUT D'ENSEIGNEMENT SUPERIEUR ANTSIRABE VAKINANKARATRA (IES-AV)

MENTION TELECOMMUNICATION

MEMOIRE

en vue de l'obtention

du diplôme de LICENCE

Domaine : Sciences de l'Ingénieur

Mention : Télécommunication

Parcours : Réseaux et Systèmes

Par : **TODISOA Hasina Fanantenana**

Titre : SECURISATION DES DONNEES DIFFUSEES PAR EMETTEUR SW (SHORTWAVE)

Soutenu le 08 Avril 2019, devant la Commission d'Examen composée de :

Président de Jury :

- RANDRIANANDRASANA Marie Emile, Docteur en Télécommunication

Examinateurs :

- ANDRIANAIVONDRIAKA Nirina Alain, Docteur en Télécommunication
- RAFALINIRINA Haingomalala Sandra, Master à visée de recherche

Directeur de mémoire:

- RALAIBOZAKA Tahina Nancy Muriel, Assistante d'Enseignement Supérieur

TENY FISAORANA

Voalohany indrindra dia isaorana Andriamanitra izay nanome herin-tsaina sy tanjaka nahafahana nanatontosa ity voka-pikarohana ity.

Hisaorana lehibe koa ireto olona manaraka ireto izay nahatonga ny fahatontosan'izao zavatra atrehantsika izao dia ny "famaranana ny fianarana" :

- Andriamatoa RAMANOELINA Panja, Filohan'ny Oniversite Antananarivo ;
- Andriamatoa RAJAONARISON Eddie Franck, Tale an'ny Institut D'Enseignement Supérieur Antsirabe-Vakinankaratra (IES-AV) ;
- Andriamatoa RANDRIANANDRASANA Marie Emile, izay Lehiben'ny sampam-pampianarana "Télécommunication", sy filohan'ny mpitsara izay nanome alalana ahy mba nahafako namita izay dingana rehetra izay ;
- Ianareo mpampianatra izay nanaiky hitsara na dia betsaka aza ireo asa sahaninareo :
  - Andriamatoa ANDRIANAIVONDRIAKA Nirina Alain ;
  - Ramatoa RAFALINIRINA Haingomalala Sandra ;
- Ramatoa RALAIBOZAKA Tahina Nancy Muriel, izay nanampy akaiky sy nanoro ara-kevitra sy ara-toromarika amin'ny fanatontosana izao dingana izao.
- Andriamatoa RAHARIMAHEFA Diary Sambatra, izay nanaiky sy nandray ahy nanao ny andrana arak'asa izay fampiharana ny fahalalana noratoviko izao ;
- Eto koa dia tsy hay ny tsy hisaotra anareo mpampianatra rehetra ato amin'ny sampam-pampianarana "Télécommunication" izay maro aminareo no avy lavitra ka tonga nidododo tsy nitandro hasasarana fa nanao izay tratra nampita fahaizana sy fahalalana aminay.

Hoy ny Ntaolo Malagasy hoe "Ny hazo no vanon-ko lakana, ny tany naniriany no tsara" ka eto dia manaja anareo Ray aman-dReny izay nahafoy fotoana ho anay mba nafahanay nanaraka izao fandratoana fahalalana sy fahaizana izao.

Tsy adino ihany koa ianareo tapaka sy namana izay niara-nisalahy teo amin'ny fianarana, indrindra fa ianareo niezaka nanampy sy nanohana ara-kevitra koa dia maneho fisaorana anareo etoana ny tenako. Misaotra Tompoko.

REMERCIEMENTS

Je remercie Dieu Tout Puissant qui m'a donné la force et le courage de réaliser ce mémoire.

Je voudrais aussi adresser tous mes remerciements à tous ceux qui ont collaboré pour que ce travail soit réalisé avec succès, plus particulièrement :

- A Monsieur RAMANOELINA Panja, Professeur, Président de l'Université d'Antananarivo ;
- A Monsieur RAJAONARISON Eddie Franck, Professeur, Directeur de l'Institut d'Enseignement Supérieur Antsirabe Vakinankaratra (IES-AV) de nous avoir donné la permission de réaliser nos 3 années d'études au sein de l'IES-AV ;
- A Monsieur RANDRIANANDRASANA Marie Emile, Docteur, Responsable de mention Télécommunication à l'IES-AV, et président de jury de cette soutenance ;
- Aux membres de jury, qui ont bien accepté de juger et d'évaluer ce travail, composés de :
  - Monsieur ANDRIANAIVONDRIAKA Nirina Alain, Docteur en Télécommunication ;
  - Madame RAFALINIRINA Haingomalala Sandra, Master à visée de Recherche ;
- A Madame RALAIBOZAKA Tahina Nancy Muriel, Assistante d'Enseignement Supérieur, mon encadreur, qui m'a dirigé et m'encouragé énormément dans mes travaux de recherche et surtout de m'avoir accordé sa confiance ;
- A Monsieur RAHARIMAHEFA Diary Sambatra, Ingénieur, Encadreur Professionnel qui m'a permis d'effectuer un stage dans son département et de m'avoir encadré pour les matériels et techniques pour la réalisation de ce mémoire.

J'exprime toute ma gratitude à tous les enseignants intervenants ainsi que tous les personnels administratifs et technique au sein de l'IES-AV.

Toute ma famille particulièrement mes Parents, mes proches, mes amis et tous ceux qui ont collaboré, de près ou de loin à la réalisation de cet ouvrage.

Je vous prie de croire à mon profond attachement.

MERCI !

TABLE DES MATIERES

NOTATIONS ET ABREVIATIONS

1. Minuscules latines

a	Valeur numérique
b	Valeur numérique
c	texte chiffré
d	Distance de rayonnement
d_k	Fonction de déchiffrement
e_k	Fonction de chiffrement
f	Fréquence
f_0	Fréquence de la Bande Latérale inférieure et Bande Latérale supérieure
f_p	Fréquence de la porteuse
k	Décalage du mot
k	Taux de modulation
k_1	Taux de modulation d'indice 1
l	Position de la lettre
m	Message
m_r	Signal équivalent au signal d'information
p	Signal porteuse
p_2	Signal porteuse d'indice 2
r	Signal reçu
s	Signal en sortie du modulateur Amplitude Modulation
s_0	Signal d'information (message)
s_1	Signal d'indice 1 en sortie du mélangeur du démodulateur AM
s_2	Signal d'indice 2 en sortie du filtre passe-bas du démodulateur AM
s_{DSB}	Signal Double Side Band

t	temps
v	Célérité de la lumière dans le vide
w	Pulsation du signal $s(t)$
w_0	Pulsation de la porteuse p(t)
x	Valeur de la variable de l'algèbre de Boole soit 0 soit 1
y	Valeur de la variable de l'algèbre de Boole soit 0 soit 1
z	Valeur de la variable de l'algèbre de Boole soit 0 soit 1

2. Majuscules latines

A	Amplitude du signal $s(t)$
A_x	Composante de $\vec{A}$ suivant l'axe x
A_y	Composante de $\vec{A}$ suivant l'axe y
A_z	Composante de $\vec{A}$ suivant l'axe z
B	Amplitude du signal $p(t)$
C	Ensemble des textes chiffrés possible
D	Ensemble des fonctions de déchiffrement possible
D_k	Déchiffrement avec la clé
D_s	Durée en seconde
D_{Sk}	Déchiffrement avec clé secrète
E	Ensemble des fonctions de chiffrement possible
E_k	Chiffrement avec la clé
E_{Pk}	Chiffrement avec clé publique
F	Facteur de bruit
F_e	Fréquence d'échantillonage
G	gain

K	Ensemble des Clés possible
K_d	Clé de déchiffrement
K_e	Clé de chiffrement
M	Signal modulé
M_r	Signal démodulé
N_{in}	puissance du bruit dans le signal d'entrée
N_{out}	puissance du bruit dans le signal de sortie
N_s	Nombres de voies
P	Amplitude de la porteuse
P_{ds}	Capacité du son
P_k	Clé publique
P_{KA}	Clé publique pour entité A
P_{KB}	Clé publique pour entité B
P_r	Puissance reçue
P_R	Puissance du récepteur
P_t	Puissance de rayonnement émise par la source
Q	Ensemble des textes clairs possibles
R_A	Nombre aléatoire pour l'entité A
R_B	Nombre aléatoire pour l'entité B
R_s	Résolution du son
S_k	Clé secrète
S_{KA}	Clé secrète pour entité A
S_{KB}	Clé secrète pour entité B
S_r	Surface de rayonnement
T	Période

T_{min}	Seuil minimal de masquage
W	Largeur de bande
X_{k1}	Mélangeur

3. Minuscules grecques

ε_o	Permittivité dans le vide
ε_r	Permittivité relative
μ_o	Perméabilité dans le vide
μ_r	Perméabilité relative
λ	Longueur d'onde
ε	Permittivité
μ	Perméabilité
ρ	Densité de charge
ρ	Phase
σ	Conductivité du milieu

4. Majuscules grecques

Ω	Pulsation

5. Notations spéciales

$\vec{\nabla}$	Opérateur différentiel
$\vec{H}$	Intensité du champ magnétique
$\vec{J}$	Densité
$\vec{E}$	Intensité du champ électrique
$\vec{B}$	Flux magnétique

$\vec{A}$	Fonction vectorielle
$\vec{D}$	Flux électrique
$\overrightarrow{grad}\, V$	Gradient d'un champ scalaire V
$\vec{\imath};\vec{\jmath};\vec{k}$	Base du repère cartésien (x,y,z)
$\frac{\delta}{\delta x}$	Dérivée partielle par rapport à x
$\frac{\delta}{\delta y}$	Dérivée partielle par rapport à y
$\frac{\delta}{\delta z}$	Dérivée partielle par rapport à z
θ_p	Phase de la porteuse
$\nabla.$	Divergence d'un vecteur
$\nabla \times$	Rotationnel d'un vecteur
$\mathcal{F}[\,]$	Transformée de Fourier d'une fonction
XOR	Opérateur OU exclusif
OU	Opérateur OU logique
ET	Opérateur ET logique
mod	Modulo
rot	rotationnel
π	Pi
$\bar{\bar{x}}$	Revenir à la valeur de x
$\bar{x}$	Non "x"
$\bar{y}$	Non "y"

6. Abréviations

aac	Advanced Audio Coding

AES	Advanced Encryption Standard
AM	Amplitude Modulation
AM-DBAP	AM-Double Bande Avec Porteuse
AM-DBSP	AM-Double Bande Sans Porteuse
AWGN	Additive White Gaussian Noise
AWR	Adventist World Radio
BF	Basse Fréquence
BLi	Bande Latérale inférieur
BLs	Bande Latérale supérieur
BLU	Bande Latérale Unique
Codec	Codeur / Décodeur
Cos	Cosinus
dB	Décibel
DES	Data Encryption Standard
DSB	Double Side Band
DSBSC-AM	Double Side Band Suppressed-Carrier-Amplitude Modulation
EHF	Extremely High Frequency
FM	Frequency Modulation
GHz	GigaHertz
HF	High Frequency
IEEE	Institute of Electrical and Electronics Engineers
IES-AV	Institut d'Enseignement Supérieur Antsirabe Vakinankaratra
ISO	International Organization for Standarization
kHz	KiloHertz
km	Kilomètre

LF	Low Frequency
m	Mètre
MDCT	Modified Discrete Cosine Transform
MF	Medium Frequency
M-GLOB	Malagasy GLObal Business
MHz	MégaHertz
MP3	MPEG-1/2 Audio Layer 3
MPEG	Moving Picture Experts Group
MUF	Maximum Usable Frequency
Pa	Pascal
SHF	Super High Frequency
Sin	Sinus
SNR_{in}	Signal Noise Ratio en entrée
SNR_{out}	Signal Noise Ratio en sortie
SSB	Single Side Bande
SW	ShortWave
THz	Térahertz
TM	Traverse Magnétique
UHF	Ultra High Frequency
UIT	Union Internationale des Télécommunications
VHF	Very High Frequency
VLF	Very Low Frequency
wma	Windows Media Audio

LISTES DES TABLEAUX ET DES FIGURES

1. Liste des tableaux

2. Liste des figures

INTRODUCTION GENERALE

De nos jours, l'homme s'intéresse beaucoup à l'actualité qui se passe dans leur entourage que ce soit mondial ou pas et ces curiosités nous prouvent à quel point la transmission d'information occupe une très grande place dans la vie. Des nouvelles technologies ne cessent d'apparaitre toujours pour s'assurer une meilleure émission d'information entre deux lieux distants. Cette émission qui devrait-être rapide, efficace, couvrant de bonne qualité et ayant un coût moins élevé au sein d'un serveur qui l'utilise tel que la radiodiffusion.

En termes de cette radiodiffusion, comment devrait-on choisir la gamme de fréquence susceptible d'envoyer une information à longue distance ?

Comment va-t-on assurer la sécurisation des données pour ce soit diffusée aux personnes cibles ?

En général pour établir une liaison radio, il faut un émetteur et un récepteur, mais en termes de diffusion on s'intéresse un peu sur l'émetteur et que les informations émises doivent être sécurisées. Les objectifs de ce mémoire sont de :

- Elaborer la technique de transmission par onde courte ou ShortWave (SW) et ;
- Etablir une sécurisation de l'information envoyée par l'émetteur

Alors notre étude se focalise autour de : **« Sécurisation des données diffusées par émetteur SW (shortwave) »**

Pour mieux cerner notre analyse le premier chapitre va donner les notions sur la propagation d'onde, les bases et les techniques à connaitre sur la cryptographie pour avoir une sécurisation fiable.

Dans le second chapitre, parlons en premier lieu les méthodes d'acquisition et de traitement sonore, les techniques de chiffrement et déchiffrement. En second lieu, abordons les détails sur la propagation en onde courte SW. Et en dernier lieu, mettons en exergue la modulation d'amplitude.

Le dernier chapitre sera consacré pour la transmission en onde courte ainsi que la sécurisation de l'information et suivi par des illustrations de la technique et du modèle mathématique utilisé.

CHAPITRE 1
GENERALITES SUR LA PROPAGATION D'ONDE ET SUR LA SECURISATION DE DONNEES

1.1 Introduction

Pour la radiodiffusion, les ondes électromagnétiques jouent un rôle très important sur la transmission de signal d'information qui devrait être sécurisé. Ce chapitre va traiter deux illustrations, premièrement, la généralité des propagations d'ondes et en donnant les différents caractéristiques de ces ondes pour une bonne transmission selon le besoin de l'utilisateur pour la transmission et deuxièmement, sur les généralités des cryptographies pour avoir une notion de sécurité pour une transmission fiable.

1.2 Propagation des ondes

1.2.1 Principes fondamentaux des ondes radio

La propagation des ondes radioélectriques est régie par la théorie de l'électromagnétisme établie par le gouvernement écossais. Le physicien et mathématicien James Clerk Maxwell qui a démontré que l'électricité, le magnétisme et la lumière sont tous des manifestations du même phénomène. La propagation des ondes électromagnétiques dépend des propriétés du support de transmission dans lequel elles voyagent. [1.01]

1.2.1.1 Equation de Maxwell

Originairement les équations de Maxwell ont fait référence à un ensemble de huit équations publié par Maxwell en 1865. Dans 1884 Oliver Heaviside, concurremment avec d'autres travaux par Willard Gibbs et Heinrich Hertz, modifient quatre de ces équations qui ont été groupées ensemble et sont connues sous le nom de nos jours " les équations de Maxwell ". Individuellement, ces quatre équations sont connues comme la loi de Gauss pour l'électrique, la loi de Gauss pour magnétisme, la loi de Faraday d'énumération et la loi d'Ampère avec la correction de Maxwell. [1.01]

L'opérateur du vecteur différentiel "Nabla" notée ∇ est l'un des opérateurs fondamental aux quatre équations de champ de Maxwell, tel que

$$\vec{\nabla} = \frac{\delta}{\delta x}\vec{\imath} + \frac{\delta}{\delta y}\vec{\jmath} + \frac{\delta}{\delta z}\vec{k} \qquad (1.01)$$

Si on considère un scalaire V et une fonction vectorielle $\vec{A}$ ayant comme composantes suivant l'axe (x,y,z).

$$\vec{A} = A_x\vec{\imath} + A_y\vec{\jmath} + A_z\vec{k} \qquad (1.02)$$

Il y a trois opérations possibles à l'opérateur ∇, qui est définit comme suit :

Le gradient d'un scalaire V est un vecteur donné par :

$$\overrightarrow{grad}\, V = \frac{\delta V}{\delta x}\vec{\imath} + \frac{\delta V}{\delta y}\vec{\jmath} + \frac{\delta V}{\delta z}\vec{k} \tag{1.03}$$

La divergence de $\vec{A}$ est un scalaire donné par :

$$\nabla . \vec{A} = div\, \vec{A} = \frac{\delta A_x}{\delta x} + \frac{\delta A_y}{\delta y} + \frac{\delta A_z}{\delta z} \tag{1.04}$$

Le rotationnel de $\vec{A}$ est un vecteur donné par :

$$\nabla \times \vec{A} = \left(\frac{\delta A_z}{\delta y} - \frac{\delta A_y}{\delta z}\right)\vec{\imath} + \left(\frac{\delta A_x}{\delta z} - \frac{\delta A_z}{\delta x}\right)\vec{\jmath} + (\frac{\delta A_y}{\delta x} - \frac{\delta A_x}{\delta y})\vec{k} \tag{1.05}$$

$$\nabla \times \vec{A} = \begin{vmatrix} \frac{\delta}{\delta x} & \frac{\delta}{\delta y} & \frac{\delta}{\delta z} \\ A_x & A_y & A_z \\ a_x & a_y & a_z \end{vmatrix} \tag{1.06}$$

Voici quelques opérateurs relatifs à ces identités : [1.01]

$$div\,(rot\,\vec{A}) = \nabla\left(\nabla \times \vec{A}\right) = 0 \tag{1.07}$$

$$rot\,(\overrightarrow{grad}\, V) = \nabla\left(\nabla\vec{A}\right) = 0 \tag{1.08}$$

$$div\,(\overrightarrow{grad}\, A) = \nabla\left(\nabla \times \vec{A}\right) = \nabla^2\vec{V} \tag{1.09}$$

Ou

$$\nabla^2 = \frac{\delta^2}{\delta x^2} + \frac{\delta^2}{\delta y^2} + \frac{\delta^2}{\delta z^2} \tag{1.10}$$

$$\nabla \times \nabla \times A = \nabla(\nabla . A) - \nabla^2 A \tag{1.11}$$

1.2.1.2 Diverses lois

En utilisant l'opérateur ∇; les 4 équations de Maxwell relient le champ électrique $\vec{E}$ (V/m) et le champ magnétique $\vec{H}$ (A/m) comme donné dans les Équations (1.11) à (1.14) :

- Loi électrique de Gauss:

$$\nabla . \vec{E} = \frac{\rho}{\varepsilon} \tag{1.12}$$

- Loi de Gauss pour magnétisme:

$$\nabla.\vec{H} = 0 \tag{1.13}$$

- Loi de l'énumération (Équation Maxwell-Faraday):

$$\nabla \times \vec{E} = -\mu \frac{\delta \vec{H}}{\delta t} \tag{1.14}$$

- Loi du circuit d'Ampère (avec la correction de Maxwell) :

$$\nabla \times \vec{H} = \sigma \vec{E} + \frac{\delta \vec{E}}{\delta t} \tag{1.15}$$

Avec : ρ : la densité de charge en coulombs par mètre cubique (C/m^3).

ϵ : la permittivité en farads par mètre (F/m).

μ : la perméabilité en Henry par mètre (H/m)

σ : la conductivité du milieu en mho par mètre ou siemens par mètre (S/m) qui est assumé pour être homogène.

