République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNVIERSITÉ ABOU BEKR BELKAID DE TLEMCEN

FACULTÉ DE TECHNOLOGIE

DÉPARTEMENT DE TELECOMMUNICATION

MEMOIRE

Présenté pour l'obtention du diplôme de MASTER
En Télécommunications
Spécialité : Systèmes de télécommunication

Conception d'une chaîne de transmissions de données cryptées sur logiciel LABVIEW

Soutenu le 8 juillet 2021 devant le jury:

Président:	Mr BORSALI Ahmed Riad	UABB Tlemcen
Examinateur:	Mme BENLALDJ Lamia	UABB Tlemcen
Encadreur :	Mme BENMANSOUR Fatima Zohra	UABB Tlemcen

Présenté par:

ZEGGAI Zeyd

ZERROUK Nassim

Année académique: 2020-2021

Résumé

Avec l'avènement d'Internet et du Smartphone, Il est évident que la transmission et la réception de données numériques est un événement quotidien commun. La communication est passée au numérique en raison des nombreux avantages concrets tels que la sécurité, la compression et la correction des erreurs. Aujourd'hui, il est nécessaire d'améliorer les systèmes de communication numérique et de les rendre plus sécurisé.

Ce travail a pour principal objectif l'implémentation d'une chaine de transmission cryptée avec le logiciel LABVIEW qui nous a permis de modéliser de façon très pédagogique cette chaine de transmission et d'analyser les performances en termes de rapport signal sur bruit.

Mot clé : Chaine de transmission, Cryptée, Signal sur bruit.

Abstract

With the advent of the Internet and the Smartphone, it is evident that the transmission and reception of digital data is a common daily event. The communication has moved to digital because of the many benefits such as security, compression and error correction. Today, it is necessary to improve digital communication systems and make them more secure.

The main objectvie of this work is to implement an encrypted transmission chain with the LABVIEW software, which allows us to model this transmission chain in a very pedagogical way and analyse the performance in terms of signal-to-noise ratio.

Key Word : Transmission chain, Encrypted, Signal-to-noise ratio.

ملخص

مع ظهور الإنترنت والهاتف الذكي، أصبح نقل البيانات الرقمية واستقبالها حدث يومي شائع.
انتقل الاتصال إلى المجال الرقمي بسبب الفوائد العديدة مثل الأمن و الضغط وتصحيح الأخطاء. واليوم، من الضروري تحسين نظم الاتصالات الرقمية وجعلها أكثر أمنا.
الهدف الرئيسي من هذا العمل هو إنشاء سلسلة إرسال مشفرة ببرنامج LABVIEW ، الذي سمح لنا بنمذجة سلسلة الإرسال هذه بطريقة بداغوجية مما سمح بتحليل أدائها تحت تأثير نسبة الضجيج.

الكلمات المفتاحية :سلسلة الإرسال مشفرة نسبة الضجيج

Remerciements

Ce travail a été réalisé dans le cadre du projet de fin d'études, au département de télécommunication de Tlemcen

Premièrement et avant tout Dieu merci de nous avoir donné foi, force et santé pour lire écrire et produire et finaliser se travail.

Ce travail a été encadré par Mme Benmansour, que nous remercions Vivement pour l'encadrement de ce projet de fin d'études.

Nous exprimons nos sincères remerciements aux membres du jury, d'avoir accepté d'examiner notre projet de fin d'études.

Nos Vifs remerciements vont aussi à l'ensemble des enseignants qui ont contribué à notre formation.

Dédicaces

C’est avec grand plaisir que je dédie ce modeste travail :

A mes très chers parents

A mon cher frère Nouh

A ma chère sœur Meriem

A tous mes proches et mes amis

ZEGGAI ZEYD

Dédicaces

Je dédie ce mémoire

A mon père allah yerhmou et à ma mère pour leur amour inestimable, leurs sacrifices, leur confiance, leur soutien et toutes les valeurs qu'ils ont su m'inculquer.

A ma sœur Meryem et mon petit frère Yanis pour leur tendresse, leur complicité, leur amour.

A mes deux grands-mères pour toute l'affection qu'elles m'ont données

A mes deux tantes et mes deux cousines, pour leurs mots d'encouragement et leurs gentillesses.

A mon ami Said pour son soutien moral, ses multiples conseils, sa disponibilité malgré ses multiples occupations.

A Mes collègues, proches, amis et connaissances…

ZERROUK NASSIM

Table des matières

Liste des figures

Liste des tableaux

Liste des Abréviations

AM : Amplitude Modulation

BPSK : Binary phase Shift Keying

QPSK : Quadrature Phase Shift Keying

FM : Frequency Modulation

QAM : Quadrature Amplitude Modulation

RII : Réponse Impulsionnelle Infinie

ARQ : Automatic Repeat reQuest

FEC : Forward Error Correction

BF : Basse Fréquence

HF : Haute Fréquence

W-CDMA : Wide Band CodeDivision Multiple Access

MIC : Modulation par impulsion et codage

BSC : Binary Symmetric Channel

TEB : Taux d'erreur Binaire

DSP : Densité Spectrale *de* Puissance

3G : Third Generation

HSPA+ : High Speed Packet Access

LTE : Long Term Evolution

4G : Fourth Generation

5G1 : Fifth Generation

WiFi : Wireless Fidelity

xDSL : «x» Digital Subscriber Line

DOCSIS : Data Over Cable Service Interface Specification

AES : Advanced Encryption Standard

J.-C : Jésus-Christ

NIST : National Institute of Standards and Technology

DES : Data Encryption Standard

PC : Personal Computer

XOR : Exclusviely-OR

ASCII : American Standard Code For Information Interchange

R.S.A : Rviest–Shamir–Adleman

DVB : Digital Vidéo Broadcasting

WiMAX : World Interoperability for Microwave Access

HSDPA : High Speed Downlink Packet Access

CBC : Cipher Block Chaining

AWGN : Additif White Gaussien Noise

SNR : Signal to Noise Ratio

BER : Bit Error Rate

ASK : Amplitude Shift Keying

PSK : Phase Shift keying

FSK : Frequency Shift Keying

PAM : Pulse Amplitude Modulation

PSD : Densité Spectrale de Puissance

BP : Bande Passante

RTC : Real Time Communication

CNA : Convertisseur Numérique-Analogique

MDP : Modulation à Déplacement de Phase

Introduction générale

Parmi les éléments essentiels à l'existence humaine, le besoin de communiquer arrive juste après le besoin de survie. Les méthodes dont nous nous servons pour partager idées et informations évoluent sans cesse. Si le réseau humain se limitait autrefois à des conversations en face à face, aujourd'hui les découvertes en matière de supports étendent sans cesse la portée de nos communications grâce aux réseaux de communications. La fonction principale d'un réseau est le transport de données d'une machine terminale à une autre.

La transmission de l'information se fait principalement avec des techniques numériques. La mise en œuvre de réseaux de communication reposant sur les signaux numériques présente des avantages considérables par rapport à l'exploitation des réseaux de type analogiques. Citons parmi ces avantages : une meilleure performance une grande souplesse et surtout une meilleure fiabilité

Cette évolution rapide des réseaux informatiques, privés ou publics, engendre un volume toujours plus important de données sauvegardées et transmises, générant ainsi de nouveaux besoins en matière de sécurité.

La cryptographie est devenue une composante essentielle de la sécurisation des systèmes de communication. Réservée pendant de nombreuses années au domaine militaire, la cryptographie compte aujourd'hui de nombreuses applications dans la plupart des secteurs d'activités. Il est difficile d'imaginer que l'utilisation de la carte bancaire serait possible sans sécurisation cryptographique. De même les échanges sur Internet utilisent des protocoles cryptographiques.

Les systèmes de communication numérique modernes sont très complexes et nécessitent des circuits de modulation et de démodulation de plus en plus complexes. Ces technologies sont conçues pour améliorer les performances de la transmission numérique en utilisant des techniques de modulation pour optimiser le taux de transmission.

La technique de modulation numérique QAM est utilisées dans les nouvelles générations de système de communication, Cette modulation est largement utilisée dans les modems et autres formes de communication numérique sur les canaux de transmission analogiques, notamment les téléphones mobiles 3G HSPA+ et LTE/4G, 5G1, WiFi, xDSL, DOCSIS.

Avec le développement de logiciels de simulation tel LABVIEW, il est maintenant facile de simuler une chaine de transmission complète réaliste : émission – canal de transmission – réception. Nous avons développé notre programme avec le logiciel LABVIEW, associe a la bibliothèque NI Modulation toolkit.

Le but de ce mémoire, est la conception d'une chaine de transmission numérique de données texte crypté avec algorithme AES. Ce programme est utilisé pour démontrer l'influence du bruit de canal sur le signal de modulation et le message récupéré.

Le mémoire est constitué de quatre chapitres comme suit :

Le premier chapitre sera consacré à donner un aperçu général sur la chaîne de transmission analogique et numérique.

Le second chapitre, parle tout d'abord de l'histoire de la cryptographie. Ensuite, il décrit plusieurs algorithmes symétriques et asymétriques.

Le chapitre III est consacré à une présentation détaillé de la technique de modulation QAM.

Dans le dernier chapitre on présente le logiciel LABVIEW pour la simulation d'une chaine de transmission QAM crypté. On observe aussi l'influence de changement de paramètres d'entrée sur le signal transmis dans le canal.

1. Chapitre 1 : La chaine de transmission

1.1 Introduction

Les systèmes de transmission numérique véhiculent de l'information entre une source et un destinataire en utilisant un support physique comme le câble, la fibre optique ou, encore, la propagation sur un canal radioélectrique. Les signaux transportés peuvent être soit directement d'origine numérique comme dans les réseaux de données, soit d'origine analogique (parole, image...) mais convertis sous une forme numérique. La tâche du système de transmission est d'acheminer le signal de la source vers le destinataire avec le plus de fiabilité possible.

Une chaîne de transmission est l'ensemble des dispositifs permettant le transport d'une information. Elle comprend trois éléments essentiels : une source, un canal de transmission et un destinataire. L'entrée et la sortie d'un canal de transmission sont constitués de deux dispositifs appelés « émetteur » et « récepteur » qui convertissent l'information à transmettre en un signal qui pourra être acheminé par le canal de transmission et inversement. [1]

1.2 Architecture d'une chaine de transmission numérique

Le schéma fonctionnel du système de transmission numérique est illustré à la figure I.1. On se limite aux fonctions de base :

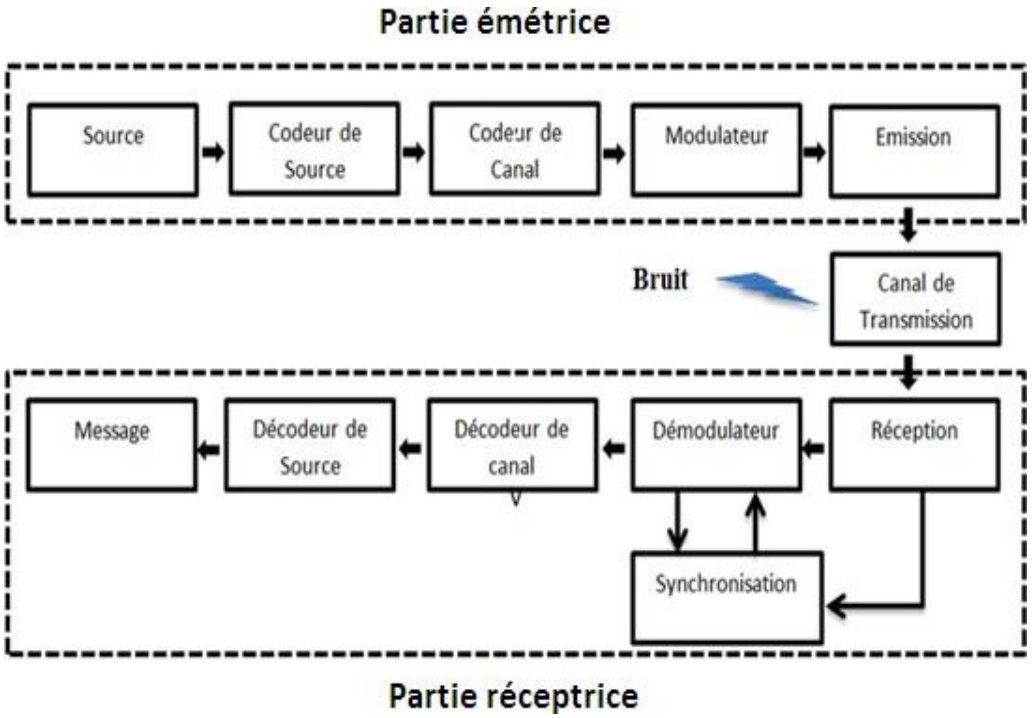


Figure I.1 : Principe d'une chaîne de transmission numérique

Remarque : cette figure est exhaustive Vis-à-vis des diverses étapes. Dans la littérature, la partie codage et l'émetteur sont quelquefois fusionnés, tout comme le récepteur-décodeur.

D’autre fois, certains graphes peuvent se focaliser sur les étapes se trouvant entre les 2 transductions.

1.2.1 Emission

Du coté émission on distingue les différents blocs

1. **Source** :

C’est le premier maillon de la chaîne de transmission. Il fournit le message porteur de l’information qui peut être soit de nature analogique ou numérique

2. **Codage de source**:

Le codage (au sens large) des signaux à transmettre se justifie pour diverses raisons, dont :

a. **Contraintes techniques**. Pour les communications radios, une onde hertzienne de même fréquence qu’un son audible est Vite atténuée. Le signal est donc porté par une onde (porteuse) de fréquence adaptée, Via un codage (**modulation**).

b. **Communications simultanées**. Toujours avec les ondes, il ne faut pas que des communications simultanées interfèrent entre elles. On utilise alors des fréquences différentes, ou du **multiplexage** (transmettre plusieurs signaux sur un même canal).

c. **Confidentialité de l’information transmise** : le message transmis peut être réservé à une personne ou un groupe. Si le signal est intercepté par une tierce personne, un cryptage peut l’empêcher d’avoir accès au contenu du message.

3. **Codage de canal :**

Le codage canal rajoute une redondance structurée aux symboles transmis pour protéger l’émission contre les erreurs. Il est appelé code détecteur d’erreur ou bien code correcteur d’erreur, c’est une fonction spécifique aux transmissions numériques elle n’a pas son équivalent en transmission analogique

Le codage canal son rôle principal dans une chaîne de communication numérique consiste donc à insérer dans le message des éléments binaires dits de redondance suivant une loi donnée. Cette opération conduit donc à une augmentation du débit binaire de la transmission.

4. Modulation numérique :

La modulation numérique a pour fonction d'adapter le signal à transmettre au canal de transmission. Elle consiste à moduler la phase, la fréquence, l'amplitude, d'une ou plusieurs porteuses centrées sur la bande de fréquence du canal, on appelle une modulation linéaire les modulations qui translate le spectre en bande de base vers la fréquence de la porteuse sans modifié l'allure de ce spectre. On appelle une modulation non linéaire toutes celles qui change la forme de spectre.

La modulation numérique permet également le partage du même canal par différent utilisateurs.

Les types de modulation numérique : Il est possible de classifie les modulations numériques de différent façon ; Les modulations linéaire : modulation d'amplitude (MDA, ASK), de phase (MDP, PSK), amplitude et phase (QAM). Les modulations non linéaire : modulation de fréquence (MDF, FSK)

La modulation peut pallier à tous les défauts liés à la transmission en bande de base, tels que :

a. Les signaux bas fréquence ont la plus grande atténuation sur la ligne,
b. Pas de propagation pour les signaux de fréquence en dehors de la bande passante du canal.
c. La perte et l'atténuation sont proportionnelles à la longueur et au type de support de transmission,
d. Il est possible de transmettre plusieurs communications sur le même support,
e. Régénération périodique du signal sur une longue distance.

5. Canal de transmission :

Le canal de transmission représente la liaison entre l'émetteur et le récepteur et peut être de différentes natures selon le type de données qu'il permet de véhiculer. Le canal de transmission est caractérisé par sa capacité et sa bande passante.

C'est le support physique dans lequel l'information qu'on désire transmettre peut être acheminée jusqu'au récepteur, l'inconvénient major de ce canal c'est le bruit qu'il soit additif, blanc, gaussien …..Etc. car il introduit toujours des modifications qui peuvent dégrader la qualité du système de communication. Selon la nature du canal, les signaux sont de nature différente :

- Atmosphère : onde électromagnétique
- Câble coaxial : signaux électrique (tensions, courant)
- Fibre optique : ondes électromagnétiques optique (lumière Visible infrarouge)

Les canaux de transmission peuvent être classés selon l'effet qu'ils ont sur le signal on distingue:

- Canal à bruit additif blanc (figure I.2)
- Canal à évanouissement

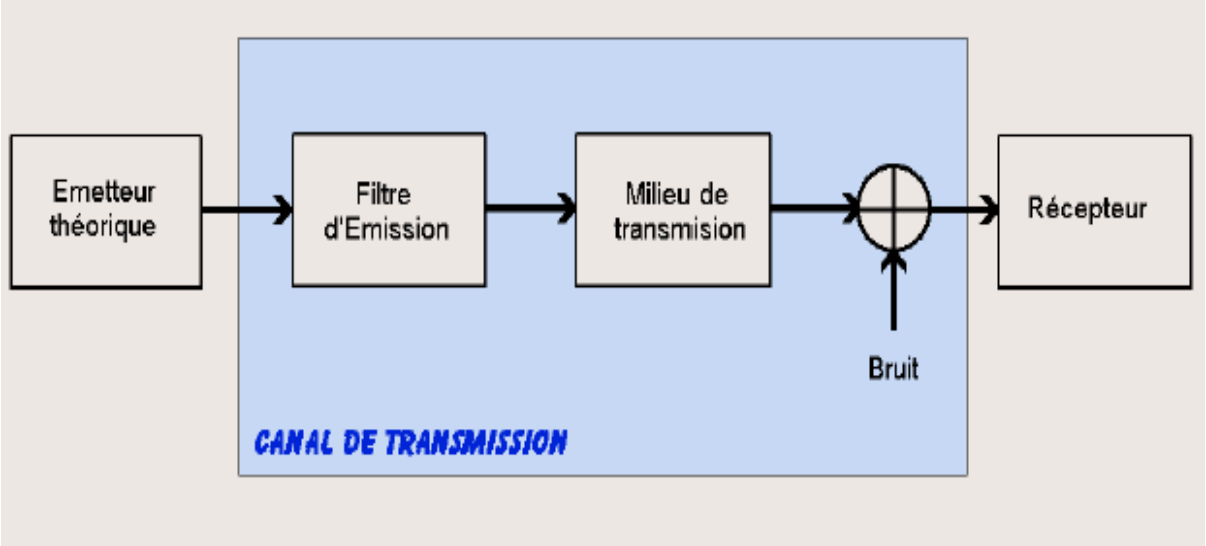


Figure I.2 : Le canal de transmission

1.2.2 Réception

1. **Démodulateur :**

Permet de récupérer chaque symbole émis à partir de chaque signal modulé reçu, Le démodulateur fournit au bloc décodeur une séquence binaire qui représente l'information émise à laquelle est superposée une séquence d'erreur

2. **Synchronisation:**

Récupère la fréquence et parfois la phase de la porteuse, ainsi que l'horloge des symboles, et dans certains cas une synchronisation trame

3. **Décodage de canal:**

Le décodeur de canal, qui connaît la loi de codage utilisée à l'émission, Vient vérifier si cette loi est toujours respectée en réception. Si ce n'est pas le cas, il détecte la présence d'erreurs de transmission qu'il peut corriger sous certaines conditions. Donc l'objectif d'un codeur de canal est d'établir un système de contrôle des erreurs par un nouveau codage du message. Une chose très importante il faut dire que Le codage de canal n'est possible que si le débit de la source binaire est inférieur à la capacité du canal de transmission. [1] Pour le décodage de canal en fait le processus inverse du codage via plusieurs algorithmes.

Le décodeur canal peut s'il détecte la présence d'erreurs demander la retransmission des données erronées, ou corriger les erreurs si la capacité du code n'est pas dépassée.