La permittivité et perméabilité sont exprimées habituellement comme :

$$\varepsilon = \varepsilon_r \varepsilon_o, \qquad \varepsilon_o = 8.85 \times 10^{-12}\ F/m \tag{1.16}$$

$$\mu = \mu_r \mu_o, \qquad \mu_o = 4\pi \times 10^{-7}\ H/m \tag{1.17}$$

Les équations de Maxwell peuvent aussi être représentées quant au flux électrique $\vec{D}$ en c/m^2, flux magnétique $\vec{B}$ en Tesla et une densité courante $\vec{J}$ en ampère par mètre carré (A/m^2), donné par :

$$\vec{B} = \mu \vec{H} \tag{1.18}$$

$$\vec{D} = \varepsilon \vec{E} \tag{1.19}$$

$$\vec{J} = \sigma \vec{E} \tag{1.20}$$

Avec $\vec{H}$: Intensité du champ magnétique

$\vec{E}$: Intensité du champ électrique

1.2.2 Evolution de la radio

Un signal radio est une onde électromagnétique qui se déplace à la vitesse de la lumière. Correctement codé, ce signal peut transporter de l'information.

James Clerk Maxwell a découvert en premier que la variation d'un champ magnétique induit un champ électrique qui induit à son tour un changement de champ magnétique et que la transition produit une onde électromagnétique. Cette découverte fut mise en pratique par Heinrich Hertz et surtout par Edouard Branly qui découvrit comment les détecter. Hertz avait fait l'émetteur, Branly, le récepteur. Il ne restait qu'à inventer l'antenne, ce dont se chargea un dénommé Popov. C'est l'Italien Guglielmo Marconi, âgé de vingt ans qui assembla les pièces pour réaliser la première communication radio en 1894 dans le grenier de ses parents après avoir entendu parler des ondes hertziennes. Il profite de plusieurs inventions et découvertes pour réaliser la première installation radio : il utilise l'éclateur d'Hertz comme émetteur, l'antenne de Popov, et le cohéreur de Branly comme récepteur. A force de la ténacité, il augmente progressivement la portée max des signaux qu'il émet jusqu'à atteindre une portée de plus de trois kilomètres en 1895. Parti en Angleterre pour concrétiser son invention, il la perfectionne en utilisant un émetteur et un récepteur accordés sur un longueur d'onde particulière en faisant varier les caractéristiques électriques des antennes et des circuits. En Décembre 1901 est reçu le premier signal radio transatlantique sur l'île de Terre-Neuve. S'engage alors une exploitation commerciale de l'invention : la radio devient un outil incontournable de l'armée et un instrument de loisirs dans les foyers. [1.02]

1.2.3 Transmission radio

1.2.3.1 Notion

Définition 1.01 : Transmission

La transmission est l'action de transmettre, de faire passer quelque chose à quelqu'un ou d'un émetteur à un récepteur.

La transmission des signaux s'effectue par émission d'onde électromagnétique.

Définition 1.02 : Onde électromagnétique

Une onde électromagnétique est une onde produite par un courant électrique variable dans le temps. Comme toutes les ondes, elle transporte de l'énergie sans transporter de matière.

Une transmission radio consiste alors à utiliser comme support de transmission une onde électromagnétique. L'émission s'effectue à l'aide d'une antenne et que la réception s'effectue sur un récepteur radio réglé sur la même fréquence.

En termes de radiodiffusion l'émetteur et la récepteur n'a qu'une seule fonction. L'émetteur rayonne des ondes électromagnétiques codé dans l'espace hertzien à l'aide de l'antenne. Et le récepteur capte le signal émis, sélectionne et décode l'information contenu dans le signal.

1.2.3.2 Types de propagation d'ondes électromagnétiques

Il existe 3 catégories d'ondes qui sont essentielles sur le domaine de transmission radio :

- Ondes de surface ou de sol.
- Ondes ionosphériques.
- Ondes d'espace

a. Propagation des ondes de surface

La propagation des ondes de surface ne concerne que les ondes ayant une fréquence inférieure 3Mhz, elles se propagent simultanément dans les bases couches atmosphériques et dans le sol comme illustré par la figure 1.01, la propagation de l'onde dépend donc des caractéristiques du sol : suivant leur fréquence, elles peuvent subir une absorption dans certains milieu ou ne pas pouvoir propager du tout. Une petite remarque, la fréquence inférieure à 10kHz permet des liaisons souterraines ou sous-marines.) (Figure 1.01)

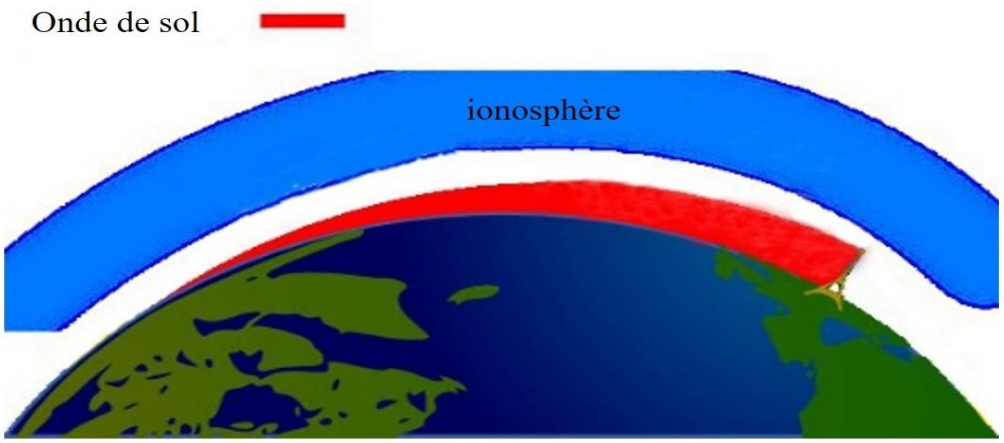

Figure 1.01 : *Onde de sol*

b. Propagation des ondes ionosphériques

Les ondes ayant une fréquence comprise entre 3MHz et 30MHz sont réfléchies par l'ionosphère. L'ionosphère, se situant entre 70km et 300km. Cette couche assure la propagation d'onde hertzienne. Cette couche est composée de 3 sous couches : D, E et F (figure 1.02). [1.02]

- La sous couche D : elle se situe à une altitude de 60 à 90 km, la pression régnant à cette altitude est de 2 Pa et la température -76°C. La densité électronique est de 10^4 électrons/cm3. C'est une zone présentant un faible degré d'ionisation car peu de rayon UV arrive, de plus la recombinaison est relativement rapide ce qui entraine la disparition de cette couche dès le coucher du soleil. Les électrons libérés sont surtout captés par les molécules de dioxygène

pour donner un ion négatif O_2^- qui est l'espèce majoritaire dans cette zone. Cette zone absorbe les ondes radio de fréquence inférieure à quelques MHz.

- La sous couche E : Elle est à l'altitude de 90 à 120 km, la pression régnante est de 0,01 Pa et la température de -50°C. La densité électronique 10^5 électrons/cm3 est plus élevé que dans la couche D. Les principaux composant sont leN_2, le O_2 ont les retrouvent sous forme de NO^+ et O_2^+ qui sont les espèces majoritaires de la couche E. Cette couche est diurne et présente tout au long du cycle solaire. Elle réfléchit les ondes de quelques MHz jusqu'à une fréquence limite qui dépend de l'angle d'incidence de l'onde sur la couche et de la densité de celle-ci. C'est une zone d'équilibre entre la production d'électrons par ionisation et leur disparition par recombinaison. Cette couche s'affaiblit beaucoup durant la nuit du fait des mécanismes de recombinaisons (radiative, dissociative, ion-ion).

- La sous couche F : Elle constitue la région la plus ionisée. Son altitude est de 120 à 800 km, la pression y régnant est de 1.10^{-4} Pa et la température de 1000°C. La densité électronique atteint 10^6 électrons/cm3 soit le maximum à l'altitude de 250 km. Dans cette région les ions et les électrons sont magnétisé, leurs mouvements sont contrôlé par le champ électrique issu du couplage vent solaire/magnétosphère qui se projettent le long de ligne de champ magnétique. Les espèces les plus représentées sont O_2^+, N_2^+ et O^+. Elle se décompose durant la journée en deux sous-couches F1 et F2, l'interface entre les deux se situant à environ 200 km d'altitude. Cette interface marque la transition entre l'ion atomique O^+ et l'ion moléculaireO_2^+. Elle s'atténue et disparaît la nuit plusieurs heures après le coucher du Soleil mais il arrive qu'elle persiste toute la nuit lors des maximums d'activité solaire. Comme pour la couche E, son rôle est essentiel pour la propagation des ondes courtes.

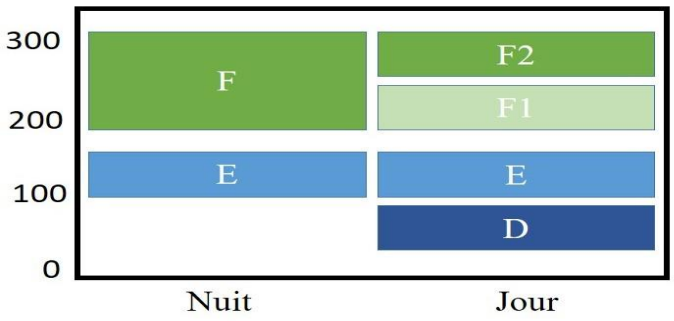

Figure 1.02 : *Couche ionosphérique*

c. Ondes d'espace

Les ondes d'espace se propage en ligne droite et nécessite une visibilité directe entre l'antenne d'émission et l'antenne de réception. Comme la surface de la terre n'est pas plane, la portée des telles ondes sont limitées.

Les ondes dont la fréquence est supérieure à 30MHz peuvent être transmises directement de l'émetteur au récepteur selon leurs situations géographique. La figure (1.03) nous montre cette propagation. [1.02]

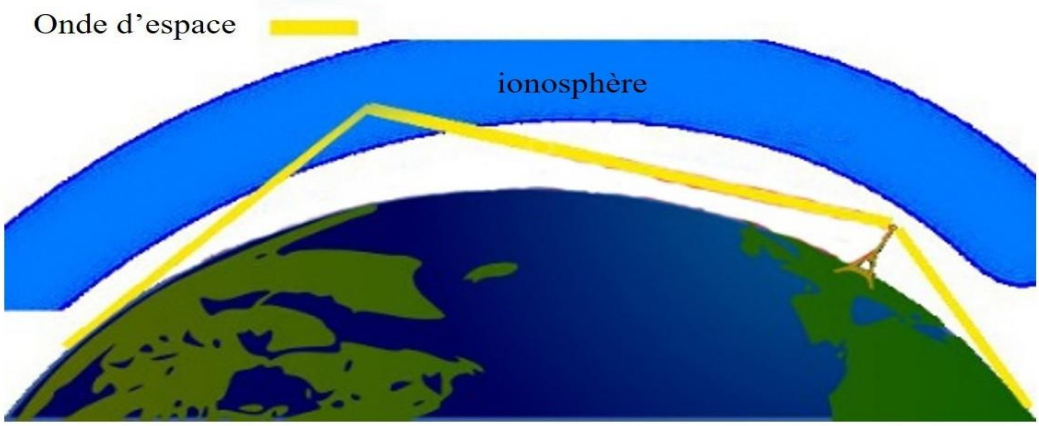

Figure 1.03 : *Propagation d'Onde d'espace*

1.2.3.3 Bandes de fréquences radio

La fréquence a un rôle très important dans les radiocommunications que ce soit sans fil ou réseaux radio. Voici un tableau donnant la gamme de fréquence utilisé : [1.03]

Tableau 1.01 : *Gamme de fréquence*

Longueur d'onde et son équivalent métrique	Gamme de la fréquence	Désignation	Numéro de la bande
Onde myriamétrique	3 - 30 kHz	VLF	4
Onde kilométrique	30 – 300 kHz	LF	5
Onde hectométrique	300 – 3000 kHz	MF	6
Onde décamétrique	3 – 30 MHz	HF	7
Onde métrique	30 – 300 Mhz	VHF	8
Onde décimétrique	300 – 3000 MHz	UHF	9
Onde centimétrique	3 – 30 GHz	SHF	10
Onde millimétrique	30 – 300 GHz	EHF	11
Onde décimillimétrique	300 – 3000GHz	-	-
Onde micrométrique	> 3 THz	-	-

1.2.4 Caractéristiques de ces fréquences selon la désignation

1.2.4.1 Very Low Frequency (VLF)

VLF est la désignation pour les fréquences radio comprises entre 3 à 30 kilohertz (kHz), correspondant à des longueurs d'onde comprises entre 100 m à 10 km. La bande est également appelée bande de myriamètre ou onde myriamètrique. En raison de sa largeur de bande limitée, la transmission audio est extrêmement peu pratique dans cette bande et par conséquent, seuls les signaux codés à faible débit de données sont utilisés. La bande VLF est utilisée pour quelques services de radionavigation, et pour les communications militaires sécurisées. Les ondes VLF peuvent pénétrer au moins de 40 mètres dans l'eau de mer. [1.04]

Les ondes radioélectriques VLF peuvent se diffracter autour de grands obstacles et peuvent se propager en tant qu'ondes de sol suivant la courbure de la Terre. La Terre est entourée d'une couche conductrice d'électrons et d'ions située dans la haute atmosphère au bas de l'ionosphère, appelée couche D, située à une altitude de 60 à 90 km, qui réfléchit les ondes radio VLF. L'ionosphère conductrice et la Terre conductrice forment un "conduit" horizontal de quelques longueurs d'onde VLF. Les ondes se déplacent suivant une trajectoire en zigzag autour de la Terre, réfléchies alternativement par la Terre et l'ionosphère, en mode TM (Transverse Magnétique). [1.04]

1.2.4.2 Low Frequency (LF)

LF ou Basse Fréquence (BF) est la désignation UIT (Union Internationales des Télécommunications) pour les fréquences radio comprises entre 30 kilohertz (kHz) et 300 kHz. Ses longueurs d'onde variant respectivement de dix kilomètres à un kilomètre, on l'appelle aussi bande de kilomètre ou onde kilométrique. Les ondes radioélectriques à basse fréquence présentent une faible atténuation du signal, ce qui les rend appropriées pour les communications à longue distance.

Les ondes radioélectriques à basse fréquence peuvent se diffracter en suivant le contour de la Terre. Ce mode de propagation, appelé onde de sol, est le mode principal de la bande BF. Les ondes de sol doivent être polarisées verticalement, de sorte que des antennes unipolaires verticales sont utilisées pour la transmission. L'atténuation de l'intensité du signal avec la distance par absorption dans le sol est inférieure à celle des fréquences plus élevées. Des ondes de sol à basse fréquence peuvent être reçues jusqu'à 2 000 kilomètres de l'antenne d'émission. Elles peuvent aussi occasionnellement parcourir de longues distances en se réfléchissant sur l'ionosphère. La réflexion se produit au niveau de la couche E ionosphérique ou des couches F. [1.04]

1.2.4.3 Medium Frequency (MF)

MF est la désignation pour les fréquences radio comprises entre 300 kilohertz (kHz) et 3 mégahertz (MHz). Une partie de cette bande est la bande de diffusion AM (Amplitude Modulation) à ondes

moyennes. La bande en ondes hectométriques est également appelée bande hectomètre, car les longueurs d'onde varient de 10 à 1 hectomètre (100 m à 1000 m). MF est principalement utilisée pour la radiodiffusion AM, les radiobalises de navigation, les communications maritimes.

Les ondes radioélectriques aux longueurs d'onde MF se propagent via les ondes de sol et les réflexions de l'ionosphère. À ces longueurs d'onde, ils peuvent se plier au-dessus des collines, bien qu'ils puissent être bloqués par des chaînes de montagnes. Les stations de radio MF peuvent couvrir un rayon de plusieurs centaines de kilomètres de l'émetteur. Ces stations de radiodiffusion MF utilisent des ondes de sol pour couvrir leurs zones d'écoute. Les ondes radioélectriques émises sous un angle perpendiculaire au ciel sont renvoyées vers la Terre par des couches de particules chargées (ions) dans l'ionosphère, les couches E et F. Cependant, à certains moments, la couche D (à une altitude inférieure à celle des couches réfractives E et F) peut être électroniquement bruyante et absorber les ondes radioélectriques MF, interférant avec la propagation des ondes célestes. Cela se produit lorsque l'ionosphère est fortement ionisée, par exemple en journée, en été et surtout en période de forte activité solaire, La nuit, en particulier en hiver et en période de faible activité solaire, la couche D ionosphérique peut pratiquement disparaître. Lorsque cela se produit, les ondes radio MF peuvent être facilement reçues à des centaines, voire des milliers de kilomètres, car le signal sera réfracté par la couche F restante. Les nuits où la propagation des ondes sont bonnes, les signaux des stations distantes peuvent être réfléchis par l'ionosphère et interférer avec les signaux des stations locales sur la même fréquence.[1.04]

1.2.4.4 High Frequency (HF)

HF est la désignation pour la gamme d'ondes électromagnétiques de radiofréquence comprises entre 3 et 30 mégahertz (MHz). Il est également connu sous le nom de bande décamètre ou onde décamétrique car ses longueurs d'onde vont de un à dix décamètres. La bande HF étant une partie importante de la bande de fréquences à ondes courtes, la communication à ces fréquences est souvent appelée radio à ondes courtes. Comme les ondes radioélectriques de cette bande peuvent être renvoyées vers la Terre par la couche d'ionosphère dans l'atmosphère une méthode connue sous le nom de propagation "sautée" ou "onde céleste", ces fréquences sont adaptées à la communication à longue distance sur des distances intercontinentales et aux terrains montagneux empêcher les communications en visibilité directe. La bande est utilisée, entre autres, par les stations de radiodiffusion internationales à ondes courtes (2,31-25,02 MHz), les communications aéronautiques, les stations du gouvernement, les stations météorologiques, la radio amateur et les services de bande destinés aux citoyens.[1.04]

Le moyen dominant de communication à longue distance dans cette bande est la propagation d'ondes indélébiles, dans laquelle les ondes radioélectriques dirigées à un angle du ciel se réfractent

à la Terre à partir de couches d'atomes ionisés de l'ionosphère. Cependant, l'adéquation de cette partie du spectre à une telle communication varie considérablement en fonction d'une combinaison complexe de facteurs: lumière du soleil / obscurité sur le site de transmission et de réception ; Emetteur / récepteur à proximité du terminateur solaire ; saison ; cycle de taches solaires ; activité solaire ; aurore polaire.

À tout moment, pour un chemin de communication "ignorer" donné entre deux points, les fréquences auxquelles une communication est possible sont spécifiées par ces paramètres : fréquence maximale d'utilisation ; haute fréquence utilisable la plus basse ; fréquence de transmission optimale.

La fréquence maximale utilisable passe régulièrement au-dessous de 10 MHz dans l'obscurité pendant les mois d'hiver, tandis qu'en été, elle peut facilement dépasser 30 MHz. Cela dépend de l'angle d'incidence des ondes; il est le plus bas lorsque les ondes sont dirigées vers le haut et il est plus élevé avec des angles moins aigus. Cela signifie qu'à des distances plus longues, où les ondes balayent l'ionosphère selon un angle très aigu, la MUF (Maximum Usable Frequency) peut être beaucoup plus élevée. La fréquence utilisable la plus basse dépend de l'absorption dans la couche inférieure de l'ionosphère (la couche D). Cette absorption est plus forte aux basses fréquences et plus forte avec l'activité solaire accrue (par exemple à la lumière du jour); l'absorption totale se produit souvent à des fréquences inférieures à 5 MHz pendant la journée. Le résultat de ces deux facteurs est que le spectre utilisable se décale vers les basses fréquences et passe dans la gamme des moyennes fréquences (MF) pendant les nuits d'hiver, tandis qu'un jour de plein été, les fréquences les plus hautes ont tendance à être plus utilisables, souvent dans les basses fréquences VHF. Lorsque tous les facteurs sont optimaux, la communication mondiale en HF est possible. À de nombreux autres moments, il est possible d'établir un contact à travers et entre les continents ou les océans. Au pire, lorsqu'une bande est "morte", aucune communication au-delà des trajets d'onde de sol limités n'est possible, quels que soient les pouvoirs, les antennes ou les autres technologies utilisées. Lorsqu'un chemin transcontinental ou mondial est ouvert sur une fréquence donnée, la communication numérique , SSB (Single Side Band) et en code Morse est possible en utilisant des puissances d'émission étonnamment basses, souvent de l'ordre du milliwatt, à condition que des antennes appropriées soient utilisées aux deux extrémités et qu'il existe peu ou pas aucune interférence naturelle ou causée par l'homme . Sur une telle bande ouverte, les brouillages provenant d'une zone étendue affectent de nombreux utilisateurs potentiels. Ces questions sont importantes pour les utilisateurs de radio HF, militaires, de sécurité et amateurs [1.04]

1.2.4.5 Very High Frequency (VHF)

VHF est la désignation UIT pour la gamme d'ondes électromagnétiques de radiofréquence (ondes radio) de 30 à 300 mégahertz (MHz), avec des longueurs d'onde correspondantes de dix mètres à un mètre. Les utilisations courantes des ondes radio dans la bande VHF sont la radiodiffusion FM, la télédiffusion, les systèmes de radio mobile terrestre bidirectionnels (urgence, affaires, usage privé et militaire). Dans le cadre de la transition mondiale vers la télévision numérique, la plupart des pays exigent que les radiodiffuseurs transmettent la télévision dans la gamme VHF en utilisant le format numérique plutôt que le format analogique.