4. **Décodage de source:**

Décomprime les données pour régénérer les symboles originaux.

5. **Message ou destinataire :**

Représente l'information restituée.

1.3 Codage :

Dans une chaîne de transmission de l'information moderne, le signal analogique associé au message initial est souvent **converti en données numériques** (encodage). Le signal numérique ne présente pas les défauts de l'analogique. Il est certes altéré durant sa transmission, mais peut être **remis en forme**, en principe **sans perte d'information**. Il est d'autre part facile à traiter. Mais, en fin de chaîne, le signal numérique est reconverti en signal analogique pour être restitué en tant que grandeur physique perceptible (onde sonore…).

1.3.1 Codage source

Le codage source consiste à la numérisation du message de la source d'information. Il peut perdre ou ne pas perdre des informations.

La numérisation d'un signal se décompose en trois opération successives, l'échantillonnage, la quantification et enfin le codage binaire.

a. Echantillonnage : une opération effectuée sur le signal à transmettre en vue de réaliser la conversion « analogique/numérique ». Il consiste à substituer, au signal d'origine, une suite des valeurs instantanées prélevées sur le signal et régulièrement espacées dans le temps à des instants précis, régulièrement espacés. (figure I.3)
b. Quantification: pour reconstituer le signal à la réception, il n'est pas indispensable de transmettre directement ces impulsions, il suffit de transmettre une information caractérisant l'amplitude de chacune d'entre elles. Cette opération consiste à faire correspondre à chaque amplitude d'échantillon, l'amplitude la plus voisine d'une suite discrète «étalons» appelée «Niveaux ».
c. Codage binaire : Chaque niveau de l'échelle de quantification est représenté par un nombre binaire.

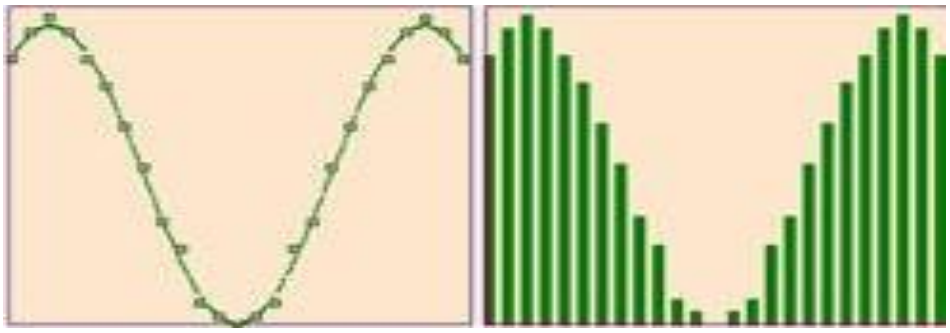


Figure I.3 : Signal échantillonné et quantifié

1.3.2 Codage canal :

Le codage canal, ou encore appelé code correcteur d'erreurs, consiste en une protection des messages binaires fournis par le codage de source par l'introduction d'une redondance d'information (figure I.4). On ajoute aux bits originaux des bits qui dépendent de ceux-ci. Cette redondance peut permettre la détection d'erreurs et éventuellement la correction d'erreurs [2].

Exemple :

Le bit de **parité** (paire ou impaire).

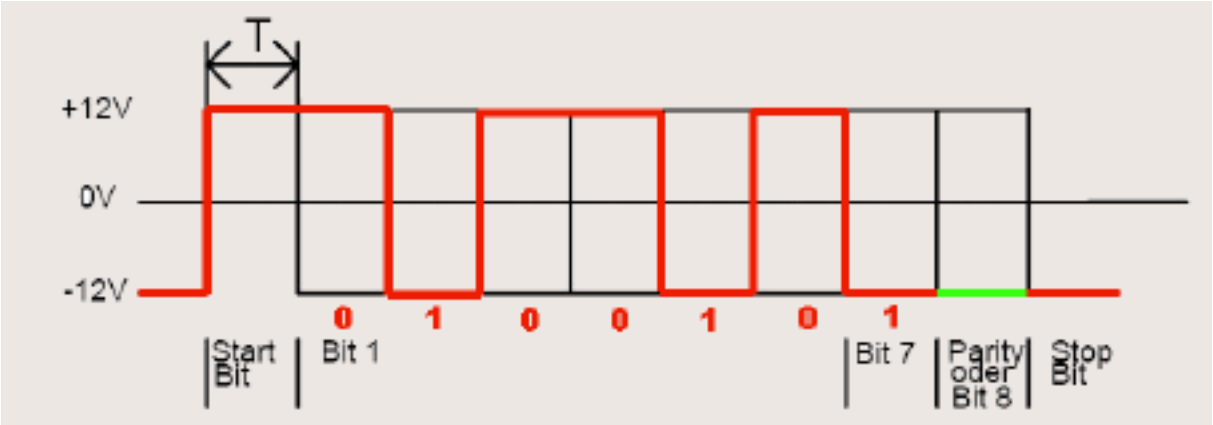


Figure I.4 : Exemple sur le bit de parité

Cause des erreurs de transmission :

Les causes d'erreur sont nombreuses et dépendent principalement de:

- Lignes de transmission utilisées.
- Type démodulation et de codage utilisé.
- Bruit thermique dû aux composants électroniques qui peut aussi provoquer

des erreurs si son niveau devient quantifiable.

- Le bruit d'impulsions qui est une source importante d'erreur, car une impulsion qui dure une dizaine de millisecondes peut induire plusieurs bits en erreur.

Méthode de correction des erreurs de transmission :

Ces bruits produisent un grand nombre d'erreurs groupées et pour cela Des systèmes de détection et de correction d'erreurs ont été développés pour protéger l'intégrité de l'information binaire émise. Ces systèmes sont basés sur un codage supplémentaire des informations transmises et une analyse des informations reçues.

Il existe deux stratégies au cas où le récepteur détecte une erreur (figure I.5):

- Soit une demande de réémission des bits erronés: c'est la stratégie ARQ.
- Soit par décodage de canal pour la correction, on parle de FEC.

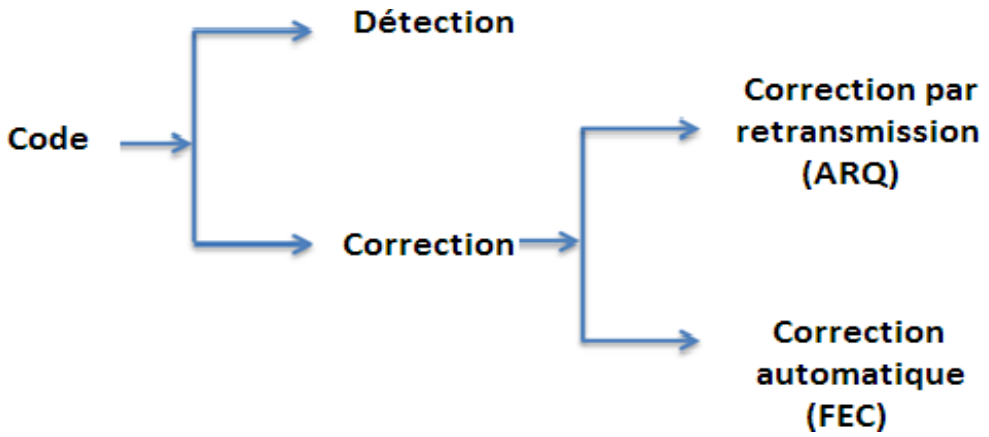


Figure I.5 : Méthode de correction d'erreurs

1.4 Modulation :

La transmission qui modifie le spectre de fréquence du signal à transmettre à l'avance est appelée transmission transbande ou modulation. Elle utilise généralement deux signaux :

- Le message analogique ou numérique, appelé signal modulant ou message (BF).
- Un signal de porteuse

La modulation peut être:

- Soit une transposition plus ou moins directe du spectre du message vers les HF (modulation d'amplitude, de fréquence).
- Soit une modification radicale du signal lui-même en utilisant des moyens

numériques, notamment l'échantillonnage (modulation par impulsions).

- Soit une combinaison des deux techniques précédentes (Wide Band Code Division Multiple Access-W-CDMA).

On peut citer les différentes modulations

- Modulation par saut (Shift Keying Modulation).
- Modulation par impulsion et codage MIC.
- Modulation d'amplitude en quadrature (QAM)

Remarque :

Dans notre projet nous avons utilisé la modulation d'amplitude en quadrature QAM que nous allons détailler dans le chapitre numéro 3.

1.5 Canal de transmission :

1.5.1 Définition

Avant toute conception d'une chaine de transmission, et notamment la sélection de la forme d'onde, la nature ainsi que les propriétés du canal utilisé doivent être étudiées. Puissance du bruit, type et stationnarité du canal, sont des paramètres dont la connaissance a priori est primordiale pour un choix efficace de la forme d'onde. Cette connaissance permet ensuite d'évaluer la capacité du canal sachant la forme d'onde adoptée. D'un point de vue operateur, les informations relatives aux conditions de propagation sont essentielles pour une première évaluation de la capacité du système ainsi que la qualité et la nature du service qu'il pourra proposer.

Les sources de perturbations sont diverses et dépendent essentiellement du milieu où se trouve le canal de transmission. Les principaux types de bruits sont : les bruits galactiques entre 20 MHz et 200 MHz dus aux rayonnements des différentes sources d'énergie de l'espace ; les bruits atmosphériques jusqu'à 20 MHz induit par les éclairs orageux, le bruit industriel, le bruit urbain, les microcoupures correspondant à de courtes interruptions du signal, les sauts de phase et scintillements liés à des variations brusques de phase ou lentes causées par les alimentations électriques ; la diaphonie lors de l'acheminement de plusieurs liaisons par un même câble. [3]

1.5.2 Capacité d'un canal numérique bruité

Une formule précise la capacité du canal de transmission pour un signal numérique traversant une ligne réelle donc bruitée :

$$D = B.log_2(1 + \frac{S}{N}) \quad (1.1)$$

Où :

D : Débit binaire maximal (bit/s)

B : Bande passante (Hz)

S/N : Rapport Signal/Bruit (W/W)

Il existe plusieurs modèles théoriques de canal de transmission en fonction des types d'erreurs les plus fréquents:

1.5.3 Canal binaire symétrique

Le modèle le plus simple est le canal binaire symétrique (figure I.6) appelé BSC (Binary Symmetric Channel). Un BSC est défini par sa probabilité d'erreur, notée P. La valeur de cette probabilité qui dépend du canal et de la modulation correspond au TEB obtenu en sortie du démodulateur. Si l'on note *c* et *y* les éléments en entrée et en sortie du BSC, alors la probabilité pour que le symbole reçu soit erroné sera égale à P équation (1.2) et inversement la probabilité pour que le symbole reçu soit correcte sera de 1-P équation (1.3)

$$P_r(y=0,c=1)=P_r(y=1,c=0)=P \quad (1.2)$$

$$P_r(y=0,c=0)=P_r(y=1,c=1)=1-P \quad (1.3)$$

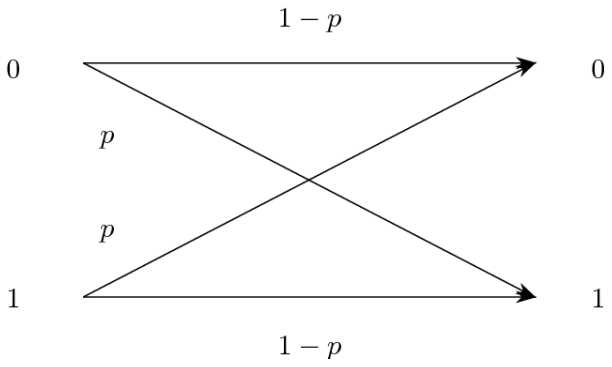


Figure I.6 : Canal binaire symétrique

1.5.4 Canal AWGN

Un canal de transmission à bruit additif gaussien blanc AWGN (Additive White Gaussian noise) est représenté sur la figure I.7. Il est constitué par l'addition d'un bruit gaussien blanc.

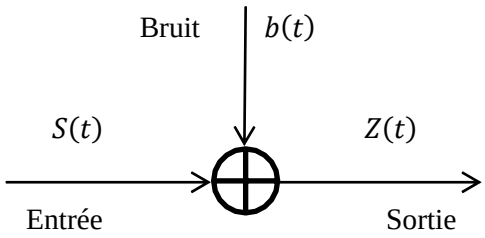


Figure I.7 : Le canal à bruit additif blanc gaussien AWGN

1.6 Modes d'exploitation d'un support de transmission:

Pour communiquer les informations entre l'émetteur et le récepteur il existe différentes possibilités pour le sens de transmission [5]:

1.6.1 Mode simplex :

Dans ce mode, une extrémité émet et l'autre extrémité reçoit (transmission unidirectionnelle).

Cette transmission est utilisée pour la diffusion télévisée.

Ce mode présente l'inconvénient de ne pas savoir si tout a été reçu par le destinataire sans erreur. (figure I.8)

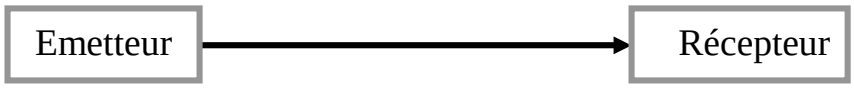


Figure I.8: Mode simplex

1.6.2 Mode semi duplex (half duplex) :

Ce mode permet une transmission dans les deux sens (transmission bidirectionnelle). (figure I.9). Alternativement chacune des deux extrémités reçoit et émet à tour de rôle, par exemple la conversation par talkie /walkie, l'émetteur est à l'écoute et il doit couper l'écoute s'il désire parler. Il est nécessaire de disposer d'un transmetteur aux deux extrémisées.

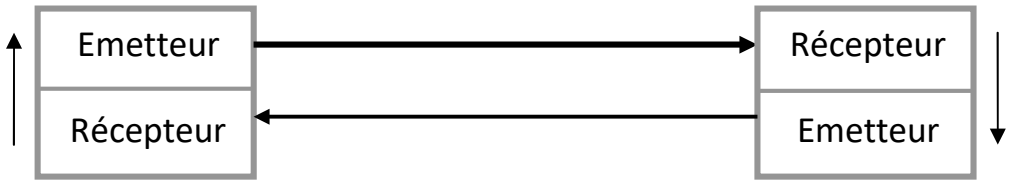


Figure I.9 : Mode semi duplex

1.6.3 Mode duplex (full duplex):

Il permet une transmission dans les deux sens au même temps, comme si deux interlocuteurs parlaient simultanément, on supposant que chacun entend et parle au même temps à titre d'exemple le téléphone. (figure I.10)

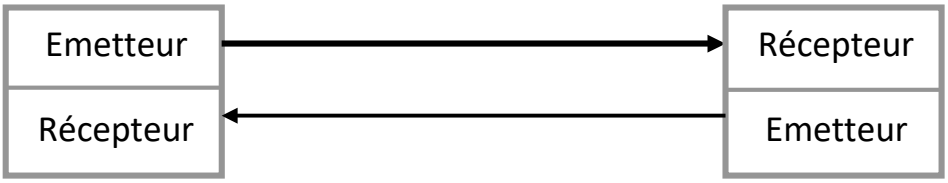


Figure I.10 : Mode duplex

1.7 Les différents types du support de transmission:

Les supports physiques de transmissions sont les éléments permettant de faire circuler les informations entre les équipements de transmission. On classe généralement ces supports en trois catégories, selon leurs constitutions physiques:

Les supports filaires : permettent de faire circuler une grandeur électrique sur un câble généralement métallique, par exemple câble coaxial, ligne bifilaire parallèle ou torsadé.

Les supports aériens : désignent l'air ou le Vide, ils permettent la circulation d'ondes électromagnétiques d'un point à l'autre par exemple les faisceaux hertzien set la transmission par satellite.

Les supports optiques: permettent d'acheminer des informations sous forme lumineuse par exemple la fibre optique.

1.8 Conclusion :

Nous avons abordé dans ce chapitre les fondements théoriques qui régissent la transmission numérique des informations [6]**.** En présentant les bases théoriques qui permettent de décrire l'ensemble des fonctions concernées par notre étude [7]. Ensuite on a présenté les notions fondamentales du codage correcteur d'erreurs et des modulations numériques car c'est l'association de ces deux fonctions qui permet de concevoir des systèmes à grande efficacité spectrale présentant de bonnes performances Vis-à-vis du bruit. Une description des modèles de canal de transmission utilisés dans l'étude a également été donnée.

2. Chapitre 2 : Transmission sécurise

2.1 Introduction :

La cryptographie est une technique de protection des messages assurant confidentialité, authenticité et intégrité. Si un message est intercepté, il ne sera pas compris ni facilement décrypté.

La cryptographie été utilisé pour assurer les communications militaires et diplomatiques. Depuis, elle n'a fait qu'évoluer. Si au début il s'agissait de chiffrement symétrique, c'est-à-dire une même clé sert à crypter et décrypter les messages, alors que au milieu des années 70 un nouveau partage de messages chiffrés révolutionnaire est apparu avec la clé public : le chiffrement asymétrique. Actuellement, ces deux modes de chiffrement sont utilisés ensemble on parle alors de cryptographie hybride.

Dans ce chapitre on a défini ce que c'est la cryptographie. Ensuite, on présentera quelques algorithmes symétriques et asymétriques, ainsi que leur implémentation.

2.2 La cryptographie:

1. Définition :

La cryptographie concerne la transformation d'un message (texte, image, chiffres) clair vers un message codé, incompréhensible à tous sauf pour les détenteurs de la clé de chiffrement. C'est une discipline qui étudie les méthodes pour assurer le secret et l'authenticité des messages. Le terme « cryptographie » Vient du grec « kriptos » (caché) et « graphein » (écrite). [8]

2.2.1 Objectifs de la cryptographie :

Cette utilisation de la cryptographie est d'autant plus importante aujourd'hui que les communications Internet circulent dans des infrastructures où la fiabilité et la confidentialité ne peuvent être garanties. Les principaux services offerts par la cryptographie moderne sont :

- **Confidentialité** : assurer que les données concernées ne pourront être dévoilées que par les personnes autorisées.
- **Intégrité** : assurer que les données ne seront pas altérées pendant leur transmission ou leur stockage.
- **Authentification/Identification** : prouver l'origine d'une donnée ou s'assurer de l'identité d'une personne.
- **Non-répudiation** : garantir que les actions ne seront pas reniées. [9]

2.2.2 Histoire de la cryptographie

Les humains ont toujours besoin de cacher des informations. Que ce soit un secret qui ne devrait pas être divulgué dans son entourage, cela nuira aux individus ou même aux tactiques dans les différentes batailles et guerres qui ont marqué l'histoire.

Cacher des informations est toujours une nécessité.

Voici une liste non exhaustive des différentes techniques utilisées au cours des siècles qui ont marqué l'évolution de la cryptographie à diverses époques.

Les premières traces de cryptographie remontent à l'Antiquité, en particulier vers le XVIème siècle avant J.-C.Un potier irakien a sculpté sur une table d'argile sa recette en supprimant les consonnes et en en modifiant l'orthographe des mots.

Par la suite, entre le Xème et le VIIème siècle avant J.-C., les Grecs utilisaient des scytales (figure II.1), des sortes de bâtons en bois. Lorsque l'expéditeur veut communiquer, il roule une bande de scytale et écrit un message dessus (une lettre par morceau de bande).

Une fois la bande déroulée, les lettres sont brouillées, elles n'ont donc aucun sens. La seule façon de comprendre ce message est d'enrouler la bande sur une scytale même diamètre pour que les lettres puissent être disposées correctement. [10][11][12]

Figure II.1: Scytale

Au 1er siècle avant J.-C, le cryptage de César est apparu. Ce cryptage a été utilisé par Jules César pour sécuriser les communications. C'était l'un des premiers chiffrements par substitution. Son principe est très simple, il suffit de remplacer chaque caractères du message original avec une lettre de l'alphabet, toujours trouver à une distance fixe. [13]

Au XVIème siècle, le chiffrement Vigenere est apparu. C'est aussi un chiffrement par substitution, mais plus avancé que celui de César. Au lieu d'utiliser un décalage fixe, le chiffrement est basé sur une clé qui détermine le décalage de chaque caractère. [14]

Après la Première Guerre mondiale, la machine Enigma est créée (figure II.2), les allemands se rendent compte de l'importance des informations sensibles et investissent dans une version militaire plus complexe de la machine. Cependant, malgré le fonctionnement de la machine, des chercheurs polonais ont étudié le fonctionnement de la machine pour tenter de déchiffrer les messages.