Les ondes radioélectriques dans la bande des ondes métriques se propagent principalement par des lignes en visibilité directe et des liaisons au sol; contrairement à la bande des ondes décamétriques, il n'y a que quelques réflexions aux basses fréquences de l'ionosphère (propagation des ondes célestes). Elles ne suivent pas le contour de la Terre. Bien qu'elles soient faiblement réfractées par l'atmosphère, elles peuvent voyager un peu au-delà de l'horizon visuel jusqu'à 160 km environ. Elles peuvent pénétrer dans les murs des bâtiments et être reçus à l'intérieur, bien que dans les zones urbaines, les réflexions des bâtiments provoquent une propagation par trajets multiples, ce qui peut gêner la réception de la télévision. Le bruit et les interférences radio atmosphériques provenant des équipements électriques posent moins de problèmes dans la bande qu'aux basses fréquences. La bande VHF est la première bande dans laquelle les antennes d'émission sont suffisamment petites pour pouvoir être montées sur des véhicules et des appareils portables. Elle est donc utilisée dans les systèmes de radiocommunications mobiles terrestres à deux voies, telles que les talkies walkies, et les radios à deux voies, communication avec les aéronefs (Airband) et les navires (radio maritime). Parfois, lorsque les conditions sont favorables, les ondes VHF peuvent parcourir de longues distances par des conduits troposphériques en raison de la réfraction des gradients de température dans l'atmosphère.[1.01]

1.2.4.6 Ultra High Frequency (UHF)

UHF est la désignation UIT pour les fréquences radioélectriques comprises entre 300 mégahertz (MHz) et 3 gigahertz (GHz), également appelée bande décimétrique, car les longueurs d'onde varient de un mètre à un dixième de mètre. Les ondes radio dont les fréquences sont supérieures à la bande UHF se situent dans la plage des hyperfréquences. Les ondes radio UHF se propagent principalement par la ligne droite. Elles sont bloquées par des collines et de grands bâtiments bien que la transmission à travers les murs du bâtiment soit suffisamment puissante pour une réception à l'intérieur. Ils sont utilisés pour la télédiffusion, la téléphonie mobile, la communication par satellite, y compris le GPS, les services de radiocommunication personnels, notamment Wi-Fi et Bluetooth, les talkies walkies, les téléphones sans fil et de nombreuses autres applications.

L’IEEE (Institute of Electrical and Electronics Engineers) définit la bande radar UHF comme des fréquences comprises entre 300 MHz et 1 GHz. [1.01]

Les ondes radioélectriques dans la bande UHF se déplacent presque entièrement par propagation en visibilité directe et réflexion par le sol; contrairement à la bande HF, il n'y a que peu ou pas de réflexion de la part de l’ionosphère (propagation des ondes célestes) ou de l’onde de sol. Étant donné que les longueurs d’onde des ondes UHF sont comparables à la taille des bâtiments, arbres, véhicules et autres objets courants, la réflexion et la diffraction de ces objets peuvent provoquer un affaiblissement dû à la propagation par trajets multiples, en particulier dans les zones urbaines construites. L'humidité atmosphérique réduit ou atténue la force des signaux UHF sur de longues distances et l'atténuation augmente avec la fréquence. Les répéteurs radio sont utilisés pour retransmettre des signaux UHF lorsqu'une distance supérieure à la ligne de mire est requise. Parfois, lorsque les conditions sont favorables, les ondes radio UHF peuvent parcourir de longues distances par des conduits troposphériques lorsque l’atmosphère se réchauffe et se refroidit au cours de la journée. [1.01]

1.2.4.7 Super High Frequency (SHF)

SHF est la bande de radiofréquences qui s'étend de 3 GHz à 30 GHz (longueur d'onde de 10 cm à 1 cm). Les SHF font partie des micro-ondes. Ces ondes électromagnétiques sont très facilement absorbées par tout matériau plein d'une certaine épaisseur. Par contre, elles passent un peu entre les mailles d'un grillage métallique qui arrête les ondes plus longues. [1.02]

1.2.4.8 Extremely High Frequency (EHF)

EHF est la désignation pour la bande de fréquences de la radio dans le spectre électromagnétique de 30 à 300 gigahertz. Les ondes radio dans cette bande ont des longueurs d'onde de dix à un millimètre, donc elle est aussi appelée le millimètre bande et la radiation dans cette bande est appelée vague du millimètre. [1.02]

1.3 Cryptographie

La cryptographie utilise des concepts issus de nombreux domaines (Informatique, Mathématiques, Electronique). Toutefois, les techniques évoluent et trouvent aujourd’hui régulièrement racine dans d’autres branches (Biologie, Physique, etc.). [1.05]

1.3.1 Vocabulaire de base

Définition 1.03 : Cryptologie

Il s’agit d’une science mathématique comportant deux branches : la cryptographie et la cryptanalyse

Définition 1.04 : Cryptographie

La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

Définition 1.05 : Chiffrement

Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.

La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de déchiffrement.

Définition 1.06 : Texte chiffré

Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

Définition 1.07 : Clé

Il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et/ou déchiffrement. Dans le cas d'un algorithme symétrique, la clé est identique lors des deux opérations. Dans le cas d'algorithmes asymétriques, elle diffère pour les deux opérations.

Définition 1.08 : Cryptanalyse

Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés (comme illustré sur la figure 1.04).

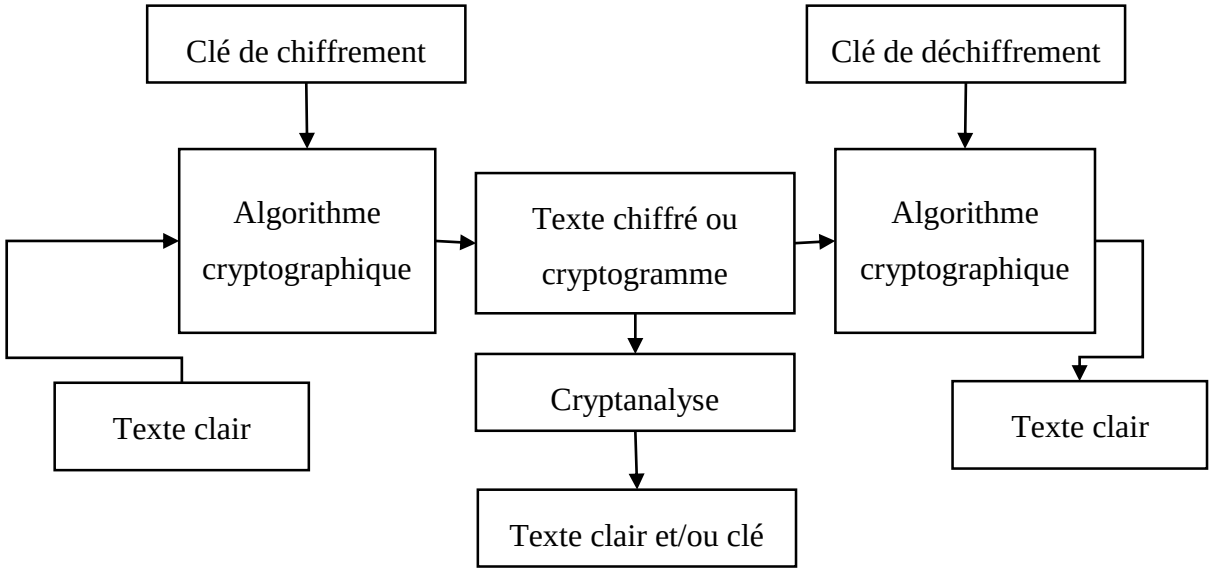

Figure 1.04 : *Protocole de chiffrement*

Définition 1.09 : Cryptosystème

Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

L'algorithme est en réalité un triplé d'algorithmes :

- l'un générant les clés K,
- un autre pour chiffrer Q,
- un troisième pour déchiffrer C.

On parle de "décryptage" pour désigner l'action permettant de retrouver le texte clair sans connaître la clef de déchiffrement.

1.3.2 Protocoles cryptographiques

Dès que plusieurs entités sont impliquées dans un échange de messages sécurisés, des règles doivent déterminer l'ensemble des opérations cryptographiques à réaliser, leur séquence, afin de sécuriser la communication ; C'est ce que l'on appelle les protocoles cryptographiques.

Lorsque l'on parle de "sécuriser un échange", on souhaite prêter attention aux 3 services suivants :

- la confidentialité,
- l'intégrité
- l'authentification.

1.3.2.1 Confidentialité

La confidentialité consiste à garder les informations secrètes de tous sauf les personnes autorisées à les voir.

1.3.2.2 Intégrité

L'intégrité consiste à s'assurer que les informations n'ont pas été altérées par des personnes pas autorisées ou inconnues.

1.3.2.3 Authentification

L'authentification consiste à garantir l'identité d'une entité donné ou origine d'une communication ou d'un fichier.

1.3.3 Différentes types de chiffrement

1.3.3.1 Chiffrement par substitution

Définition 1.10 : Un chiffrement par substitution est un algorithme par lequel chaque caractère du message clair est substitué par un autre caractère dans le message chiffré.

En cryptographie classique, il y a quatre types de chiffrement par substitution :

- Substitution simple
- Substitution homophonique
- Substitution polygamique
- Substitution poly alphabétique

a. Chiffrement par substitution simple

Un caractère du message clair est substitué par un caractère unique de message chiffré. Cela correspond le plus souvent à une permutation des caractères de l'alphabet des messages clairs.

b. Chiffrement par substitution homophonique

Un caractère du message clair correspond à plusieurs caractères du message chiffré.

Le principe est qu'à chaque caractère de l'alphabet des messages clairs est associé une liste de lettre dans l'alphabet des messages chiffrés, l'ensemble de ces listes formant une partition de l'alphabet des messages chiffrés.

c. Chiffrement par substitution polygamique

Le principe est de substituer des blocs de caractères, au lieu d'un seul caractère.

d. Chiffrement par substitution poly alphabétique

Il s'agit d'un ensemble de substitutions simples. Suivant la position du caractère dans le message clair, on applique une des substitutions simples. Ce sont des sortes de permutations à paramètres.

1.3.3.2 Chiffrement de César

Il s'agit d'un des plus simples et des chiffres classiques les plus populaires. Son principe est un décalage des lettres de l'alphabet.

Dans les formules ci-dessous, " l " est l'indice de la lettre de l'alphabet, k est le décalage.

Pour le chiffrement, on aura la formule

$$C = E(l) = (l + k)\ mod\ 26 \qquad (1.21)$$

Pour le déchiffrement, il viendra

$$l = D(C) = (C - k)\ mod\ 26 \tag{1.22}$$

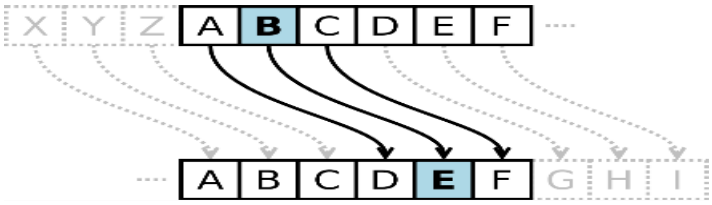

Figure 1.05 : *Décalage de chiffrement de César*

1.3.3.3 Chiffrement par transposition

Le chiffrement par transposition consiste à appliquer une permutation des caractères sur le message clair en entier. De ce fait, le message chiffré est fait du même matériel que le message clair.

1.4 Conclusion

Dans ce chapitre, les différentes fonctions des ondes électromagnétiques ont été vues pour introduire la notion pour les propagations d'ondes accompagnés de différentes caractéristiques de ces ondes pour avoir la gamme de fréquence pour nos radiodiffusions. Nous avons introduit aussi, la notion de base pour la cryptographie afin de connaitre déjà les différents types pour la sécurisation d'une information.

CHAPITRE 2
TECHNIQUE DE TRAITEMENT ET DE SECURISATION DES DONNEES

2.1 Introduction

Ce chapitre est consacré sur la théorie de l'acquisition et traitement sonore basé sur les différents techniques de traitement de signal de l'analogique vers la numérique et inversement et ainsi la technique de chiffrement que soit symétrique ou asymétrique et enfin, procédons à l'étude de la technique de modulation utilisée pour la propagation onde courte.

2.2 Acquisition et traitement sonore

2.2.1 Introduction

D'un point de vue physique, un son est une énergie qui se propage sous formes de vibrations dans un milieu compressible (dans l'eau, dans l'air, dans les matériaux solides, mais pas dans le vide). On peut observer ce phénomène de propagation des ondes à la surface en lançant une pierre dans l'eau comme illustré dans la figure 2.01. [2.01]

Figure 2.01 : *Propagation d'onde*

2.2.2 Propagation de son dans l'air

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 (figure 2.02).

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 le déplacement de l'air en signaux électriques. [2.01]

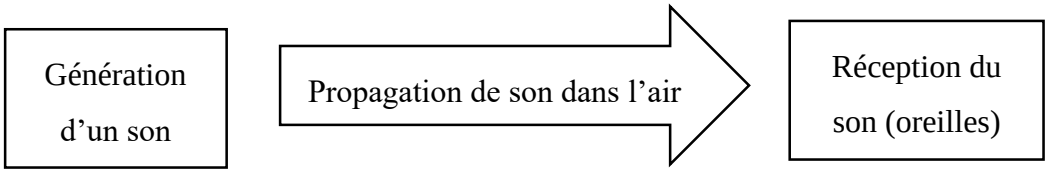

Figure 2.02 : *Emission, propagation et réception d'un son*

2.2.3 Caractéristique d'un son

Comme tout phénomène vibratoire, le son peut être analysé comme un signal qui varie dans le temps. Deux caractéristiques essentielles sont l'amplitude et la fréquence. [2.01]

2.2.3.1 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).

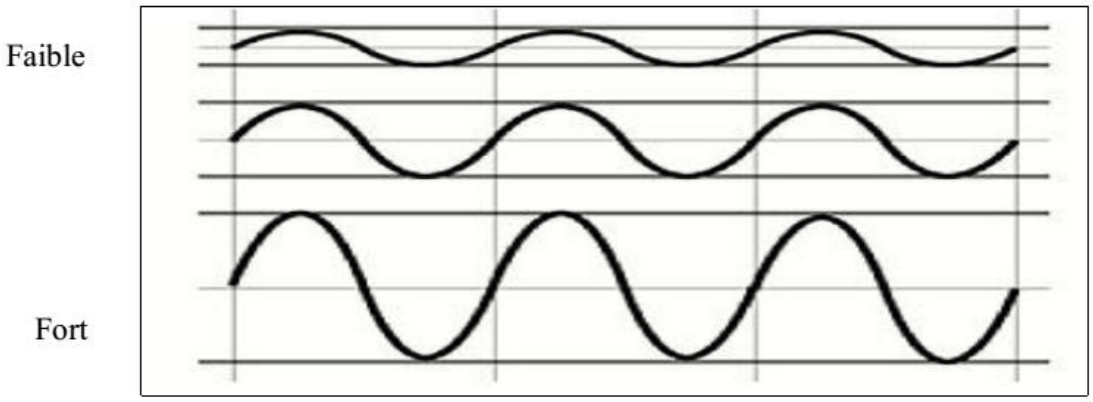

Figure 2.03 : *Types d'amplitude sonore*

- L'évolution de l'amplitude sonore dans le temps s'appelle l'enveloppe.

2.2.3.2 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 paraitra "aigue", à l'inverse, elle paraitra "grave". (Figure 2.04)

Le spectre de fréquence entendu par l'oreille humaine n'est pas infini, il s'étend environ de 20 Hz à 20 000 Hz (20KHz). En dessous on parle d'infra-son et au-dessus on parle d'ultra-son.

- Infra son < 20Hz
- Basse 20Hz - 200Hz

- Bas-Médium 200Hz - 2000Hz
- Haut-Médium (ou aigus) 2000Hz - 12000Hz
- Aigu (ou sur-aigu) 12000Hz - 20000Hz
- Ultra son >20000Hz

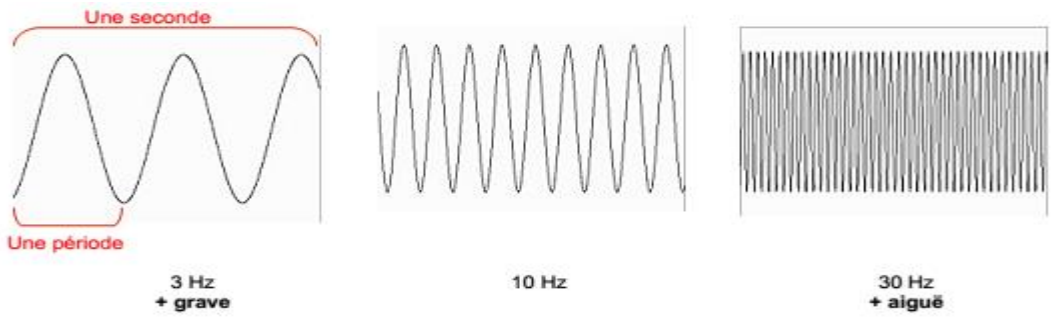

Figure 2.04 : *Types de fréquence*

2.2.4 De l'analogique au numérique

2.2.4.1 Son analogique : un signal continu

On capte le son à partir d'un microphone et le microphone transforme l'énergie mécanique qui est due par la vibration de la membrane exercée par la pression de l'air en une variation de tension électrique continue

Le signal analogique pourra ensuite amplifier et envoyer via le hautparleur dont la fonction est transformée à nouveau le signal électrique en une énergie mécanique

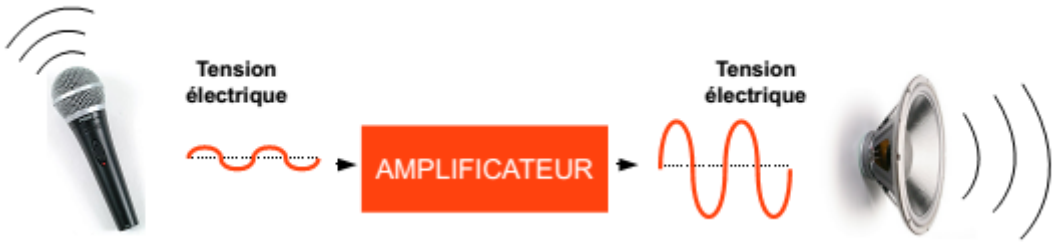

Figure 2.05 : *Exemple d'une chaine analogique.*

2.2.4.2 Son en numérique : un signal discontinu

A l'aide de l'informatique, ce même signal peut être capturé à l'aide d'un microphone et converti en une suite de nombre binaire et on parle de numérisation du signal. Et c'est un appareil électronique programmé qui charge la conversion de l'analogique vers le numérique puisqu'il contient une table en entrée de CAN (Convertisseur Analogique Numérique) et en sortie CNA (Convertisseur Numérique Analogique) (figure 2.06).