Par la suite, le célèbre mathématicien et informaticien Alan Turing a collaboré pour déchiffrer les messages cryptés par machine.

Pour cette raison, les Britanniques ont pu décrypter les informations, ce qui était un avantage important qui leur a permis de gagner la guerre. [15]

Figure II.2 : La machine Enigma

Dans les années 70, le développement de l'informatique et l'émergence des réseaux de communications modifient la situation. La sécurité des nouveaux moyens de communications doit être assurée. C'est pourquoi, en 1975, le Bureau Américain des Standards propose de

normaliser un système de chiffrement : le DES (Data Encryption Standard) qui est un système de chiffrement par blocs de 64 bits basée sur l'utilisation d'une clé secrète identique pour le chiffrement et le déchiffrement dont la taille est de 56 bits.

La principale difficulté de cet algorithme réside dans la sécurité de l'échange des clés. Un autre inconvénient est que tout couple d'utilisateurs doit au préalable s'entendre sur une clé commune. La gestion des clés devient vite problématique [16].

Ainsi, le DES 56 bits, qui était l'algorithme le plus utilisé pour les échanges transactionnels sur les réseaux étendus, a été remplacé par le nouvel algorithme AES (Advanced Encryption Standard) qui a des clés de longueur plus importante (128, 192 et 256 bits) ainsi que des blocs de taille plus grande (128 bits contre 64 pour DES).

Parallèlement en 1976, W. Diffie et M. E. Hellman publient leur célèbre papier « New Directions in Cryptography ». Ils y décrivent les fondements de la cryptographie asymétrique moderne permettant de résoudre en partie les problèmes d'échange des clés secrètes. Ce type de crypto système utilise une clé secrète pour le déchiffrement, alors que c'est une clé publique qui est employée pour chiffrer le message.

La première application pratique de la cryptographie asymétrique est le système **RSA** proposée en 1978 par R.L. Rivest, A. Shamir et L. Adleman. Ce système est d'ailleurs le crypto système asymétrique le plus répandu à l'heure actuelle.

Aujourd'hui, la cryptographie ne se restreint plus au simple chiffrement des messages pour en garantir la confidentialité et elle n'est plus réservée aux diplomates et militaires : aujourd'hui, des centaines de millions d'individus, à travers le monde, ont en permanence sur eux un ou plusieurs processeurs cryptographiques, pour leur téléphone mobile ou leur carte bancaire en particulier.
Dans la cryptographie moderne toute la sécurité est basée sur la clé (ou les clés), et non dans les détails des algorithmes. Cela signifie qu'un algorithme peut être publié et analysé, mais la clé doit être protégée.

2.3 Différents types de cryptographie

Les techniques cryptographiques se divisent en deux grandes parties :

- La cryptographie à clés secrètes ou cryptographie symétrique.
- La cryptographie à clés publiques ou cryptographie asymétrique.

Ils ont tous deux leurs avantages et leurs inconvénients. La différence qui existe entre ces deux types se situe au niveau de la clé.

2.3.1 Cryptographie symétrique

La cryptographie symétrique est la forme la plus ancienne de cryptographie [16]. Ce chiffrement fonctionne en principe avec une clé secrète, qui est utilisé pour crypter et décrypter les données. L'expéditeur et le destinataire ont des copies identiques de la clé (figure II.3).

Dans le cas des chiffrements symétrique le principe est le suivant :

- L'expéditeur utilise une clé de chiffrement (habituellement une chaîne de lettres et de chiffres) pour chiffrer son message.
- Le message crypté, appelé crypto-texte, ressemble à des lettres brouillées et ne peut être lu par quiconque le long du chemin.
- Le destinataire utilise la même clé de décryptage pour transformer le texte chiffré en texte lisible.

L'émetteur et le destinataire doivent échanger la clé de façon sécurisée. Le système de cryptographie à clé symétrique le plus populaire est le Data Encryptions System (DES).

Figure II.3 : Schéma de fonctionnement de la cryptographie symétrique

2.3.2 Avantages et inconvénients de cryptographie symétrique :

Avantages :

- Le chiffrement/déchiffrement est très rapide.
- Les algorithmes de chiffrement symétrique sont généralement beaucoup moins complexes que les algorithmes de chiffrement asymétrique

Inconvénients :

- Le chiffrement symétrique ne garantit que la confidentialité des données, une seule clé pose un problème: Communiquer la clé en tout sécurité avec la personne avec qui on souhaite dialoguer.
- Il est nécessaire d'assurer la confidentialité de cette clé. [17]

2.3.3 Méthodes de chiffrement

2.3.3.1 Chiffrement par flot

Les algorithmes basés sur le principe du chiffrement par flot peuvent instantanément crypter ou décrypter les messages. Leur fonctionnement est basé sur un générateur de nombres pseudo-aléatoires et un mécanisme de remplacement bit à bit. Comme nous le savons tous, l'algorithme basé sur ce principe est très rapide. [16]

2.3.3.2 Chiffrement par blocs

Les chiffrements par blocs fonctionnent différemment. Les messages ne sont pas remplacés bit a bit, mais sont découpés en blocs (la taille du bloc dépend de la clé). Ensuite, chaque bloc est chiffré par la clé, par une permutation, une opération XOR ou d'autres types de traitement sont appliqués à chaque bloc. [16]

2.3.4 Algorithmes

2.3.4.1 DES

Le cryptage DES a été publié en 1977, Par conséquent, le premier algorithme de cryptage à petite clé privé (56 bits) à avoir été rendu public.

Le message à chiffrer est divisé en Blocs de 64 bits, chaque bloc est divisé en deux sous-blocs de 32 bits.

DES est un algorithme symétrique, combinant transpositions et substitutions :

- La transposition est le fait de déplacer des éléments du fichier clair (plain text) dans le fichier crypté (cyphertext). Nous rencontrerons aussi le terme permutation au lieu de transposition.
- La substitution est la transformation d'un élément du fichier clair en un autre élément dans le fichier chiffré. Les substitutions non linéaires permettent de compliquer la liaison entre le fichier crypté et les clés secrètes.

2.3.4.2 AES

L'algorithme AES est la norme cryptographique actuelle. Il est actuellement impossible de déchiffrer à moins d'utiliser la méthode brute force. Une clé de 128 bits est utilisée pour la norme AES. À l'origine, le cryptage de Rijndael prévoyait également des clés 192 et 256 bits. Différentes tailles de clé ne modifient pas l'algorithme déchiffrement. Le tableau 2 montre le nombre d'itérations effectuées. Ce nombre dépend du nombre de colonnes contenues dans la matrice contenant la clé ainsi que du nombre de ses lignes. Ainsi, dans AES 128 bits, le nombre de tours de boucle sera égal à Nr - 1. Son fonctionnement se déroule en plusieurs étapes. (Généralement appelés « rounds »).

	Nk	Nb	Nr
128	4	4	10
192	6	4	12
256	8	4	14

Tableau II.1 : Tableau du nombre d'itérations par rapport à la clé

Le round initial permet d'effectuer l'opération initiale principale de clé. Puis les quatre opérations sont répétées neuf fois.

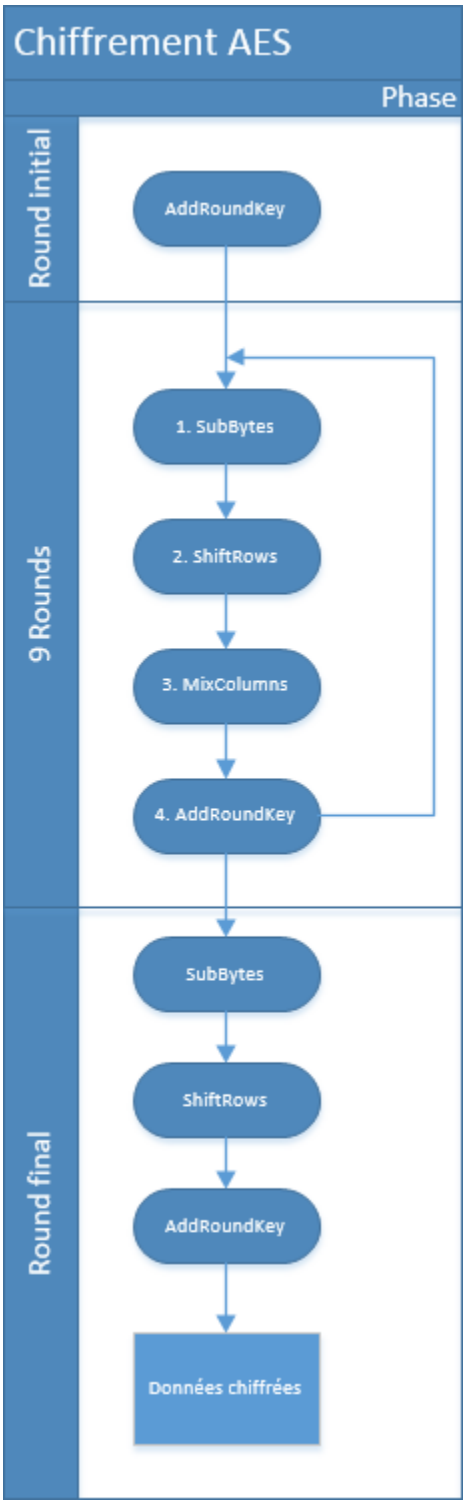


Figure II.4: Schéma de fonctionnement d'AES

2.4 Cryptographie asymétrique

Un système de chiffrement est dit asymétrique si la clé utilisée lors du chiffrement est différente de celle utilisée lors du déchiffrement. Un tel système est aussi qualifié de système de chiffrement à clé publique. Ce principe a été imaginé par Diffie et Hellman en 1976. Le premier algorithme le mettant en œuvre est du à Rivest, Shamir et Adleman en 1977, et porte leurs noms : R.S.A. L'article de Diffie et Hellman contient les bases théoriques de la cryptographie asymétrique, mais ils n'avaient pas trouvé concrètement d'algorithme de chiffrement répondant à ce principe. Ce fut donc l'œuvre de Rivest, Shamir et Adleman.