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 2.06 : *Exemple d'une chaine 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.

2.2.4.3 Caractéristiques du son numérique

- Fréquence d'échantillonnage en (Hz)

  Lorsqu'un son est numérisé, le signal analogique (continu) qui entre dans l'ordinateur est mesuré, un certain nombre de fois par seconde (d'où la discontinuité). Le son est donc découpé en "tranches", ou échantillons (en anglais "samples"). Le nombre d'échantillons disponibles dans une seconde d'audio s'appelle la fréquence d'échantillonnage exprimée en hertz.

  Pour traduire le plus fidèlement possible le signal analogique de notre micro, il faudra prendre le plus grand nombre de mesures possible par seconde. Autrement dit, plus la fréquence d'échantillonnage sera élevée, plus la traduction numérique du signal sera proche de l'original analogique.

- Résolution et quantification

  Un autre caractéristique importante est la résolution numérique du son, soit le nombre de "niveaux" ou de "paliers" qu'il est possible d'enregistrer pour produire l'amplitude du signal. Avec une résolution de 16 bit, on dispose de 2^{16}, soit 65535 valeurs possibles pour traduire l'amplitude du son.

  L'amplitude de chaque échantillon doit prendre l'une des valeurs définies par l'échelle de quantification. Si la valeur de l'amplitude de l'échantillon se situe entre deux paliers de l'échelle de quantification, elle est approximée au palier le plus proche.

Ainsi, plus la résolution est élevée, meilleure sera la dynamique (l'écart entre le son le plus faible et le plus fort qu'il est possible de reproduire).

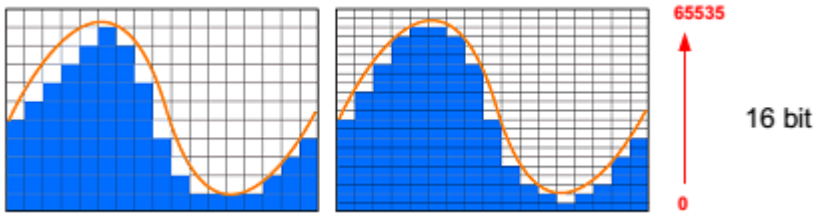

Figure 2.07 : *Quantification du son*

La zone bleue dans la figure 2.08 montre qu'en doublant la résolution, on est plus proche de la courbe analogique soit le signal parfait que l'on souhaite reproduire.

La quantification consiste en une deuxième phase où le chiffre de l'amplitude prélevé sera arrondi à l'entier le plus proche.

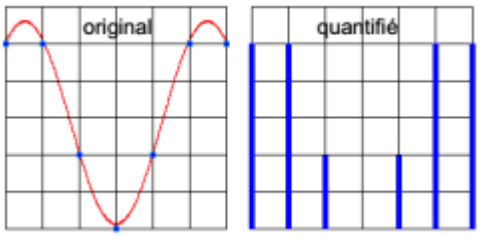

Figure 2.08 : *Signal quantifié*

- Mémoire requise pour stocker un son

  Il est simple de calculer la taille d'une séquence sonore non compressée en connaissant le nombre d'échantillons par second (fréquence d'échantillonnage), la résolution (nombre de bits sur lequel est codé un échantillon), le temps de la séquence (en seconde) et le nombre de voies utilisées :

$$P_{ds} = F_e \times R_s \times D_s \times N_s \qquad (2.01)$$

Avec P_{ds} : Capacité du son exprimé en octet

F_e : Fréquence d'échantillonnage en Hertz

D_s : Durée en séconde

R_s : Résolution du son

N_s : Nombres de voies

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.

a. Algorithme 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. [2.01]

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

b. Format de fichier audio

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.

Les formats audio varient selon : (figure 2.09)

- Le nombre de canaux sonores encodés.
- Le nombre d'échantillons par seconde avec lequel on découpera numériquement, pour chaque canal, une onde sonore ou un signal électrique.
- La résolution donnée à chaque échantillon et la grandeur physique qu'on lui donne. l'application d'une compression ou non.

En particulier, les codecs de MP3 ont réalisé des progrès très importants depuis le début de l'utilisation de ce format. 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. [2.01]

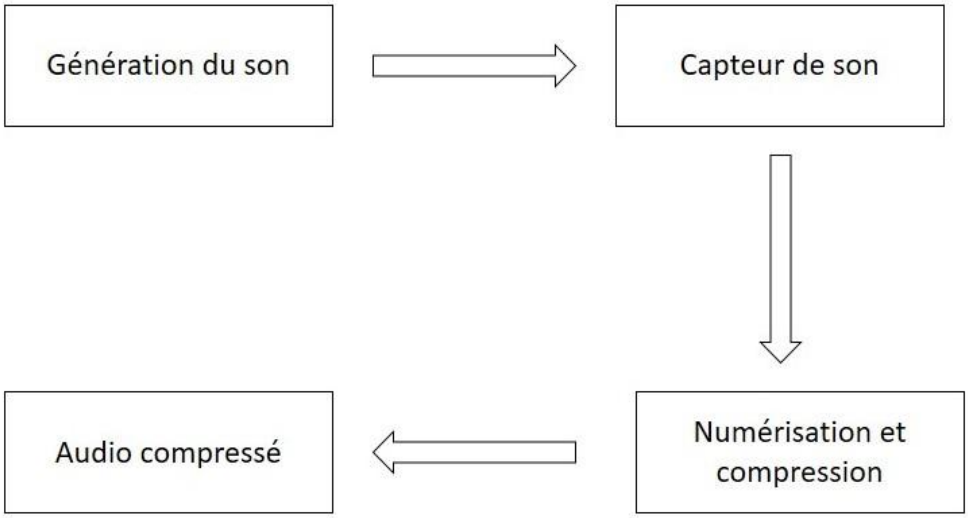

Figure 2.09 : *Compression du son*

2.3 Chiffrement et déchiffrement

2.3.1 Notation

- Q : ensemble des textes clairs possibles.
- C : ensemble des textes chiffrés possibles.
- K : ensemble des clés possibles
- E : ensemble des fonctions de chiffrement possible
- D : ensemble des fonctions de déchiffrement possible.

$$\forall\, m\ \in Q, \forall k\ \in K, \exists e_k \in E, \exists d_k \in D, d_k\big(e_k(m)\big) = m \qquad (2.02)$$

2.3.2 Chiffrement

On réalise sur les données *m* une transformation $c = E_k(m)$, par l'intermédiaire d'un algorithme de chiffrement E. Cet algorithme prend en entrée le message clair *m* et un paramètre secret *k*, qu'on appelle *la clé*. Le message m varie dans un ensemble Q et la clé k dans un ensemble K. [2.03]

2.3.3 Déchiffrement

La restauration du texte clair à partir du chiffré ou cryptogramme c se fait par un algorithme de déchiffrement D_k , prenant en entrée le chiffré et la même clé. On doit avoir $D_k(E_k(m) = m$.

En général, le chiffré prend sa valeur dans le même espace Q et l'on a aussi $E_k(D_k(c)) = c$, c'est-à-dire que l'algorithme E_k et D_k réalisent une permutation de Q.[2.03]

2.3.4 Différentes techniques de chiffrement

On distingue deux types de grandes catégories de chiffrement très reconnue en termes de sécurisation d'information : [2.03]

- Chiffrement à clé privée ou chiffrement symétrique
- Chiffrement à clé publique ou chiffrement asymétrique

2.3.4.1 Chiffrement à clé symétrique

Voici ces caractéristiques (figure 2.10) :

- Les clés sont identiques : $K_e = K_d = K$
- La clé doit rester secrète,
- Les algorithmes les plus répandus sont le DES, AES, 3DES, etc.
- Au niveau de la génération des clés, elle est choisie aléatoirement dans l'espace des clés,
- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé,
- La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256,
- L'avantage principal de ce mode de chiffrement est sa rapidité.

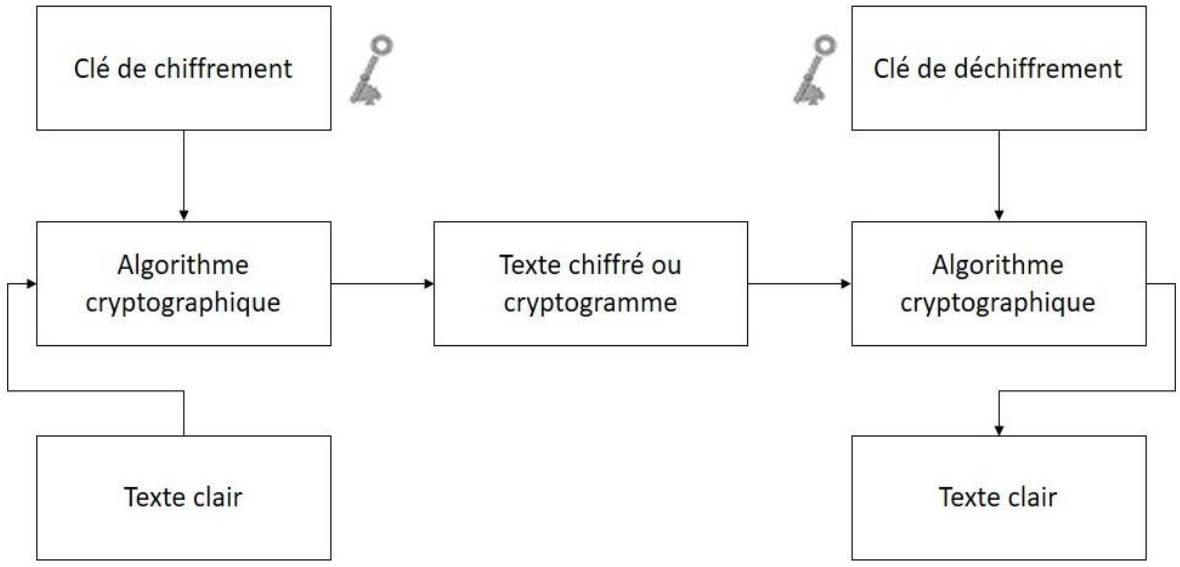

Figure 2.10 : *Chiffrement symétrique*

a. Confidentialité

Dans le cas de systèmes à clés symétriques, la même clé est utilisée pour $E_k(Q)$ et $D_k(C)$ .Ce type de chiffrement nécessite un échange sûr préalable de la clé Kentre les entités A et B comme dans la figure 2.11.

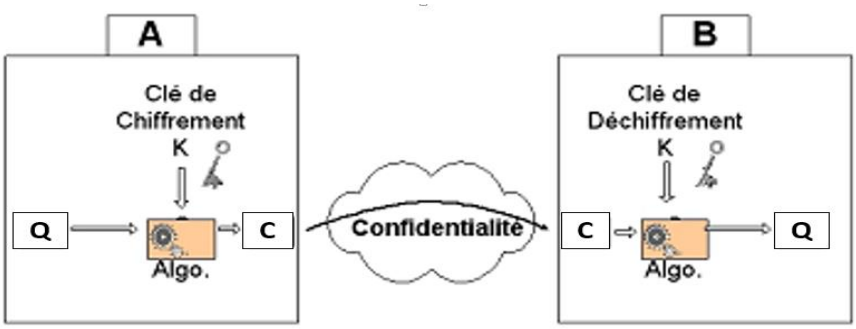

Figure 2.11 : *Confidentialité d'un système symétrique*

b. Intégrité

Un service d'intégrité garantit que le contenu d'une communication ou d'un fichier n'a pas été modifié.

c. Authentification

Au niveau des parties communicantes, dans le cas d'un système symétrique (figure 2.13). A la première figure, R_A est un nonce, propre à l'utilisateur A. Les lettres A et B représentent des identificateurs personnels.

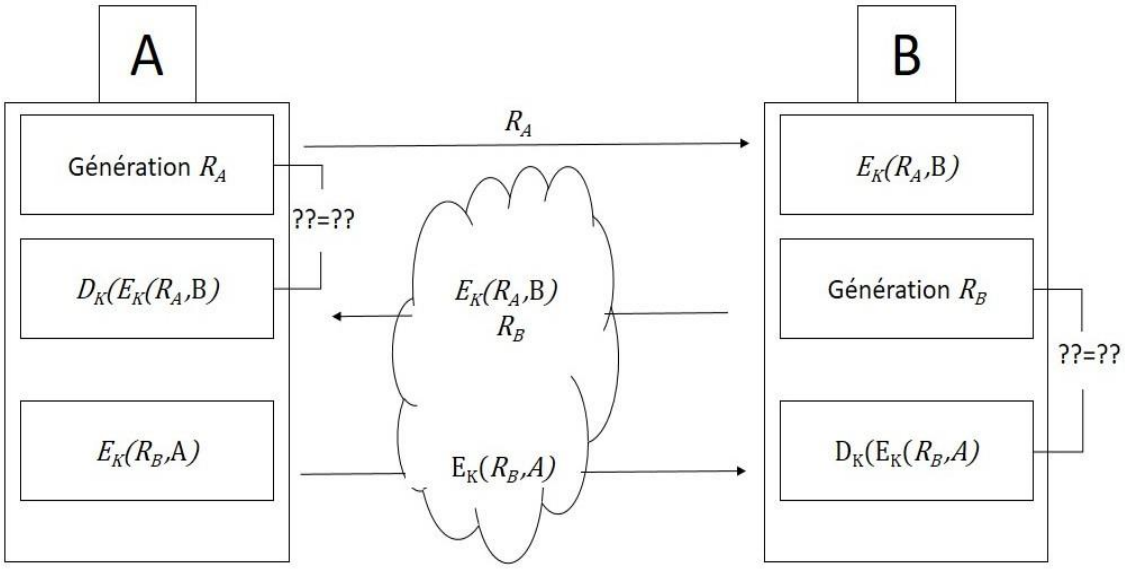

Figure 2.12 : *Authentification dans un système symétrique*

2.3.4.2 Chiffrement à clé asymétrique

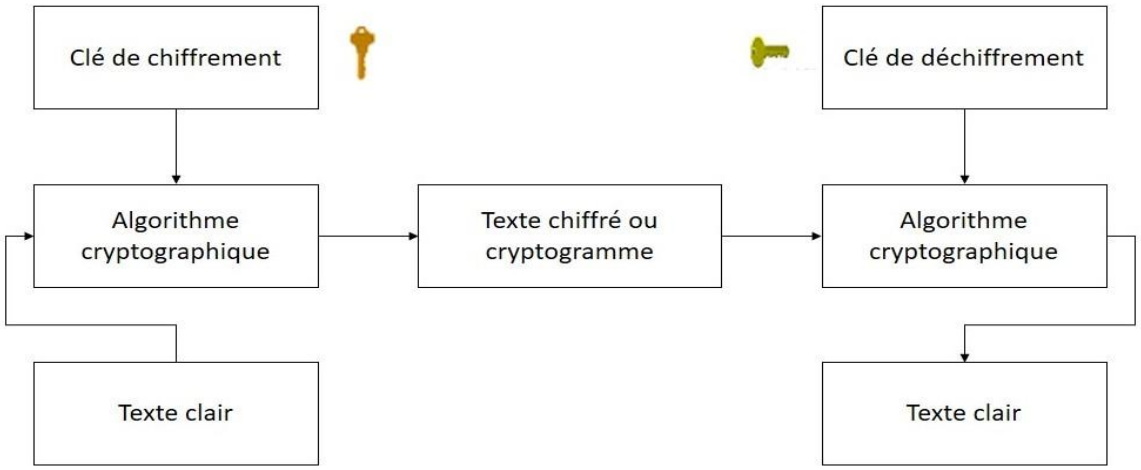

Figure 2.13 : *Chiffrement asymétrique*

Caractéristiques :

- Une clé publique P_k (symbolisée par la clé verticale)
- Une clé privée secrète S_k (symbolisée par la clé horizontale),
- Propriété : La connaissance de P_k ne permet pas de déduire S_k,
- $D_{S_k}(E_{P_k}(Q) = m$;
- L'algorithme de cryptographie asymétrique le plus connu est le RSA,
- La taille des clés s'étend de 512 bits à 2048 bits en standard.

a. Confidentialité

A l'aide d'un cryptosystème asymétrique, cet échange préalable n'est pas nécessaire. Chaque entité possède sa propre paire de clés. On aura donc la paire P_{K_A}, S_{K_A} pour l'entité A et la paire P_{K_B}, S_{K_B} pour l'entité B (figure 2.14).

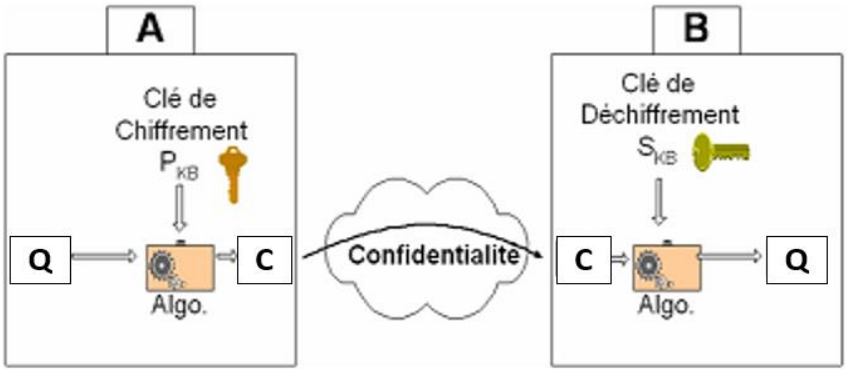

Figure 2.14 : *Confidentialité d'un système asymétrique*

b. Intégrité

Ce service est le même pour tout chiffrement. Son fonction est de garantir que le contenu d'un fichier n'a pas été édité.

c. Authentification

La clé de chiffrement utilisée est bien la clé privée. Comme le propriétaire de cette clé est le seul à la connaître, cela prouve qu'il est bien la personne ayant chiffré le message. Attention, dans cet exemple, seule l'authentification est souhaitée. Le message envoyé pourra être lu par toute personne possédant la clé publique, c'est-à-dire, n'importe qui. La confidentialité est ici nulle.

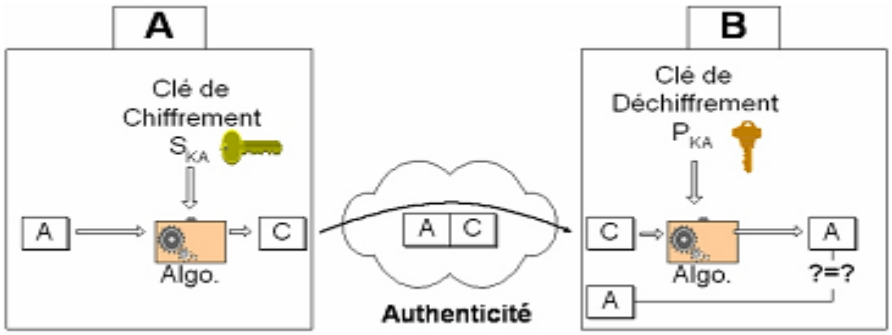

Figure 2.15 : *Authentification dans un système asymétrique*

2.4 Propagation en ondes courtes SW (ShortWave)

Contrairement à la radio locale sur les bandes VHF et à ondes moyennes, la réception des ondes courtes repose sur la réfraction des signaux provenant de couches situées à des centaines de kilomètres de la surface de la Terre (l'ionosphère). Ces couches sont "excitées" lorsque le soleil les éclaire, changeant leurs caractéristiques: certaines d'entre elles deviennent plus réfléchissantes aux signaux radio lorsqu'elles sont soumises au rayonnement solaire, tandis que d'autres commencent à absorber les signaux radio. C'est pourquoi certaines fréquences d'ondes courtes conviennent à la réception de nuit et d'autres au jour. Le coucher du soleil et le lever du soleil offrent d'autres possibilités intéressantes car les couches d'ionisation de nuit et de jour commencent à s'échanger. Cette interaction complexe de signaux radio et de couches de l'atmosphère terrestre est généralement appelée "propagation". [2.02]

En général, les couches qui apparaissent pendant la nuit réfractent les fréquences radio inférieures à environ 12 MHz (ou 12 000 kHz), tandis que les fréquences supérieures à environ 9 MHz (ou 9 000 kHz) sont réfractées par les couches qui apparaissent pendant le jour. Les fréquences inférieures à environ 5 MHz (ou 5 000 kHz) sont en grande partie absorbées par les couches diurnes. Le diagramme de droite montre quelles fréquences sont généralement les meilleures pour la réception

d’ondes courtes à différentes heures de la journée. Au-dessus de 12 MHz, les conditions de la journée sont généralement bonnes mais peuvent être très variables, surtout si vous montez en fréquence: les raisons en sont décrites ci-dessous. [2.02]

Bien qu'il soit possible de généraliser sur la manière dont la propagation radio affectera la réception d'ondes courtes, les conditions réelles varieront de jour en jour, de mois en mois et d'année en année. Les gaz de l'ionosphère sont affectés par les radiations du soleil et, comme la Terre, le soleil a des conditions météorologiques qui consistent en des orages ainsi qu'en des "saisons" d'hiver et d'été (connues sous le nom de cycle solaire). Alors que les tempêtes solaires sont en grande partie imprévisibles, le cycle solaire peut être suivi et il faut 11 ans pour passer de l'hiver à l'été. La météo sur le soleil (en ce qui concerne son effet sur la propagation radio) est mesurée en comptant les "taches solaires". Ce sont des zones d'activité solaire intense qui vont et viennent au cours du cycle solaire de 11 ans. Lorsque le nombre de taches solaires est élevé, les fréquences les plus élevées continuent de se propager dans les heures d'obscurité et même pendant la journée, des fréquences plus élevées que la normale fonctionnent. Lorsque le nombre de taches solaires est faible, la propagation est généralement moins bonne et se concentre davantage sur les basses fréquences, qui peuvent souvent devenir encombrées lorsque les radiodiffuseurs tentent de comprimer toutes leurs émissions dans les bandes de fréquences inférieures.

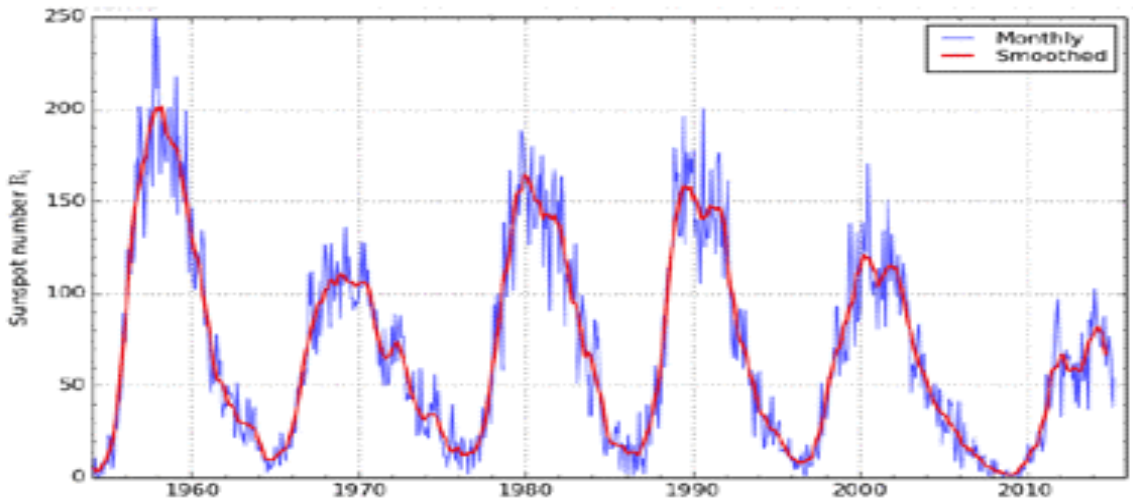

Figure 2.16 : *Signal avec la tache solaire*

2.5 Modulation

Lorsqu'un courant électrique parcourt un conducteur, il engendre, dans l'espace qui l'entoure, des modifications, on dit que le courant engendre un champ. Ce champ possède deux composantes, une composante électrique et une composante magnétique. Dès lors, on dit qu'il s'agit d'un champ électromagnétique. Ce champ électromagnétique peut se propager de proche en proche, et il est

capable de créer dans un conducteur, placé à une certaine distance, une force électromotrice de même fréquence et d'amplitude proportionnelle à celle du signal émis. Cette propriété est utilisée pour transmettre des informations entre deux points éloignés. [2.04]

La modulation consiste à transformer un signal $m(t)$ sous une forme qui lui permet d'être transmis dans un canal de transmission ; par exemple, aux canaux de communication radioélectriques, aux canaux à fibres optiques, aux câbles coaxiaux, aux liaisons radio mobiles, etc.

Les phénomènes de propagation ne sont pas abordés ici mais on voit quelque notion dans le chapitre 1, par contre nous allons étudier "comment faire passer le message", c'est à dire comment moduler une onde porteuse avec une information.

Le signal à haute fréquence peut s'écrire sous la forme :

$$s(t) = A\cos(wt + \rho) \qquad (2.03)$$

On va servir de "porteur" à un message et à cette fin il faut "imprimer" la forme de ce message sur l'onde porteuse, et on dit qu'il faut moduler un des paramètres de l'onde porteuse.

La modulation peut-être analogique ou numérique. On dit qu'une modulation est "analogique" lorsqu'un des paramètres de l'onde porteuse varie proportionnellement à l'onde modulante et on dit qu'elle est "continue" lorsque que l'onde modulée est émise sans aucune interruption. Parmi ces types de modulations on retrouve :

- la modulation en amplitude en agissant sur le paramètre A
- la modulation de fréquence en agissant sur le paramètre f avec $f = \frac{w}{2\pi}$
- la modulation de phase en agissant sur le paramètre ρ

On ne va pas aborder tous ces techniques de modulation mais on va se focaliser un peu sur l'analyse de la modulation d'amplitude que nous allons utiliser autant en terme de radiodiffusion en ondes courtes.

2.5.2 Modulation d'amplitude

2.5.2.1 Introduction

La modulation d'amplitude dit "Amplitude Modulation (AM)" en anglais est une technique de modulation utilisée dans les communications électroniques, le plus souvent pour transmettre des informations via une onde porteuse radio. En modulation d'amplitude, l'amplitude (force du signal) de l'onde porteuse varie proportionnellement à celle du signal de message transmis. Le signal du message est, par exemple, fonction du son à reproduire par un haut-parleur ou de l'intensité lumineuse des pixels d'un écran de télévision, etc.

La modulation d'amplitude était la méthode de modulation la plus ancienne utilisée pour transmettre la voix par radio mais il est encore utilisé de nos jours dans de nombreuses formes de communications, par exemple, elle est utilisée dans les radios portables bidirectionnelles, les radios VHF pour les avions. AM est souvent utiliser aussi pour la radiodiffusion à ondes courtes. [2.05]

On distingue 3 types de modulation d'amplitude

- AM-Double Bande Sans Porteuse (AM-DBSP) : utilisé pour le multiplexage fréquentiel et le cryptage analogique.
- AM-Double Bande Avec Porteuse (AM-DBAP) : utilisé en radio diffusion
- AM-ande latérale unique (BLU) : utilisé par le multiplexage fréquentiel, la téléphonie, la radiocommunication maritime et marine.

On va aborder le principe général de l'un de ces technique de modulation qu'on va utiliser dans cette recherche.

2.5.2.2 Principe général de l'AM-DBSP

Soit donc une information qu'on l'appelle "message" notée $s_0(t) = A\cos\Omega\, t$ de fréquence F à faire véhiculer par une porteuse $p(t) = B\cos w_0\, t$ de fréquence f et $s(t)$ le signal modulé. [2.05]

a. AM double bande sans porteuse (AM-DBSP)

Voici un schéma illustrant la fonctionnalité d'une AM-DBSP :

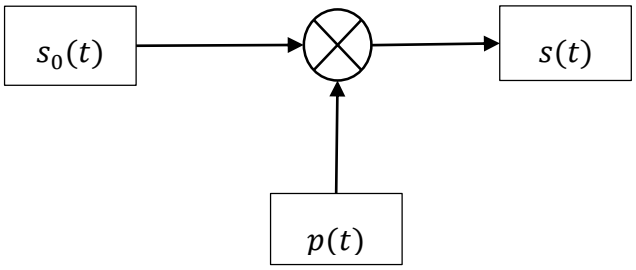

Figure 2.17 : *AM-DBSP*

Pour avoir le signal $s(t)$ en sortie, en pratiquant la méthode AM-DBSP, le signal d'information $m(t)$ doit se multiplier par la porteuse $p(t)$. Par exemple, prenant un signal modulant sinusoïdal.

- Cas d'un signal modulant sinusoïdal

Prenant l'expression du signal AM-DBSP est $s(t) = p(t).k\, s_0(t) = kAB[\cos w_0\, t.\cos\Omega t]$

Avec k = taux de modulation.

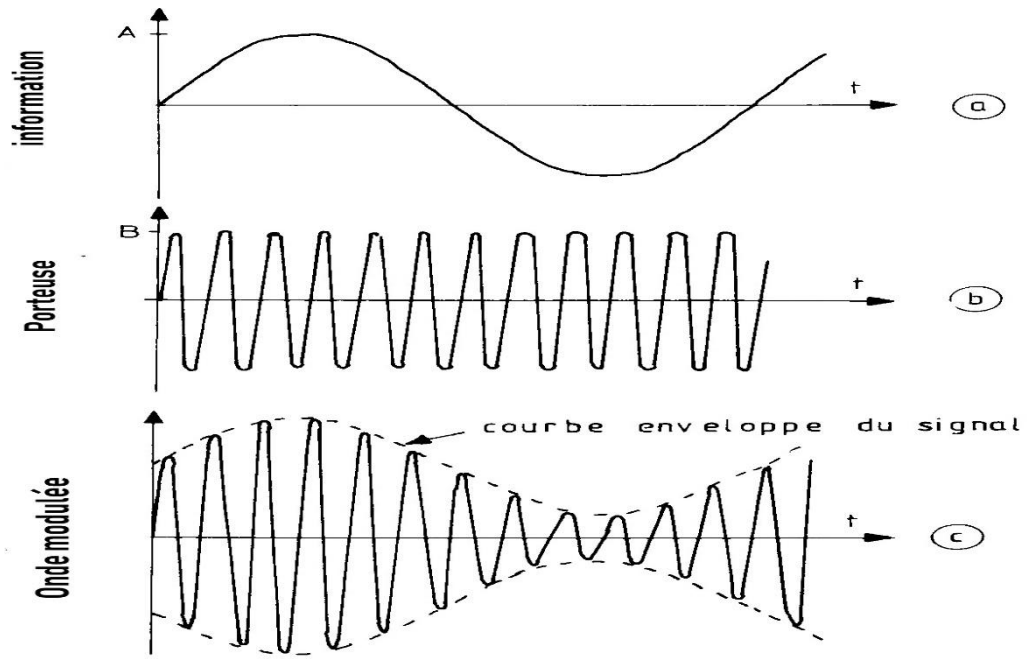

Figure 2.18 : *Représentation temporelle*

Pour déterminer le spectre du signal $s(t)$, il faut décomposer ce signal en une somme des signaux sinusoïdaux :

$$s(t) = kAB[\cos w_0\, t.\cos \Omega t]$$

$$= \frac{kAB}{2}\cos(w_0 - \Omega)t + \frac{kAB}{2}\cos(w_0 + \Omega)t$$

Rappel trigonométrique :

$\cos(a+b) = \cos a \cos b - \sin a \sin b$

$\cos(a-b) = \cos a \cos b + \sin a \sin b$ +

$\cos(a+b) + \cos(a-b) = 2\cos a \cos b$

Pour $a = w_0 t \; et \; b = \Omega t$

$\cos\big((w_0 + \Omega)t\big) + \cos\big((w_0 - \Omega)t\big) = 2\cos(w_0 t)\cos(\Omega t)$

$\cos(w_0 t)\cos(\Omega t) = \frac{1}{2}\cos\big((w_0 + \Omega)t\big) + \frac{1}{2}\cos\big((w_0 - \Omega)t\big)$

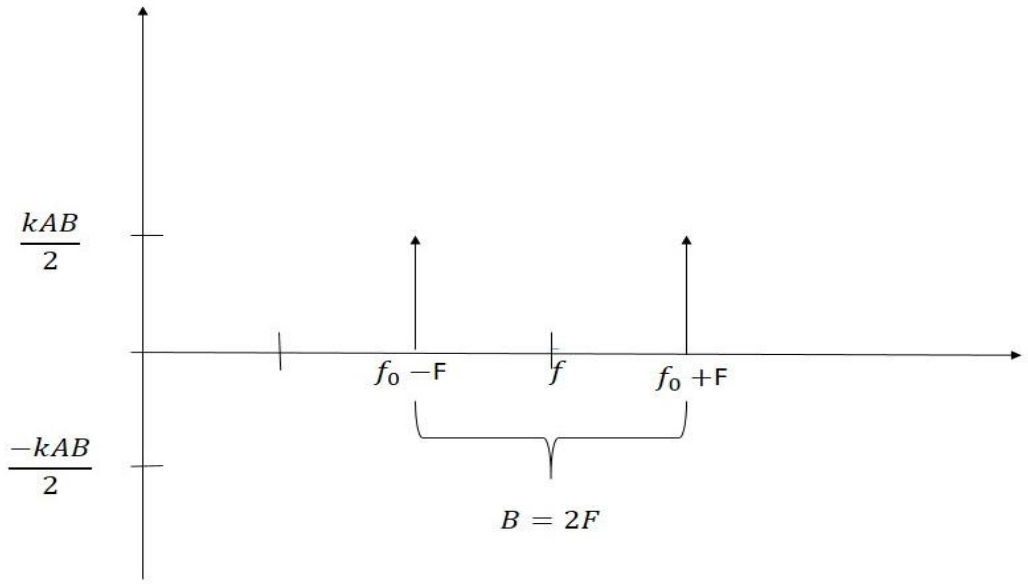

Figure 2.19 : *Représentation spectrale*

- Cas d'un signal modulant quelconque

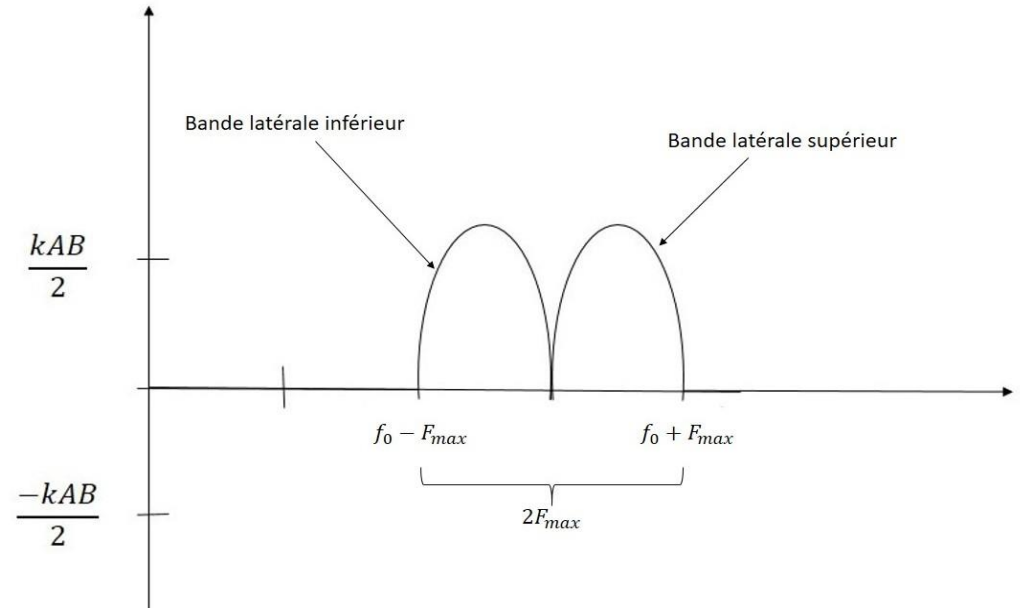

Figure 2.20 : *Représentation spectrale*

Le spectre d'amplitude du signal AM-DBSP avec un signal modulant quelconque est constitué de 2 bandes symétriques centrée autour de f_0 = BLi (Bande latérale inférieur) et BLs (Bande latérale supérieur.

L'occupation spectrale du signal AM-DBSP est $= 2F_{max}$.

La transmission d'un signal en modulation AM-DBSP nécessite donc une largeur de bande double de celle du signal modulant.

2.5.3 Démodulation d'amplitude

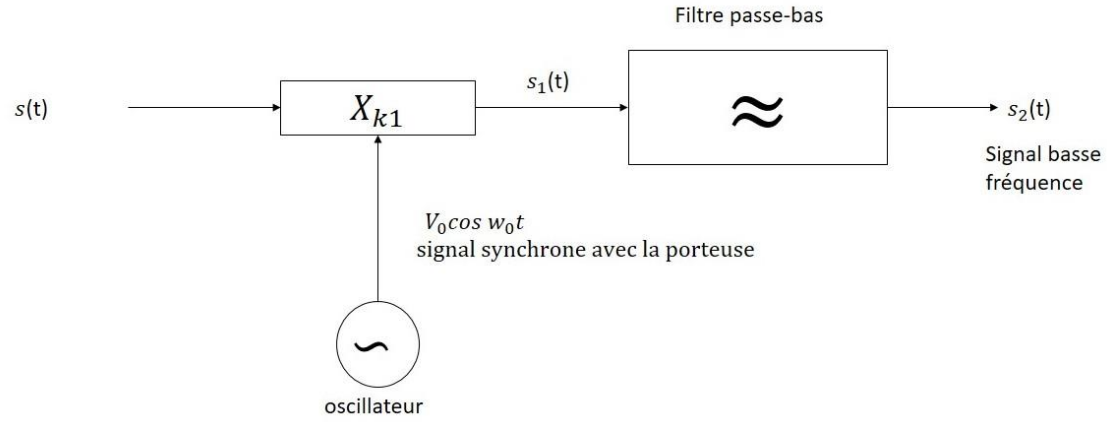

Figure 2.21 : *Démodulateur AM-DBSP*

Voici l'expression du signal $s_1(t)$

$$s_1(t) = V_0 \cos w_0 t . k_1 . s(t)$$

$$= k_1 V_0 \cos w_0 t . kAB[\cos w_0\, t . \cos \Omega t]$$

$$= kk_1 V_0 AB cos^2(w_0 t) \cos \Omega t$$

$$= kk_1 V_0 AB \left(\frac{1 + \cos(2w_0 t)}{2}\right) . \cos \Omega t$$

$$s_1(t) = kk_1 V_0 AB \frac{\cos \Omega t}{2} + \frac{kk_1 V_0 AB}{4} \cos(2w_0 - \Omega)\, t + \frac{kk_1 V_0 AB}{4} \cos(2w_0 + \Omega)\, t$$

$$s_2(t) = kk_1 V_0 AB \frac{\cos \Omega t}{2}$$

2.6 Conclusion

Dans ce chapitre, nous avons parlé les différentes caractéristiques sonores avec leurs traitements pour avoir son numérique afin de le transmettre sur l'onde courte en introduisant déjà les deux catégories de chiffrement et la technique de modulation d'amplitude sans porteuse comme notion de base à connaitre.

CHAPITRE 3

ETUDE ET SECURISATION DES DONNEES DANS UNE TRANSMISSION SW

3.1 Introduction

Le modèle de transmission radio peut se faire de différente manière selon la méthode utilisée par le concepteur (par exemple, le type de modulation qu'on utilise, le choix de fréquence pour émettre l'information, etc. En particulier, la technique de transmission par onde courte qui a été utilisée d'ailleurs est toujours mise à profit pour l'établissement de liaison à très longues distance sans nécessiter le recours à un satellite. Les communications sont bien adaptées aux besoins de la plupart des organisations. Ce chapitre traite la transmission par onde courte en utilisant la modulation d'amplitude et qui essaie aussi d'établir la sécurisation de l'information lors de la transmission.