Le principe est simple mais très astucieux. Les correspondants ont chacun une clé qu'ils gardent secrète et une clé dite publique qu'ils communiquent à tous (figure II.5). Pour envoyer un message, on le chiffre à l'aide de la clé publique du destinataire. Celui-ci utilisera sa clé secrète pour le déchiffrer. C'est comme si le destinataire mettait à disposition de tous des cadenas ouverts dont lui seul a la clé. Quand on lui écrit, on insère le message dans un coffre que l'on ferme avec un tel cadenas, et on lui adresse le tout. En effet, dans la cryptographie asymétrique, il existe une clé publique et une clé privée.

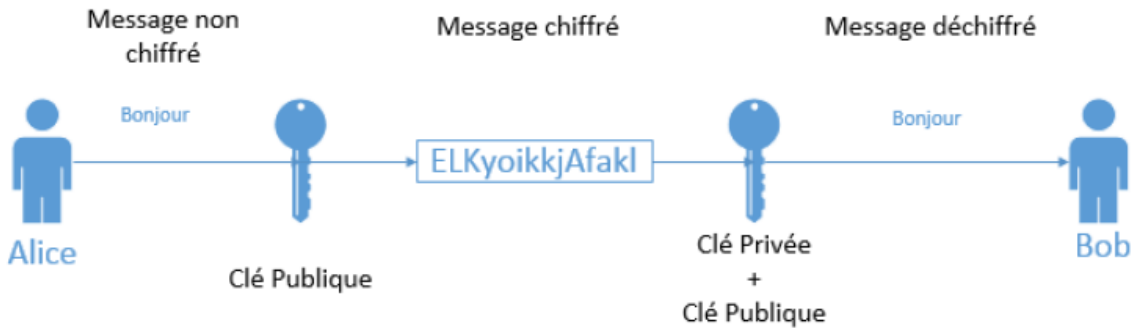


Figure II.5 : Schéma de fonctionnement de la cryptographie asymétrique

2.4.1 Avantages et inconvénients de cryptage asymétrique :

Avantages :

- Pas besoin d'établir un canal pour la transmission de la clé.
- Plusieurs fonctions de sécurité: confidentialité, authentification, et non-répudiation.

Inconvénients:

- Le cryptage asymétrique et dix fois plus long que le cryptage symétrique.
- Problèmes de l'implémentation sur les appareils à faible puissance de calcul.

2.4.2 Algorithmes

2.4.2.1 Diffie-Hellman :

Le protocole Diffie-Hellman a été inventé par les deux cryptologues Diffie et hellman. Leur idée de base est la suivante : si Alice veut partager une clé secrète avec Bob afin de pouvoir envoyer des messages cryptés, c'est facile à faire. Mais si Alice veut partager un message avec dix personnes, cela peut toujours être possible, mais cela nécessite tout de même 45 clés différentes (9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1 clés).

L'algorithme de chiffrement :

1. Alice et Bob choisissent une base **g** et un nombre premier **p**

2. Alice engendre un nombre secret **a** et Bob un nombre secrète **b**.

3. Alice calcul l'élément public Ka puis elle l'envoie à Bob :

$$K_a = g^a \bmod p \quad (1.1)$$

Bob calcul l'élément public Kb puis elle l'envoie à Alice :

$$K_b = g^b \bmod p \quad (1.2)$$

4. Pour obtenir la clé secrète, Alice doit réaliser la fonction suivant :

$$K_{Alice} = ((g^b \bmod p)^a \bmod p) \quad (1.3)$$

Bob réalise la même opération qu'Alice, avec les valeurs qu'il a reçues, pour obtenir la même clé secrète, à savoir :

$$K_{bob} = ((g^a \bmod p)^b \bmod p) \quad (1.4)$$

Exemple : **g** = 37 et **p** = 43.

Alice choisit comme nombre **a** = 6 et envoie à Bob 1 (le résultat de $37^6 \bmod 43$) Bob choisit comme nombre **b** = 11 et envoie donc 7 (le résultat de $37^{11} \bmod 43$).

Maintenant Alice n'a plus qu'à faire l'opération suivante : $(6^7 \bmod 43 = 1)$ et Bob doit faire$(1^{11} \bmod 43 = 1)$. Alice et Bob obtiennent bien sur le résultat 1, qui est à présent leur clé secrète.

Maintenant qu'un échange de clés est effectué, cette clé obtenue, peut être utilisée comme clé pour crypter les données avec un cryptage AES. Evidemment, pour que la clé secrète résultante soit indéchiffrable en un temps raisonnable, il faut utiliser des nombres premiers plus grands que les nombres premiers utilisés dans l'exemple. Idéalement, il faudrait utiliser des nombres premiers avec plusieurs centaines de chiffres.

2.4.2.2 RSA

Le chiffrement RSA a été inventé en 1977 par les mathématiciens Ronald Rivest, Adi Shamir et Leonard Adleman. Les initiales de leur nom ont donné RSA. Même si l'idée de base est la même que celle de Diffie-Hellman, (échanger une clé avec un grand nombre de personnes), son fonctionnement est différent bien qu'il soit basé sur la difficulté à factoriser de très grands nombres premiers. Il est massivement utilisé à travers le monde. En effet, c'est entre autres le chiffrement utilisé lors de connexions sécurisées sur un navigateur Web. Avec tous les utilisateurs du réseau Internet, il serait inimaginable d'utiliser un chiffrement symétrique. C'est pour cette raison que la clé privée est calculée avec RSA. Comme les algorithmes asymétriques sont plus lents que les symétriques, RSA ne calcule que la clé qui servira à chiffrer les données avec un chiffrement symétrique tel qu'AES.

L'algorithme de chiffrement

Départ :

Il génère facilement de grands nombres premiers p et q (+- 100 chiffres)

Etant donné un nombre entier n = p*q, il est très difficile de retrouver les facteurs p et q.

La Création des clés :

- La clé secrète : 2 grands nombres premiers p et q
- La clé publique : n = p*q
- $\varphi = (p-1)(q-1)$
- Un entier e, sachant que $1<e<\varphi$

Chiffrement :

Le chiffrement d'un message M en un message crypté C est effectué par la transformation suivante :

$$C = M^e \bmod n \quad (1.5)$$

Déchiffrement :

Il s'agit de calculer la fonction réciproque suivante :

$$M = C^d \bmod n, \text{ tel que } D = e^{-1} \bmod \varphi \quad (1.6)$$

Exemple : chiffrer le mot BONJOUR

1. Alice crée ses clés :

- La clé secrète : **p = 53, q = 97** (Note : en réalité, p et q devraient comporter plus de100 chiffres)
- La clé publique : **e = 7 (premier avec 52*96), n = 53*97 = 5141**

2. Alice diffuse sa clé publique.

3. Lorsque Bob trouve le couple (n, e), il sait qu'il l'utilise pour crypter ses messages.
Tout d'abord, il remplacera chaque lettre du mot BONJOUR par le numéro correspondant à sa position dans l'alphabet.

B = 2, O = 15, N = 14, J = 10, U = 21, R = 18
BONJOUR = 2 15 14 10 15 21 18

4. Bob découpe ensuite son message chiffré en blocs de même longueur, chacun représentant un nombre inférieur à n Cette opération est nécessaire, car si nous ne faisons pas le bloc assez longs, nous tomberons dans un simple chiffre que nous pouvons attaquer avec une analyse de fréquence.
BONJOUR = 002 151 410 152 118

5. Bob crypte chaque bloc que l'on note **B** par la transformation $C = B^e \bmod n$ (où C est le bloc chiffré) :

$C_1 = 2^7 \bmod 5141 = 128$

$C_2 = 151^7 \bmod 5141 = 800$

$C_3 = 410^7 \bmod 5141 = 3761$

$C_4 = 152^7 \bmod 5141 = 660$

$C_5 = 118^7 \bmod 5141 = 204$

Donc, nous obtenons un message crypté C : 128 800 3761 660 204.

2.5 Conclusion

Dans ce chapitre, nous avons présenté une introduction à la cryptographie où les différents types de cryptographie ont été exposés avec leurs avantages et inconvénients. Une conclusion est faite que les protocoles cryptographiques à clé publique présentent l'avantage d'échanger des messages de manière sûre sans échange préalable de secret et les protocoles symétriques sont rapides.

3. Chapitre 3 : La modulation en quadrature (QAM)

3.1 Introduction

Les signaux actuels sont souvent de type numérique ‘data’. Il peut s'agir à l’origine de signaux audio ou Vidéo analogique numérisées ou de données numériques générées par des ordinateurs. Dans tous les cas la porteuse de ces signaux est analogique sinusoïdale. La modulation considérées dans ce chapitre c’est Modulation m-QAM ou modulation d'amplitude en quadrature à m-nivaux.

L’utilisation de la modulation d’amplitude en quadrature M-QAM à m niveaux devient de plus en plus courante dans les systèmes de transmission. Grace à ses M bits par symbole numérique (M bits/symbole), elle fournit l'efficacité de bande passante la plus élevée disponible dans les signaux numériques d’aujourd'hui. Les espérances sont que M-QAM évoluera pour devenir un format dominant de modulation numérique.

3.2 Les performances d’un canal

Pour quantifier les performances d'un canal utilisant la modulation numérique, il est nécessaire de connaître la définition des paramètres suivants :

a. La rapidité de modulation *R* se définit comme étant le nombre de changements d'états par seconde d'un ou de plusieurs paramètres modifiés simultanément.