3.2 Transmission par onde courte

3.2.1 Principe des ondes courtes

Les ondes courtes aussi appelées "ondes décamétrique" ou "haute fréquence" ont une très grande portée avec une puissance d'émission relativement réduite. [3.04]

Elles présentent en effet la particularité de se réfléchir sur la couche ionosphérique : elles se propagent par réflexions successives entre le sol (ou la mer) et certaines couches ionisées de la haute atmosphère.

Elles peuvent ainsi être reçues à une grande distance de l'émetteur d'un continent à l'autre, même en présence d'obstacles comme relief.

Un autre avantage réside dans la simplicité et le faible coût des récepteurs. La radio en onde courte constitue donc un média essentiel dans certains points du globe.

Les ondes courtes permettent une continuité du service là où le satellite, les ondes FM ou internet ne sont pas disponibles.

3.2.2 Applications des ondes courtes

La radiodiffusion en ondes courtes ne permet pas une communication de qualité : son application se limite à la transmission de la parole (et non de musique) et son signal peut être brouillé par les conditions atmosphériques.

Les ondes courtes hautes fréquences sont peu à peu abandonner par les services officiels. Pourtant, elles restent incontournables pour les services maritimes et aériens, pour garantir la sécurité des liaisons océaniques et les liaisons fixe ou mobile dans les zones sans infrastructure. Elles constituent aussi une technologie de secours, en cas de catastrophe naturelle.

3.2.3 Schéma synoptique général de cas existant de l'AWR

Voici un schéma illustrant toutes étapes dès les débuts jusqu'à la station cible lors d'une transmission par onde courte au sein de l'AWR (Adventist World Radio).

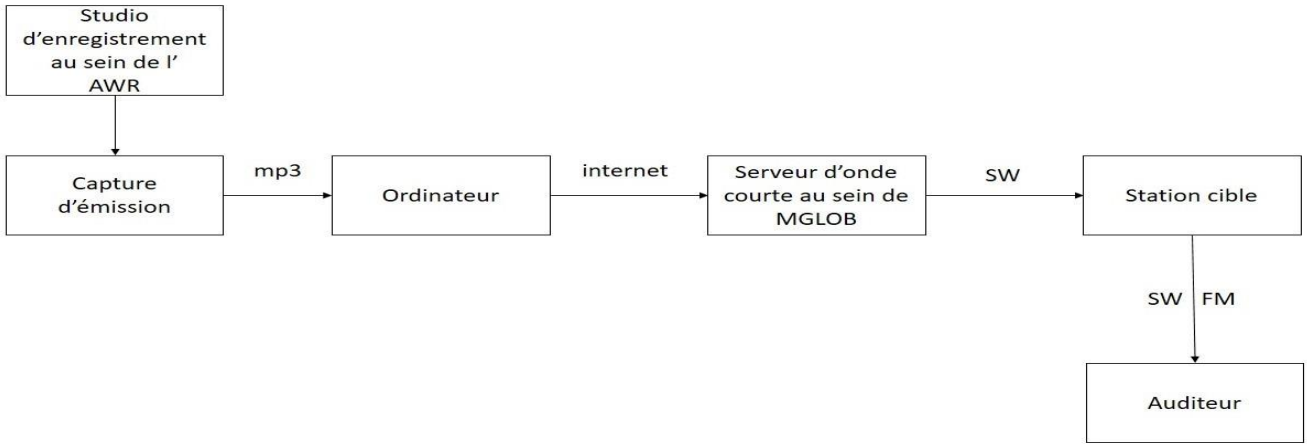

Figure 3.01 : *Transmission par onde courte*

La faiblesse de cette transmission dans la figure (3.01) c'est que : au niveau de MGLOB, il envoie tout simplement l'information qu'ils ont reçu pour être envoyé vers la station cible en utilisant l'onde courte ou SW. Or, lors du chemin de l'émission vers les stations cibles il y aurait des personnes de mauvaise foi qui veulent perturber la réception.

3.2.4 Solution pour la transmission en onde courte

En radiodiffusion, on sait que, la transmission par onde courte est un peu démodé par rapport au radio fréquence ou bien FM dans le terme de qualité de son à la réception ; or la transmission par onde courte peu atteint jusqu'à plusieurs milliers de kilomètres qui dépend de la puissance émise par l'émetteur.

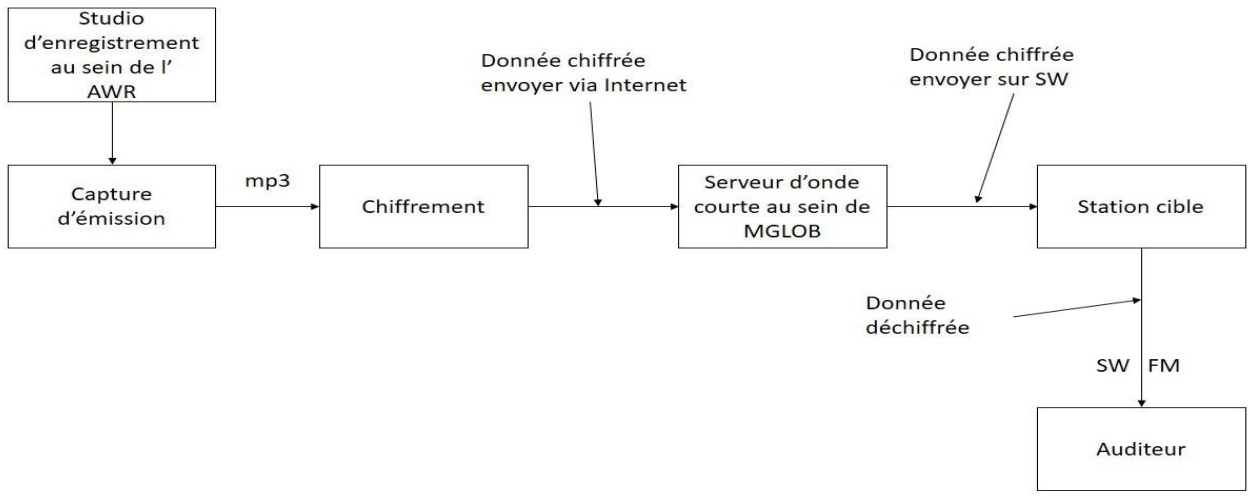

Figure 3.02 : *Transmission par onde courte avec sécurisation*

En termes de sécurisation nous proposons de faire recours au système de chiffrement.

Ce schéma bloc dans la figure 3.02 représente la de la transmission en général par onde courte.

3.2.5 Compression en MP3

L'algorithme de compression en MP3 est divisé en 5 étapes :

- Banque de filtres d'analyse de sous-bandes, pour diviser le signal en sous-bandes de fréquences.
- Application du modèle psycho acoustique, pour déterminer dans chaque sous-bande les fréquences qui peuvent être entendues et celles qui ne le peuvent pas.
- La transformation MDCT (Modified Discrete Cosine Transform)
- Quantification
- Formatage de bitstream

Voici le schéma synoptique illustrant ces étapes :

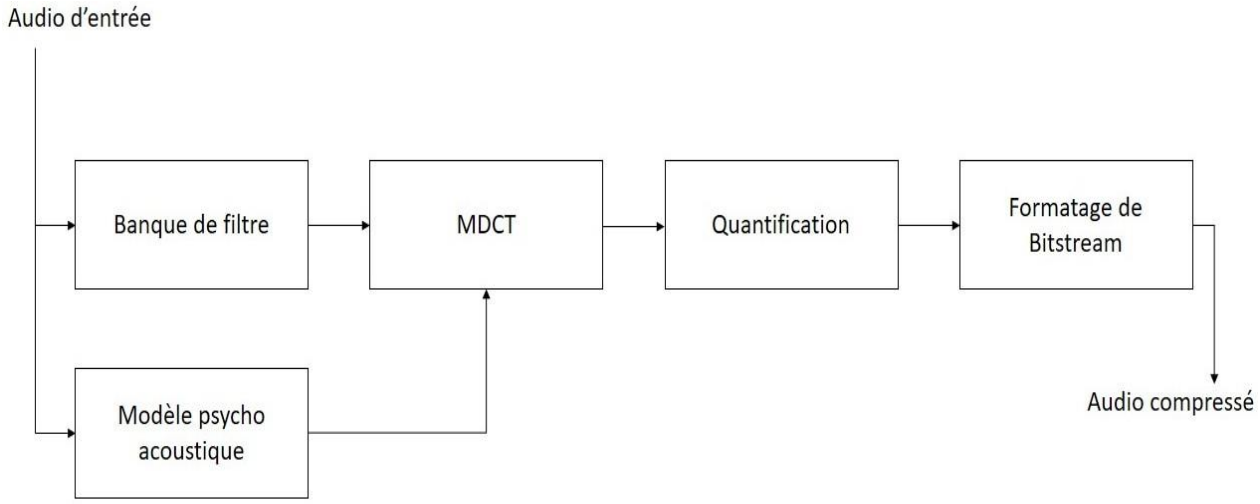

Figure 3.03 : *Compression en MP3*

On va voir un peu c'est que fait ces blocs :

a. Banque de filtre d'analyse de sous-bandes

Le standard MP3 recommande l'utilisation de filtre passe-haut. Ce filtre utilise un seuil (entre 2Hz et 10Hz) pour faire passer les fréquences supérieures à ce seuil. Une banque de filtres d'analyse de sous-bandes est un ensemble de filtres couvrant toute la gamme de fréquences audio. Cette banque de filtres est utilisée pour diviser le signal d'entrée avec une certaine fréquence d'échantillonnage (44.1kHz, …) en 32 sous-bandes

b. Modèle psycho acoustique

L'unité de calcul de la fréquence est l'hertz qui représente les cycles par seconde. Seulement un intervalle de fréquences est perceptible par l'humain. Le rang audible est entre 20 Hz et 20 kHz. La voix de l'être humain est limitée entre 80 Hz et 850 Hz. La parole normale entre 110 Hz et 300 Hz.

La psycho acoustique est la branche de la psychophysique qui fait appel à l'acoustique (qui étudie la nature et les propriétés des ondes sonores), à la physiologie de l'audition et à la psychologie pour régler quelques paramètres et seuils.

c. Transformation MDCT (Modified Discrete Cosine Transform)

La sortie de la banque de filtres ne permet pas une reconstruction parfaite. Pour cela, on utilise la transformée MDCT, et on appelle cette combinaison banque de filtres hybride.

d. Quantification

La quantification permet de supprimer des composantes situées en dessous du seuil minimal de masquage $T_{min.}$

e. Formatage de bitstream

Le bitstream (ou le flux) est organisé en trames de 1152 bits (soit 26ms environ à 44,1kHz).

Chaque trame contient toutes les informations nécessaires au décodage, comme :

- Entête de 32 bits;
- Les informations de protection sur 16 bits;
- Les coefficients d'amplification et les informations de quantification utilisées dans cette trame sur 136 à 256 bits;
- Les données audio compressées

Ces méthodes sont appliquées et utilisées par la plupart des logiciels de compression et de numérisation utilisé de nos jours. Et en terme de diffusion par onde courte qui fait de broadcast c'est cette audio compressé qu'il va émettre sur l'émetteur à onde courte.

3.2.6 Chiffrement

Les systèmes de cryptage à clé privée, appelés aussi systèmes de cryptage symétrique ou cryptage conventionnel, sont utilisés depuis plusieurs siècles déjà. C'est l'approche la plus authentique du chiffrement de données et mathématiquement la moins problématique. Dans ce chapitre nous présentons les différents algorithmes utilisés dans le chiffrement des fichiers audio (fichier son). Un expéditeur et un destinataire souhaitant communiquer de manière sécurisée à l'aide du cryptage

conventionnel doivent convenir d'une clé et ne pas la divulguer. Dans la majorité des systèmes de cryptage symétrique la clé de chiffrement et la clé de déchiffrement sont identiques.

3.2.6.1 Algorithmes de chiffrement classique

a. Chiffrement XOR

Le système de chiffrement XOR est un système de cryptage basique mais pas trop limité. Ainsi, il a beaucoup été utilisé dans les débuts de l'informatique et continue à l'être encore aujourd'hui car il est facile de l'implanter, dans tous les programmes.

Le XOR est un opérateur logique qui correspond à un "OU exclusif" : c'est le (A OU B) qu'on utilise en logique mais qui exclue le cas où A et B sont simultanément vrais. Voici sa table de vérité :

Tableau 3.01 : *Tableau de vérité de XOR*

A	B	$A \otimes B$
FAUX	FAUX	FAUX
FAUX	VRAI	VRAI
VRAI	FAUX	VRAI
VRAI	VRAI	FAUX

En informatique, chaque caractère du message à coder est représenté par un entier, le code ASCII.

Ce nombre est lui-même représenté en mémoire comme un nombre binaire à 8 chiffres (les bits).

On choisit une clé que l'on place en dessous du message à coder, en la répétant autant de fois que nécessaire, comme dans le cryptage de Vigenère.

Le message et la clé étant converti en binaire, on effectue un XOR, bit par bit, le 1 représentant

VRAI et le 0 FAUX. Le résultat en binaire peut être reconverti en caractères ASCII et donne alors le message codé.

L'algorithme est complètement symétrique : la même opération est réappliqué au message final pour retrouver le message initial.

Dans notre cas on va crypter un signal en utilisant cette technique en convertir le MP3 tout d'abord sous forme binaire et après on effectue le XOR avec un nombre bien précis qu'on peut appeler la clé de cryptage puisque ce nombre doit toujours le même en décryptage.

b. Propriété d'opération sur le XOR en binaire

- Tableau de vérité : [3.03]

I_1	I_2	Out
0	0	0
0	1	1
1	0	1
1	1	0

- Equation logique

$Out = I_1 \oplus I_2 = I_1.\overline{I_2} + \overline{I_1}.I_2$

3.2.6.2 Algèbre de BOOLE

a. Définition

Les variables de l'algèbre de BOOLE ne peuvent prendre que 2 valeurs possibles (0 : faux et 1 : vraie)

Chaque valeur de la variable possède un état (soit bas, soit haut).

Les 3 opérations élémentaires sont : l'addition logique, la multiplication logique et l'inversion logique.

b. Propriétés de l'algèbre de BOOLE

- L'involution :

$$\bar{\bar{x}} = x \tag{3.01}$$

- Commutative :

$$x.y = y.x \tag{3.02}$$

$$x + y = y + x \tag{3.03}$$

- Idempotence :

$$x + x = x \tag{3.04}$$

$$x.x = x \tag{3.05}$$

- Théorème de complémentation :

$$x + \bar{x} = 1 \tag{3.06}$$

$$x.\bar{x} = 1 \tag{3.07}$$

- Distributivité de ET par rapport à OU

$$x.(y + z) = xy + xz \tag{3.08}$$

- Distributivité de OU par rapport à ET

$$x + yz = (x + y).(y + z) \tag{3.09}$$

- Théorème d'absorption

$$x + xy = x \tag{3.10}$$

$$x + (x + y) = x \tag{3.11}$$

- Théorème de Consensus

$$ax + b\bar{x} + ab = ax + b\bar{x} \tag{3.12}$$

$$(a + x)(b + \bar{x})(a + b) = (a + x)(b + \bar{x}) \tag{3.13}$$

- Théorème de DEMORGAN

$$\overline{x + y} = \bar{x}.\bar{y} \tag{3.14}$$

$$\overline{x.y} = \bar{x} + \bar{y} \tag{3.15}$$

3.3 Représentation de l'émission en SW sous simulink

Le bloc suivant (figure 3.04) est un bloc de simulation qui fait la transmission par onde courte en utilisant les différentes méthodes comme la technique de modulation et démodulation en amplitude sans porteuse.

Le signal audio va tout d'abord s'importer et après importation, il va entrer dans le bloc modulateur qui va moduler le signal audio entrant et après, il suit le canal de transmission contenant toujours de bruit. Après cela, le signal modulé s'achemine vers un bloc démodulateur en passant vers un filtre passe bas et ce dernier met en effet retour vers le signal d'origine.

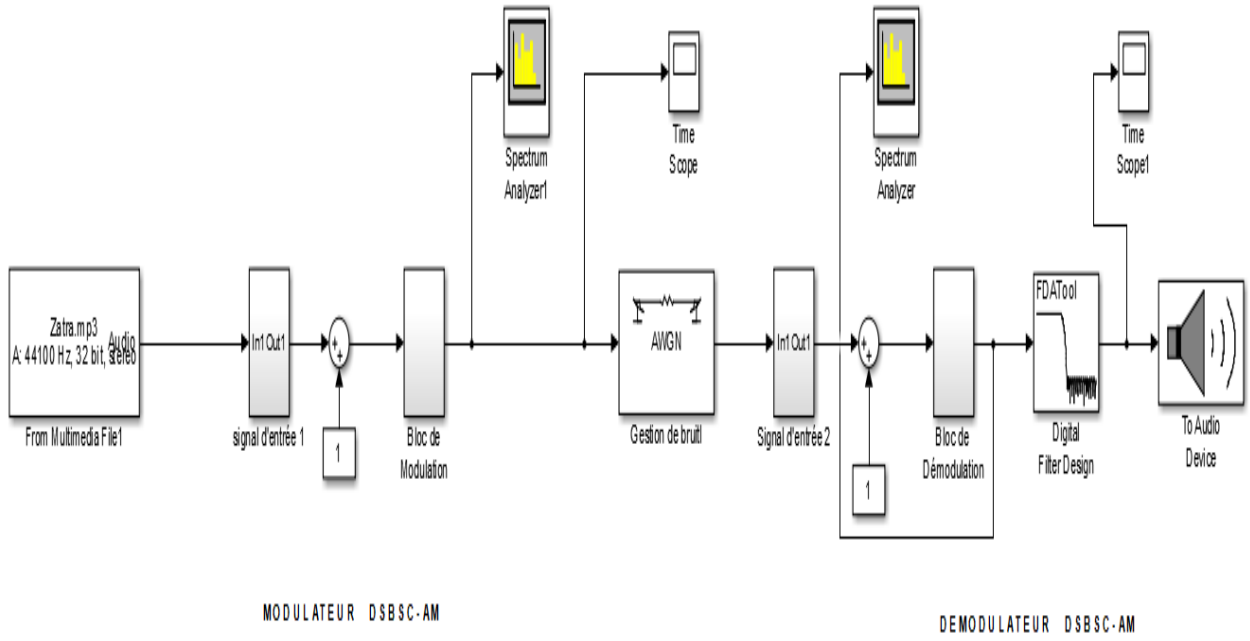

Figure 3.04 : *Modèle de transmission onde courte sous simulink*

3.3.2 Fonctionnalité de chaque bloc

3.3.2.1 Bloc de récupération de fichier multimédia

Le bloc (figure 3.05) suivant a pour fonction de charger les échantillons de fichier audio ou vidéo selon le type de média choisi par l'utilisateur contenu dans le disque dur de l'ordinateur.

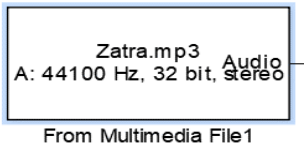

Figure 3.05 : *Bloc de récupération de fichier multimédia*

3.3.2.2 Bloc de signal d'entrée

Le bloc (figure 3.06) va spécifier la nature de signal d'entrée, il est programmable si on connait le type de signal d'entrée et il va générer le signal en entrée et sortie et produit une erreur si la sortie et l'entrée ne convient pas de même nature. Mais si on ne connaît pas le type de signal, ce bloc va classer par défaut le signal.

Figure 3.06 : *Check signal attributes*

3.3.2.3 Bloc de modulateur DSBSC-AM

a. Sous simulink Matlab

C'est cet bloc qui va générer la modulation du signal à l'entrée et comme son nom l'indique, il utilise la technique de modulation d'amplitude double bande sans porteuse. Le DSBSC-AM est un terme en anglais qui veut dire Double Side Band Suppressed-Carrier-Amplitude Modulation.