   La rapidité de modulation $\mathrm{R} = \frac{1}{\mathrm{T}}$ s’exprime en bauds.

b. Le débit binaire *D* se définit comme étant le nombre de bits transmis par seconde. Il sera égal ou supérieur à la rapidité de modulation selon qu'un changement d'état représentera un bit ou un groupement de bits. Le débit binaire $D = \frac{1}{T_b}$s'exprime en "bits par seconde". Pour un alphabet M-aire, on a la relation fondamentale $T = n.T_b$soit $D = n.R$ Il y a égalité entre débit de sourceet rapidité de modulation uniquement dans le cas d'une source binaire (alphabet binaire).

c. Taux d'erreur bit ou BER 'Bit Error Rate' : Le problème ici est différent de celui de la transmission des signaux analogiques. Lors de la transmission de signaux analogiques, on cherche à avoir le meilleur rapport S/B à la réception pour pouvoir reconstituer le signal analogique émis. Dans le cas de la transmission de signaux numériques, il faut reconstituer la séquence binaire émise et donc prendre la bonne décision : est-ce un "1" ou un "0" ? La performance de la chaîne de communication numérique se mesure en taux d’erreurs binaires (nb d’erreurs / nb de bits transmis).

$$\text{BER} = \frac{\text{Nombre de bits faux}}{\text{Nobmre de bit transmis}} \quad (3.1)$$

d. Le rapport $\boldsymbol{\eta = \frac{D}{B}}$ ou η est l'efficacité de l'utilisation de la bande passante Vis-à-vis le débit binaire.

3.3 La modulation QAM

La modulation d'amplitude sur deux porteuses en quadrature est connue par son abréviation anglaise : QAM pour « Quadrature Amplification Modulation ». C'est une modulation dite bidirectionnelle.

La modulation QAM c'est une technique de modulation numérique qui permet une meilleure utilisation du spectre électromagnétique que les autres techniques de modulation numérique comme la ASK (amplitude Shit keying), PSK (Phase shift keying) ou la FSK (frequency shift keying), parce quelle n'envoie pas information comme un flux de bits mais transmet des symboles par deux canaux différents qui sont connu comme le canal I et le canal Q chacun envoie avec une onde sinusoïdale ou cosinusoïdal, et ceci sans rajouter des problèmes d'interférence puisque les deux ondes sont orthogonales.

La modulation QAM peut être QAM4, QAM16, QAM64 dépendant du nombre de bits qui forment le symbole.

La notation générale des axes est :

- I (In phase) pour l'axe représentant l'origine.
- Q (Quadrature) pour l'axe déphasé de 90, en avance par rapport a l'axe I.

le signal modulé m(t)peut s'écrire :

$$\text{m(t)} = a(t).\cos(w_0 t + \varphi_0) - b(t).\sin(w_0 + \varphi_0) \quad (3.2)$$

et les signaux a(t) et b(t) ont pour expression :

$$a(t) = \sum a_k\, g(t - kT)\ et\ b(t) = \sum b_k\, g(t - kT) \quad (3.3)$$

Le signal modulé m(t) est donc la somme de deux porteuses en quadrature, modulée en amplitude par les deux signaux a(t) et b(t).

3.3.1 Propriété de la modulation d'amplitude QAM :

a. L'efficacité spectrale :

On définit l'efficacité spectrale ou débit spécifique par le débit binaire passant dans un hertz de bande. La bande de fréquence occupée étant chiffrée par l'occupation spectrale du canal centré sur la fréquence porteuse fp, site OS canal.

$$D_{spéctrale} = \frac{D_b}{OS_{canal}} \left[\frac{\frac{bits}{sec}}{Hz}\right] \quad (3.4)$$

Pour une même rapidité de modulation$R = \frac{1}{T}$, le débit binaire $D_b = \frac{1}{T_b}$de la M-QAM est multiplie par $n = log_2(M)$ par rapport celui de la 2-QAM. Autrement dit, pour une largeur de bande B donnée, l'efficacité spectrale $\eta = \frac{D}{B}$ est multiplié par $n = log_2$(M).

n	$\mathbf{M = 2^n}$	Modulation	Débit binaire	Efficacité spectrale $\boldsymbol{\eta}$
1	2	2-QAM	D	η
2	4	4-QAM	2-D	2-η
4	16	16-QAM	4-D	4-η
6	64	64-QAM	6-D	6-η
8	128	128-QAM	8-D	8-η

Tableau III.1 : Le gain en débit binaire et en efficacité spectrale.

Le tableau ci-dessus montre le gain obtenu sur le débit binaire et sur l'efficacité spectrale pour différentes modulations MAQ-M, ceci pour une même rapidité de modulation. L'intérêt d'augmenter *M*, même au prix d'une complexité accrue, est évident

b. Densité spectrale de puissance des constellations de QAM :

Pendant que des constellations carrées de QAM peuvent être considérées comme deux modulations indépendantes orthogonales de PAM qui sont transmises simultanément le PSD de la QAM est simplement deux fois les PSD de différentes modulations de PAM.

c. La bande passante :

La bande passante notée B ou BP est la largeur d'intervalle de fréquence, mesurée en hertz, d'une plage de fréquence $f_2 - f_1$ pour laquelle l'atténuation est inferieure à 3dB. (figure III.1)

Figure III.1: La bande passante a -3 dB

Exemple de valeurs de bandes passantes :

- Paire téléphonique (RTC) = 3100 Hz
- Câble coaxiale = 10 Mhz
- Paire torsadée = 100 Mhz
- Fibre optique = quelques GHz

Soit transmettre des données binaire au rythme $f_b \left[\frac{b}{s}\right]$. chaque bit a donc une durée $T_b = 1/f_b$

La bande passante minimale pour transmettre ces données appelée bande de NYQUIST est $(1/2.Tf_b) = (\frac{f_b}{2})$

En effet, le canal se comporte comme un filtre passe-bas qui filtre le signal carré composé de signaux binaires de duréeT_b. Ce signal est composé de plusieurs raies et il faut au minimum que le fondamental de ce signal soit transmis.

La fréquence de ce fondamental est $(1/2.f_b)(\frac{f_b}{2})$.

3.3.2 Principe de la modulation QAM :

Le schéma synoptique d'un modulateur en quadrature QAM est représenté dans la figure III.2 Les deux chemins à l'additionneur désigne typiquement sous le nom du 'I' (en phase) et du 'Q' (quadrature).

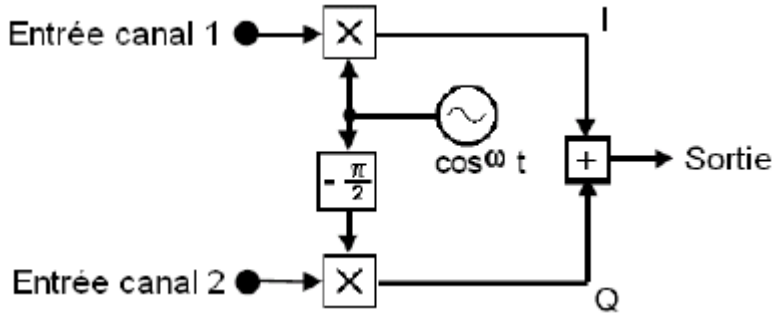


Figure III.2 : Schéma synoptique d'un modulateur

Cette modulation permet de diminuer la largeur spectrale du signal module en utilisant deux ondes porteuses. Cette technique consiste a diviser le signal informatif S(t) en deux signaux $S_1(t)$ et $S_2(t)$modulant deux porteuse $S_{p1}(t)$ et $S_{p2}(t)$de même fréquence et en quadrature de phase :

$$S_{p1}(t) = A.\cos(\omega t + \varphi) \quad (3.5)$$

$$S_{p2}(t) = A.\sin(\omega t + \varphi) \quad (3.6)$$

Les signaux $S_1(t)$ et $S_2(t)$peuvent être constitue en prenant deux composantes de S(t): données paires et impaire, la composante de droite et la composante de gauche d'un signal stéréophonique. Le dédoublement du signal a la sortie du codeur permet de diviser par deux la rapidité de modulation et donc diminuer la largeur spectrale par le même facteur. Par conséquent, on trouve une occupation spectrale du signal module identique a une modulation BLU du signal initial S(t). Ce type de modulation est très utilise dans le domaine de la modulation des signaux numériques.

3.4 Modulation et démodulation QAM

Lorsque le signal m(t) est obtenu par une combinaison de deux porteuse en quadrature modulées en amplitude par des symboles a_k et b_k indépendants, cela simplifie le modulateur et le démodulateur.

En effet, pour le modulateur le train binaire entrant$\{i_k\}$ est facilement divisé en deux trains$\{a_k\}$ et $\{b_k\}$.(figure III.3)

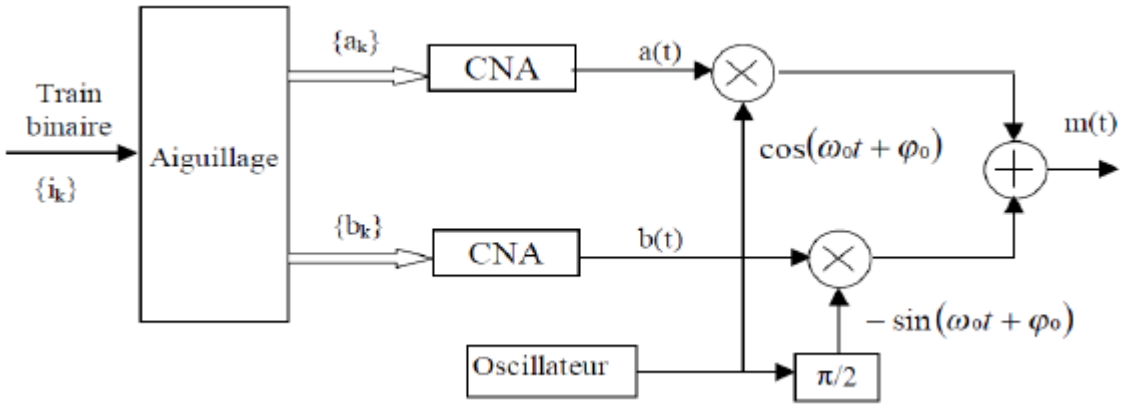


Figure III.3 : Modulateur QAM

La réception d'un signal QAM fait appel a une démodulation cohérente et par conséquent nécessite extraction d'une porteuse synchronisée en phase et en fréquence avec la porteuse à l'émission.

Le signal reçu est démodulé dans deux branches parallèles, sur l'une avec la porteuse en phase et sur l'autre avec la porteuse en quadrature. Les signaux démodulés sont convertis par deux CAN, puis une logique de décodage détermine les symboles et régénère le train de bits reçus.