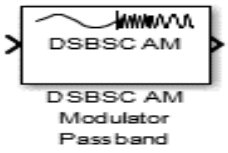

Figure 3.07 : *Modulateur DSBSC-AM*

En envoyant la musique dans la simulation qui va passer du modulateur DSBSC-AM, on obtient ces résultat en voyant le Spectrum qui va donner le résultat spectrale du modulateur et sur l'oscilloscope pour voir le résultat temporelle.

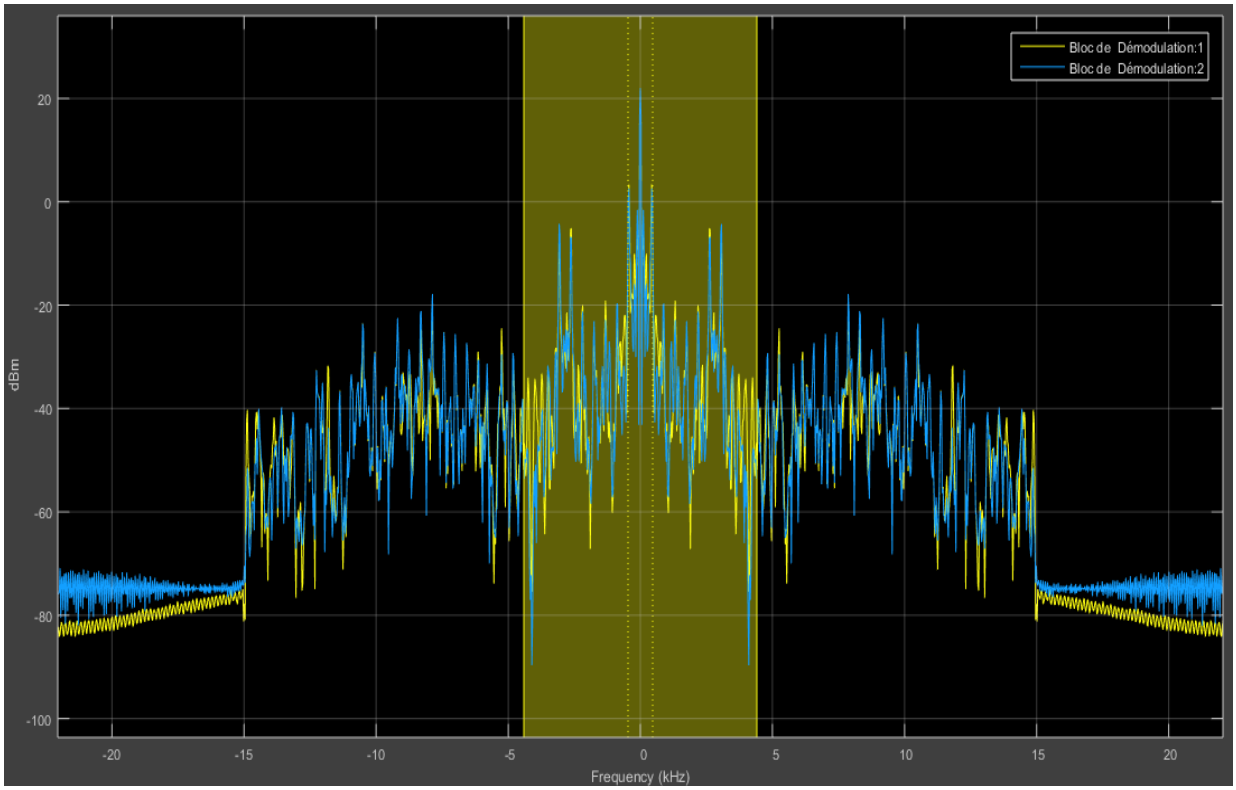

Figure 3.08 : *Représentation spectrale du modulateur sous matlab*

Dans cette figure (3.08), on voit le spectre de signal modulé avec la bande latérale supérieure et la bande latérale inférieure.

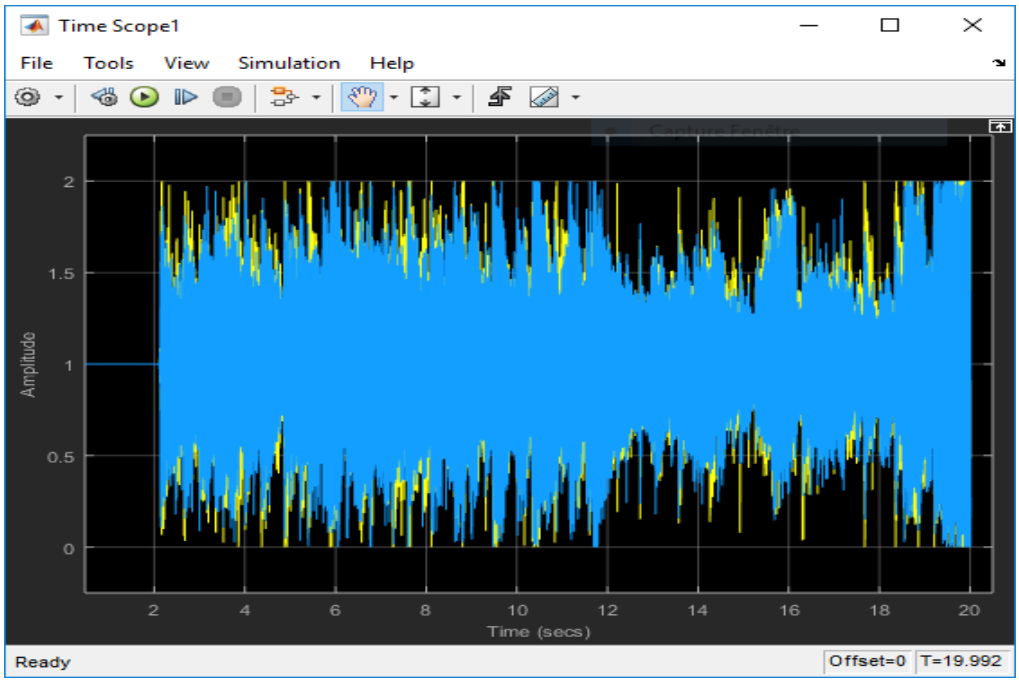

Figure 3.09 : *Représentation temporelle du modulateur sous matlab*

Les figures (3.08) et (3.09) sont les représentations respectives de la représentation spectrale et temporelle sous matlab.

b. Modélisation de la modulation DSBSC-AM

En modulation d'amplitude, l'information du message à transmettre (ou signal modulant $m(t)$ est représenté par l'amplitude du message modulé $s_{DSB}(t)$.

Soit $m(t)$ le message, de largeur de bande W et $p(t)$ la porteuse.

Message : $m(t)$

Porteuse : $p(t) = P\cos(2\pi f_p\, t + \theta_p)$

Remarque : la fréquence de la porteuse $f_p >> W$ et $\theta_p = 0$ puisqu'on ne s'intéresse beaucoup qu'à l'amplitude. Le signal modulé est obtenue en multipliant le message avec la porteuse.

$$s_{DSB}(t) = P.m(t).\cos(2\pi f_p\, t)$$

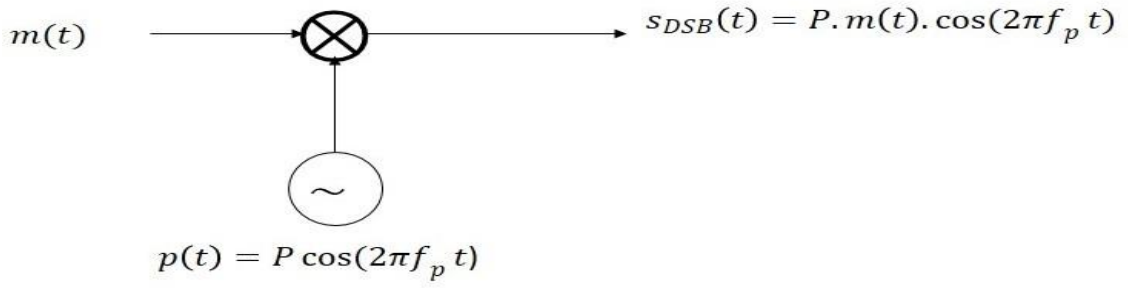

Figure 3.10 : *Modulateur DSBSC-AM*

Dans le domaine fréquentiel, le signal modulé $s_{DSB}(f)$, peut être exprimé en fonction du spectre du message $M(f)$ en bande de base.

$$s_{DSB}(f) = \mathcal{F}[s_{DSB}(t)] = \mathcal{F}[m(t) \times p(t)]$$

$$s_{DSB}(f) = \mathcal{F}[m(t)] * \mathcal{F}[p(t)]$$

$$s_{DSB}(f) = M(f) * \mathcal{F}[\mathrm{P}\cos(2\pi f_p\, t)]$$

$$s_{DSB}(f) = M(f) * \frac{P}{2}[\delta(f + f_p) + \delta(f - f_p)]$$

Avec $\mathcal{F}$ est la transformée de Fourier de l'argument. On obtient donc le spectre du signal modulé :

$$s_{DSB}(f) = \frac{P}{2}[M(f + f_p) + M(f - f_p)]$$

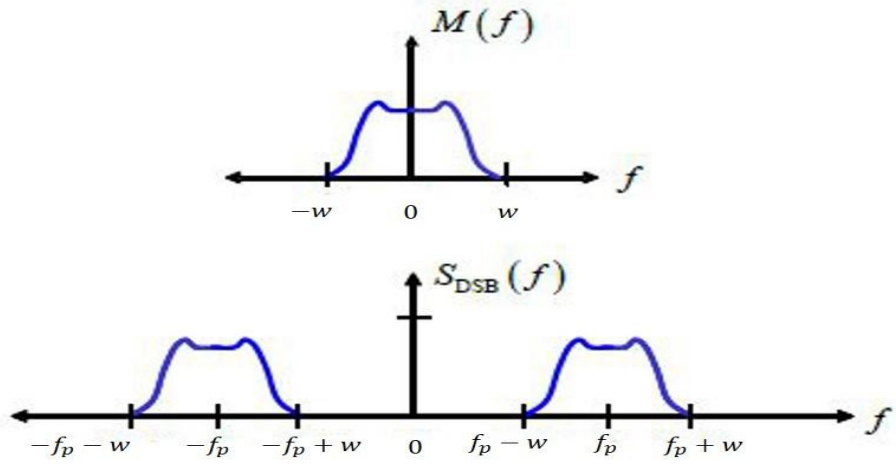

Figure 3.11 : *Spectre du signal modulé $s_{DSB}(f)$*

Dans le domaine temporel, le signal modulé a une allure comme suit (figure 3.12) : [3.03]

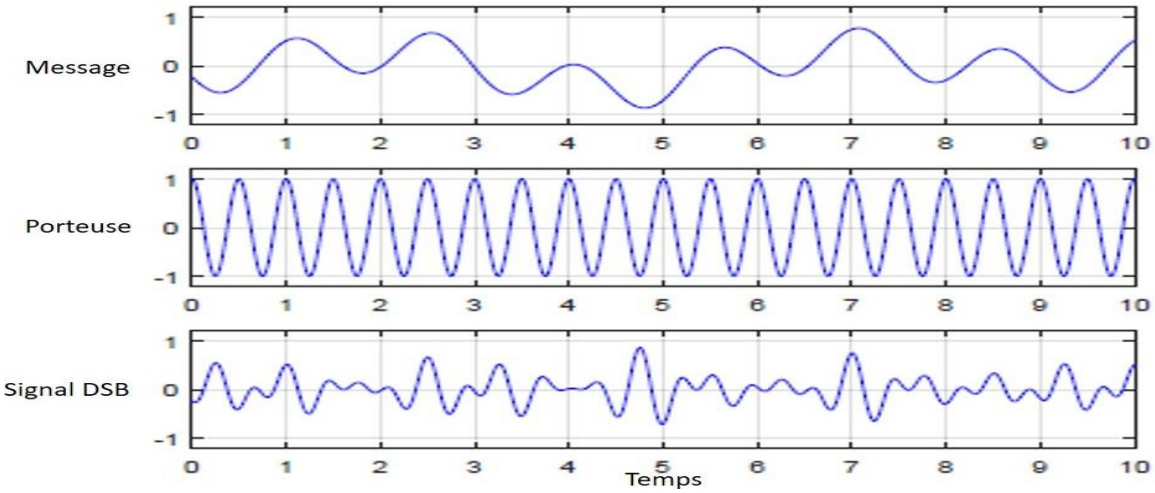

Figure 3.12 : *Exemple du signal modulé*

3.3.2.4 Bloc de démodulateur DSBSC-AM

a. Sous Simulink

C'est ce bloc qui va générer la démodulation du signal à l'entrée.

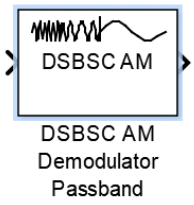

Figure 3.13 : *Démodulateur DSBSC-AM*

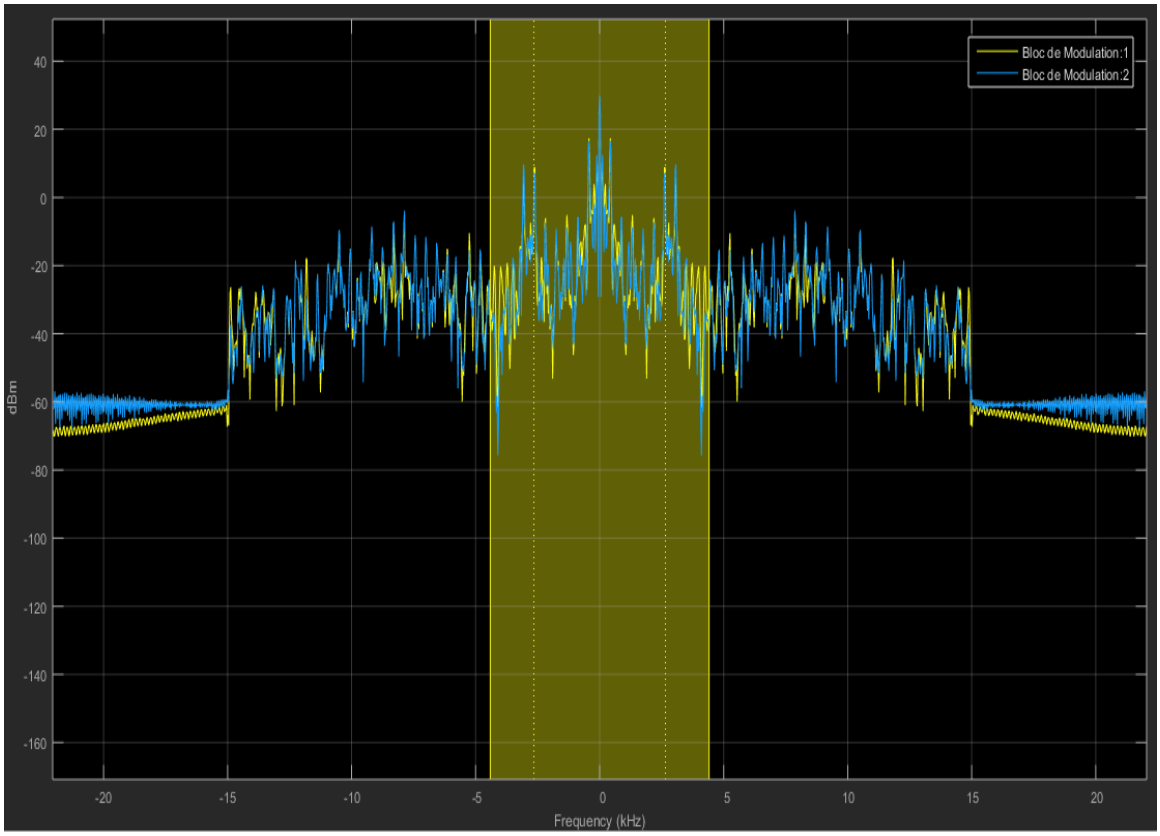

Figure 3.14 : *Résultat spectrale du démodulateur sous matlab*

b. Modélisation du démodulateur DSBSC-AM

Au récepteur, le signal reçu $r(t)$ doit être démodulé dans la forme originale du message $m(t)$. Par exemple le signal $r(t)$ reçu d'une station de radiodiffusion doit être reconverti aux fréquences radio.

Dans la figure (3.15), on voit le fonctionnement d'un démodulateur DSBSC-AM. Le signal reçu $r(t)$ va entrer dans le mélangeur avec une porteuse, et après cela il va entrer dans un filtre passe bas qui va filtrer les signaux basses fréquences et qui atténue les hautes fréquences c'est-à-dire les fréquences supérieures à la fréquence de coupure pour avoir en sorti le signal $m_r(t) \backsimeq m(t)$

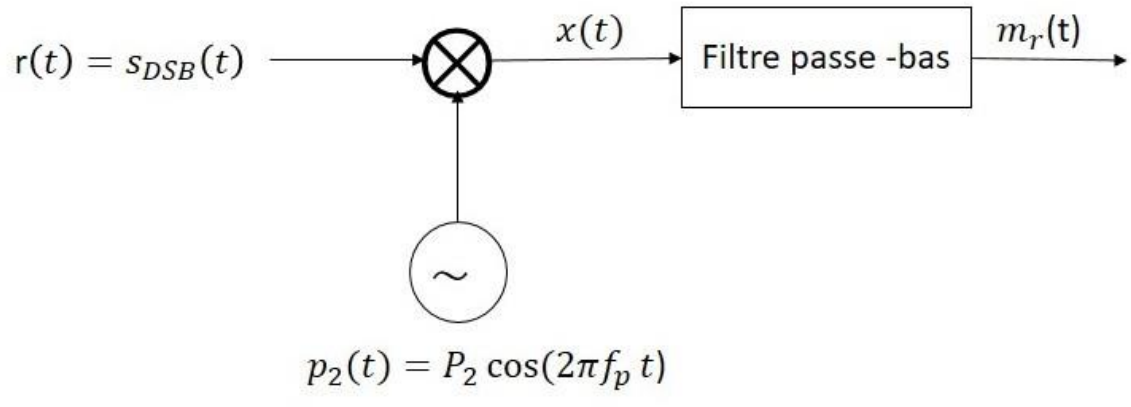

Figure 3.15 : *Démodulateur DSBSC-AM*

m_r(t) est l'estimé à la réception du signal d'origine $m(t)$. A la sortie de mélangeur, on a le signal $x(t)$ de la forme

$$x(t) = r(t)p_2(t) = [P\ m(t)\cos(2\pi f_p\ t)]P_2\cos(2\pi f_p\ t)$$

$$x(t) = P\ P_2 cos^2((2\pi f_p t)$$

$$x(t) = P\ P_2 m(t)\frac{1}{2}[1 + \cos(4\pi f_p\ t)]$$

$$x(t) = \left(\frac{P\ P_2}{2}m(t)\right) + \left(\frac{P\ P_2}{2}m(t)\cos(4\pi f_p\ t)\right)$$

Avec : $\frac{P\ P_2}{2}m(t)$: composante en bande de base

$\frac{P\ P_2}{2}m(t)\cos(4\pi f_p\ t)$: Composante à $2f_p$

Le signal $m_r(t)$ est obtenu par le filtrage du sgnal $x(t)$ à l'aide d'un filtre passe-bas dont la fréquence de coupure f_c est : $w < f_c < f_c - w$.

Cette fréquence de coupure f_c est légèrement supérieure à w afin de laisser passer tout le message $m(t)$ sans toutefois passer le bruit hors bande. $m_r(t)$ est donc comme suit:

$$m_r(t) = \frac{P\ P_2}{2}m(t)$$

Cette valeur de $m_r(t)$ est proportionnel au message original $m(t)$. Dans le domaine fréquentiel

$$X(f) = \mathcal{F}[x(t)] = \mathcal{F}[m(t)p(t)p_1(t)] = \mathcal{F}[m(t)] * \mathcal{F}[p(t)] * \mathcal{F}[p_1(t)]$$

$$X(f) = M(f) * \frac{P}{2}[\delta(f - f_p) + \delta(f + f_p) * \frac{P_2}{2}[\delta(f - f_p) + \delta(f + f_p)]$$

$$X(f) = \left(\frac{PP_2}{4}\right)M(f) * [\delta(f - f_p) + \delta(f + f_p)] * [\delta(f - f_p) + \delta(f + f_p)]$$

$$X(f) = \left(\frac{PP_2}{4}\right) M(f) * \left[\delta(f - 2f_p) + 2\delta(f) + \delta(f + 2f_p)\right]$$

$$X(f) = \left(\frac{PP_2}{4}\right) [M(f - 2f_p) + 2M(f) + M(f + 2f_p)$$

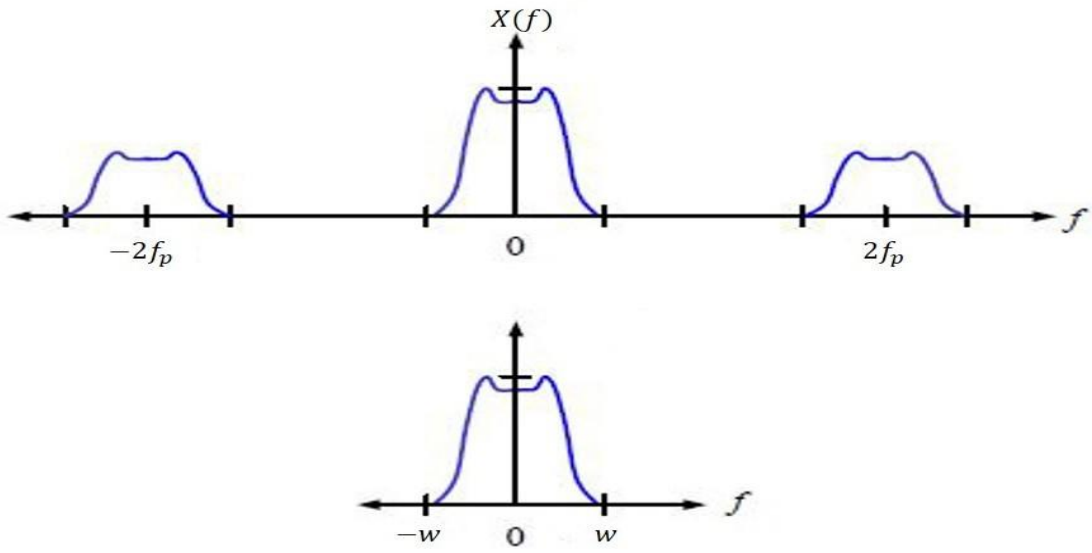

Figure 3.16 : *Spectre du signal DSBSC-AM à la sortie du mélangeur*

Après filtrage passe-bas de $X(f)$, on obtient finalement

$$M_r(f) = \left(\frac{PP_2}{2}\right) M(f)$$

3.3.2.5 Bloc de canal de AWGN

Le bloc de canal de AWGN (Add White Gaussian Noise) ajoute un bruit gaussien blanc au signal d'entrée selon leur nature : réel ou complexe. Lorsque le signal est réel, ce bloc ajoute de vrais bruits réels. Et lorsque le signal d'entrée est complexe, ce bloc ajoute un bruit gaussien complexe et produit ainsi un signal de sortie complexe.

Donc, ce bloc hérite de la durée d'échantillonnage de signal d'entrée. La représentation de canal d'AWGN sous matlab est le suivant :

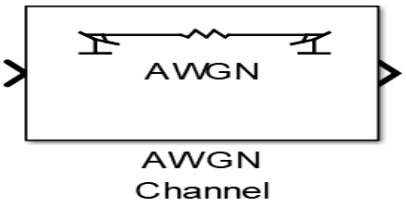

Figure 3.17 : *Représentation de canal de AWGN sous matlab*

3.3.2.6 Bloc de filtre passe-bas

Ce bloc (figure 3.18) peut utiliser comme bloc de conception de filtre numérique et qu'on peut mettre en œuvre plusieurs fonctionnements puisqu'il est paramétrable selon nos besoins. Le filtre qu'on conçoit peut filtrer les signaux monocanaux ou multicanaux. Le bloc de conception de filtre numérique est idéal pour simuler le comportement numérique de notre filtre sur un système virgule flottante tel qu'un ordinateur personnel ou une puce DSP. On peut utiliser le produit de code Simulink comme illustrer le figure suivante :

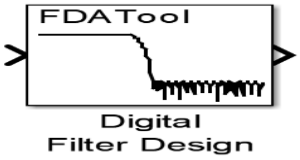

Figure 3.18 : *Filtre numérique sous matlab*

3.4 Conclusion

Ce dernier chapitre contient, premièrement, l'étude au niveau de la transmission en onde courte accompagné par le modèle mathématique appliqué qu'on assimile sous matlab pour voir les résultats et deuxièmement la sécurisation de données pour avoir une information cachée en utilisant une méthode de chiffrement.

CONCLUSION GENERALE

Le choix de la transmission d'informations par onde courte ou ShortWave (SW) (qui utilise la gamme de fréquence HF (High Frequency) et la technique de modulation d'amplitude) est la capacité de cette onde de suivre la courbure de la terre sans recours à un satellite et peut surmonter à toute obstacle qui la face, il peut atteindre donc des lieux qui se situent entre plusieurs milliers de kilomètre.

Les ondes transmises par l'émetteur ne sont pas toujours faites et utiles pour tous les récepteurs. Elles peuvent donner une mauvaise foi aux hacheurs de brouiller le signal ou de pirater la fréquence de l'émetteur afin que l'émission à émettre n'arrive plus à sa destination. C'est pour cela que nous utiliserons la méthode de cryptographie pour cacher l'information.

Pour les stations cibles qui reçoivent des signaux ou des informations cryptées de part des émetteurs différents, il est nécessaire d'apporter plus d'amélioration pour une implantation de serveur pour le stockage des données et pour le décryptage.

Nous pouvons créer un destinataire comme perspective, car personne ne peut pas capter le signal sécurisé ou l'information cryptée sans passer par ce serveur qui est le destinataire capter et le décrypter pour réémettre le signal dans une zone bien délimitée.

Pour une meilleure sécurisation, on suggère une méthode qui consiste à combiner deux différentes méthodes de chiffrement pour avoir plus de confidentialité et d'assurer plus de sécurité au niveau des informations diffusées.

ANNEXE 1 LOGICIEL MATLAB

A1.1 MATLAB

A1.2 Interface graphique

Le logiciel Matlab est un logiciel qui propose un environnement interactif de développement qui dispose d'un langage propre qui facilite les manipulations de données numériques ou analogique et souvent utiliser dans les sciences appliquées. L'application intègre un langage de haut niveau qui autorise l'exécution de tâches qui nécessitent une grande puissance de calcul. Ce logiciel offre ainsi le support de fonction mathématique de base pour l'algèbre linéaire, les statistiques, l'analyse de Fourier, le filtrage, etc. C'est-à-dire il utilise une écriture plus proche du langage naturel scientifique. Il offre aussi de logiciel de simulation interne pour les sciences appliquées en utilisant les différents schéma bloc.

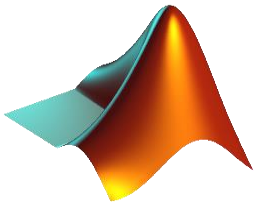

Figure A1.01 : *Logo de logiciel Matlab*

Même si la simulation a été fait sur Simulink dans le cas de la transmission SW et à l'aide avec des lignes de commande pour le traitement de signal sous matlab, une interface graphique a été conçue pour faciliter l'exécution du programme et pour me permettre plus de désigne de présentation. Et on a une interface comme suit :

Figure A1.02 : *Interface d'accueil projet*

ANNEXE 2 ONDES ELECTROMAGNETIQUE

A2.1 Caractéristique de l'onde électromagnétique

L'onde l'électromagnétique peut être caractérisé par sa puissance, sa polarisation et sa fréquence.

A2.1.1 Puissance de rayonnement d'une onde

L'onde électromagnétique est une forme d'énergie, l'énergie de rayonnement qui est d'autant plus forte que les intensités des champs électriques et magnétique. Il est courant de parler de la puissance de rayonnement émise par une source et de la densité de puissance existant autour de la source. L'expérience montre qu'une source d'onde S de puissance de rayonnement P_t émettant uniformément dans toutes les directions de l'espace distribuera à une distance d une densité de puissance P_r , tel que:

$$P_r = \frac{P_t}{4\pi d^2} \tag{3.16}$$

Avec P_r : densité de puissance de l'onde exprimée en watt par mètre carré (W/m^2)

P_t : Puissance de rayonnement émise par la source

- Puissance de rayonnement reçue par un récepteur

Un récepteur de surface de réception S_r recevra une puissance

$$P_R = \frac{P_t . S_r}{4\pi d^2} \tag{3.17}$$

A2.1.2 Polarisation d'une onde

La polarisation d'une onde est le plan dans lequel varie le champ électrique. Certaine émission d'onde électrique se font à polarisation horizontale et d'autre à polarisation verticale ou même circulaire ou elliptique.

Voyons deux exemples de ces polarisations très utilisées :

- Pour la polarisation circulaire $E \operatorname{Sin} wt$ est le composante horizontale et $E \operatorname{Cos} wt$ est le composante verticale du champ électrique $\vec{\mathrm{E}}$ avec w étant la pulsation à laquelle le champ électrique évolue

  Voici la forme canonique pour une polarisation circulaire

$$E_x{}^2 + E_y{}^2 = E^2 \tag{3.18}$$

Cette figure (A2.01) illustrant l'exemple d'une polarisation horizontale.

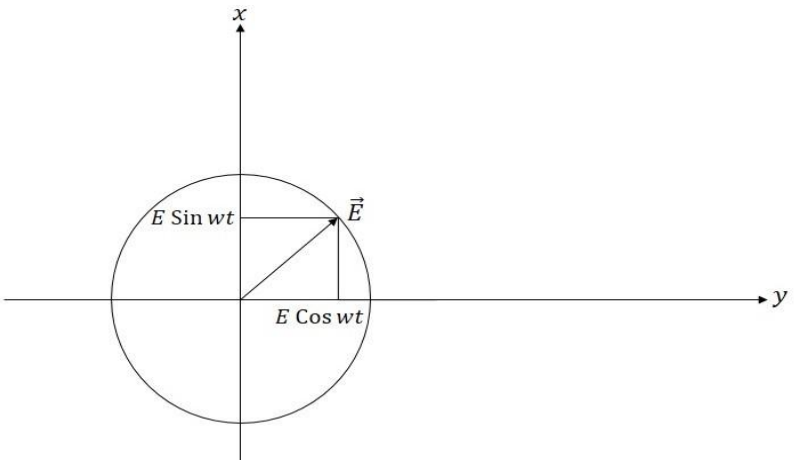

Figure A2.01 : *Polarisation horizontale*

- De même les composantes horizontales et verticales d'une onde à polarisation elliptique seront respectivement E_1 Sin wt et E_2 Cos wt tel que E_x et E_y dépend bien au cordonnée d'une ellipse donné sous la forme canonique

$$\frac{{E_x}^2}{{E_1}^2} + \frac{{E_y}^2}{{E_2}^2} = 1 \qquad (3.19)$$

Avec E_1 , E_2 : sont les axes des composantes horizontale et verticale des champs électrique

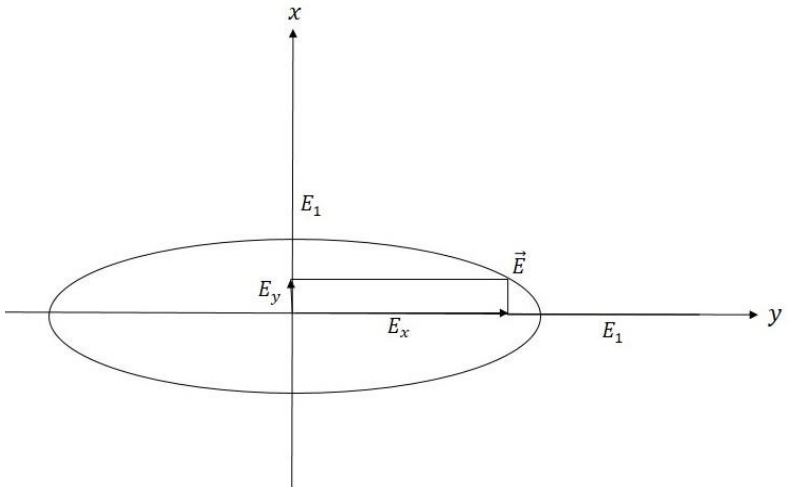

Figure A2.02 : *Exemple de polarisation elliptique*

A2.1.3 Fréquence et longueur d'onde

A2.1.3.1 *Fréquence*

La fréquence d'une onde électromagnétique est la fréquence des champs électriques et magnétiques qui la compose.

Voici la formule générale de la fréquence :

$$f = \frac{1}{T} \tag{3.20}$$

Avec T : période pour chaque oscillation

A2.1.3.2 *Longueur d'onde*

La longueur d'onde λ est le trajet parcourue par une onde après une période d'oscillation T.

$$\lambda = v.T \tag{3.21}$$

Avec v : vitesse de la lumière dans le vide équivaut à $3.10^8\ m/s$.

A2.2 Bruits dans la communication

Les émissions électromagnétiques s'accompagnent toujours de parasite ou bruit qui fait perturber.

A2.2.1 Quelque type de bruit

A2.2.1.1 *Bruit électromagnétique*

Les bruits électromagnétiques sont des ondes dont on ne peut prédire la fréquence ou même le moment d'apparition, il se mêle à l'émission électromagnétique dont il limite la portée. Leur puissance est en général faible et lorsque la puissance de rayonnement de l'émission est de l'ordre de grandeur de celle des bruits, l'émission n'est plus détectable.

A2.2.1.2 *Bruit atmosphérique*

Les bruits atmosphériques sont des bruits provenant des éclairs, il y a en moyenne près de 100 éclaires/s sur la terre et la présence des bruits dépend donc de la saison et la géographie. Ses bruits perturbent les émissions en ondes courtes et en ondes moyennes.

A2.2.1.3 *Bruit cosmique*

Les bruits cosmiques sont des rayonnements provenant des diverses étoiles galactiques ou extragalactiques. Le soleil émet des bruits non négligeables surtout comme l'orage solaire qui pouvait durer de quelque heure en quelque jour.

Facteur de bruit

Le traitement du signal réalise par les différents blocs analogiques a comme conséquence secondaire une addition de bruit en sortie de ces blocs. Le facteur de bruit est le paramètre qui caractérise la dégradation de la qualité du signal suite à l' augmentation du niveau de bruit causé par le passage dans les blocs analogiques.

Il est défini par:

$$F = \frac{SNR_{in}}{SNR_{out}} = \frac{P_{in}/N_{in}}{P_{out}/N_{out}} = \frac{N_{in}}{N_{out}G} \tag{3.22}$$

Avec

P_{in}: puissance du signal d'entrée

P_{out}: puissance du signal à la sortie

N_{in}: puissance du bruit dans le signal d'entrée

N_{out}: puissance du bruit dans le signal de sortie

G: gain definit le rapport entre le la puissance du signal de sortie et la puissance du signal d'entrée.

REFERENCES

[1.01] S. Salous, *« Radio Propagation Measurement and Channel Modeling »*, Wiley, 2013.

[1.02] N. Blaunstein, C. Christodoulo, *« Radio Propagation and Adaptive Antennas for Wireless Communication Links »*, Wiley,2007.

[1.03] T.N.M. Ralaibozaka *« Modèle de Propagation des Canaux SISO dans un système de communication sans fil »*, Mémoire pour obtention du DEA, Département Télécommunication, ESPA, A.U. : 2012-2013.

[1.04] J. Joseph, W. Hippisley *« Pratical Antenna Handbook »*, McGraw-Hill, 5ème edition, US, 2012.

[1.05] P.L. Cayrel, *« Cours de cryptographie »*, Hubert, 2010.

[2.01] https://fr.scribd.com/document/129262196/3-traitement-numerique-du-son-pdf, consulté le 06/02/19.

[2.02] Y. Gerini *« Shortwave Propagation and Communications systems », 2009.*

[2.03] S. Jacques, G. Louis, N. Phong, *« Conception et preuves d'algorithmes »,2004.*

[2.04] C.R. Anderson, « Modern Communication Systems Amplitude Modulation »,2015

[2.05] H.S. Rafalinirina, *« Communication Analogique »* cours 3ème année, Télécommunication, IES-AV, A.U : 2017-2018.

[3.01] S.N. Ghosh, *« Electromagnetic theory and wave propagation »*, 2002.

[3.02] L.Guezoli, *« Master Cryptographie & Sécurité », 2011.*

[3.03] M.E. Randrianandrasana, *« Logique combinatoire »* cours 3ème année, Télécommunication, IES-AV, A.U : 2017-2018.

FICHE DE RENSEIGNEMENTS

Nom : TODISOA

Prénoms : Hasina Fanantenana

Adresse de l'auteur : Lot 0514 L 334 Tomboarivo

Antsirabe 110 - Madagascar

Téléphone : +261 34 87 142 32

E-mail : thfanantenana@gmail.com

Titre du mémoire :

« SECURISATION DES DONNEES DIFFUSEES PAR EMETTEUR SW (SHORTWAVE) »

Nombre de pages : 50

Nombre de tableaux : 2

Nombre de figures : 47

Directeur de mémoire :

Nom : RALAIBOZAKA

Prénoms : Tahina Nancy Muriel

Grade : Assistante d'Enseignement Supérieur

Téléphone : +261 34 01 045 97

Email : nancytahina@gmail.com

FAMINTINANA

Ny fitaovana fandefasam-peo mampiasa onja fohy dia afaka mahatratra ny mpihaino amina faritra rezionaly sy iraisam-pirenena. Izany dia azo avy amin'ny fanapariahana lavitr'ezaka avy amin'ny fampielezana onja fohy mitondra taratra manana toetra mamerina hazavana any amin'ireo tongoana habaka avo indrindra. Ny fampielezam-peo mampiasa onja fohy dia tena ilain'ny mponina izay sarotra tratrarina. Io fampitana onja lavitr'ezaka io dia mety hisy olona mpisompatra ka izany indrindra no antony hanoloran-kevitra hiarovana ny angon-kevitra alohan'ny hanapariahana azy ary mba hametrahana mpizara eo amin'ny mpandray hafatra, izay afaka mamaky izany, ary mandefa indray any amin'ny faritra voafaritra tsara.

Teny misongodina : onja fohy SW, fanafenana hafatra, fikirakirana famantarana manokana, fampitana, DSBSC-AM.

RESUME

Un émetteur à ondes courtes est capable d'atteindre des auditeurs à l'échelle régionale et internationale. Ceci est dû aux propriétés de propagation à longue distance de la radiodiffusion en ondes courtes portée par de multiples réflexions dans les différences couches de la haute atmosphère. La radiodiffusion en ondes courtes est donc essentielle pour les habitants de région isolée. Cette transmission d'onde à longue distance peut être captée par des personnes gaffeuses et c'est pour cela qu'on propose de chiffrer les données avant d'émettre et d'implanter un serveur au niveau de destinataire qui peut capter et déchiffrer le signal envoyé. Et il réémettre le signal vers une zone de couverture bien délimiter.

Mots clés : onde courte SW, chiffrement, traitement de signal, transmission, DSBSC-AM.

ABSTRACT

A shortwave transmitter is able to reach listeners on a regional and international scale. This is due to the long-range propagation properties of short-range broadcasting by multiple reflections in the upper atmosphere layer differences. This long-distance transmission can be picked up by gaffers and that is why it is proposed to encrypt the data before issuing and implementing a server at the recipient level that can capture and decrypt the sent signal. And he re-emit the signal to a well-defined coverage area.

Keywords : ShortWave SW, encryption, signal processing, transmission.