Le synoptique du démodulateur M-QMA représenté dans la figure III.4 est très voisin de celui propose pour la démodulation MDP (Modulation à Déplacement de Phase).

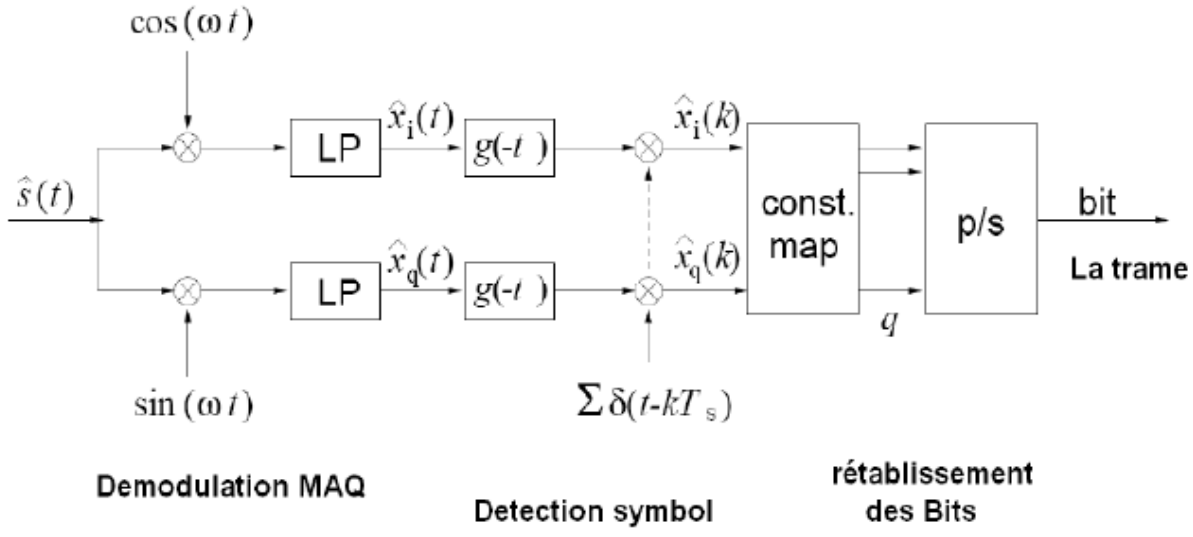


Figure III.4 : Démodulateur QAM

1. Exemple pour k=2 bits par symbole (modulation 4-aire). (figure III.5)

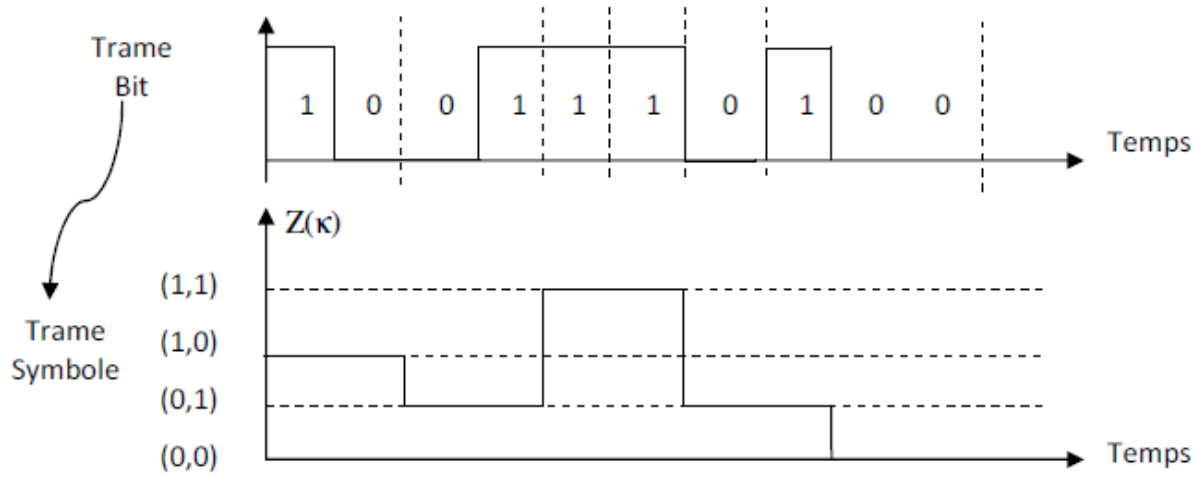


Figure III.5 : Un exemple simple de modulation QAM

2. Exemple de 8QAM ou 8 états.

Un signal modulé QAM avec 3 bits transmis par baud, soit $2^3 = 8$ combinaisons en faisant l'hypothèse de deux amplitudes différentes (voir le tableau ci-dessous et les constellations correspondantes).

Groupe de bits	Amplitude	Déphasage
000	0.5	0
001	1	0
010	0.5	$\pi/2$
011	1	$\pi/2$
100	0.5	π
101	1	π
110	0.5	$3\pi/2$
111	1	$3\pi/2$

Considérons par exemple la séquence suviante : 100 | 001 | 011 | 110.

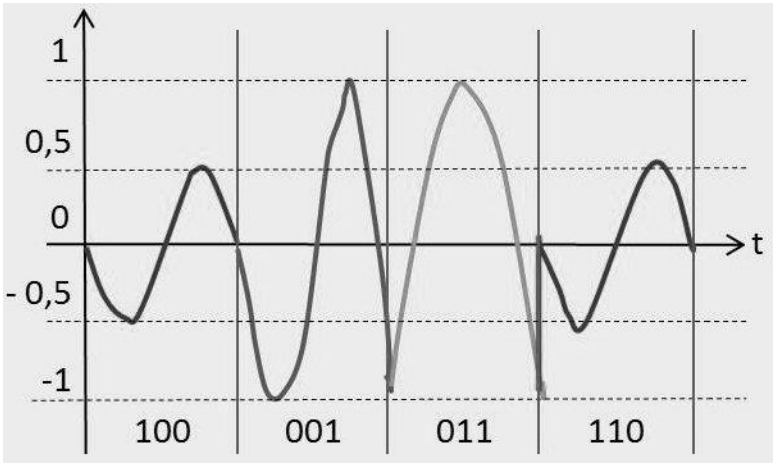


Figure III.6 : Représentation temporelle de la 8-QAM précédent

3.5 Constellation M-QAM :

Les combinaisons possibles en modulations QAM sont souvent représentées par une constellation de points, représentant chacun un groupe de bits. (figure III.7)

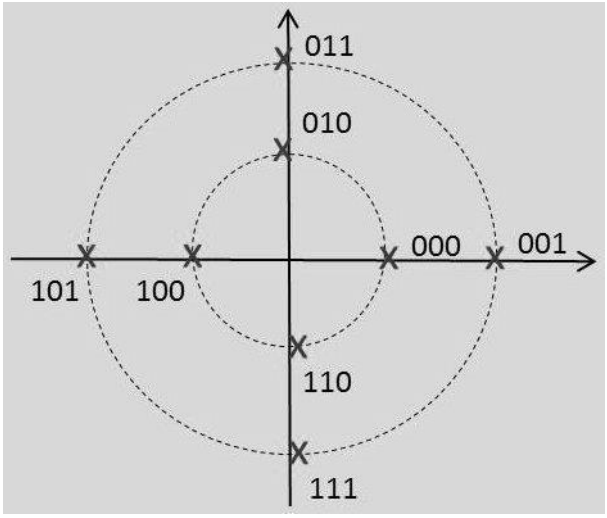


Figure III.7 : constellation associée à une modulation QAM a 8 états (3bits par symbole)

Dans la constellation QAM, l'éloignement de chaque point par rapport à l'origine indique l'amplitude, l'angle et le décalage de phase. Les combinaisons possibles en modulation QAM sont souvent représentées par une constellation de points représentant chacun un groupe de bits, dans notre exemple ci-dessus 3bits par baud.

Dans la pratique, nous augmentons le débit sans augmentation de bande passante, mais au prix d'une relative fragilité du signal. En effet, les points de la constellation étant plus rapproché, ils seront plus difficiles à décoder en cas de bruitage de la ligne.

Une autre façon de représenter la constellation consiste à utiliser un modèle vectoriel, c'est-à-dire un repère polaire, représenté par un module (longueur) et un argument (angle). Comme nous avons ici (figure III.8) deux porteuses en quadrature, nous aurons un point de fonctionnement qui sera défini par un vecteur égal à la somme de deux vecteurs en quadrature.

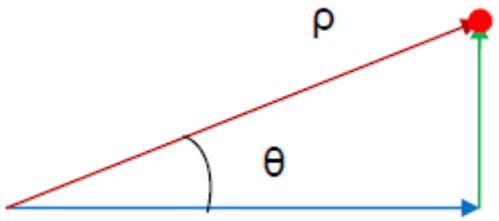


Figure III.8 : Représentation vectorielle d'un point

Les symboles a_k et $b_k$prennent respectivement leurs valeurs dans deux alphabets à M éléments $((A_1, A_2, \ldots . A_M,)$ donnant ainsi naissance a une modulation possédant un nombre$E = M^2$ chaque état est donc présente par un couple $(a_k et b_k)$ ou ce qui revient au même par un symbole complexe $c_k = a_k + jb_k$

Le signal émis pendant un intervalle de durée T peut être défini par les valeurs des deux symboles a_k et $b_k$ou par la valeur de son amplitude et de la phase. On peut donc écrire :

$$m(t) = \sum A_k . g(t - kT)\cos(w_0 t + \psi_k) \qquad (3.7)$$

Avec :

$$A_k = \sqrt{{a_k}^2 + {b_k}^2} \text{ et } \psi_k = A \tan \frac{b_k}{a_k} \qquad (3.8)$$

Cette écriture fait apparaître que la modulation QAM peut être considérée comme une modulation à la fois de phase et d'amplitude.

Par exemple, la MAQ-16 est construite à partir de symboles que prennent leurs valeurs dans l'alphabet $\{\pm d, \pm d3\}$ où d est un constante donnée. On obtient ainsi la constellation suivante pour M=16 et M=64. (figure III.9)

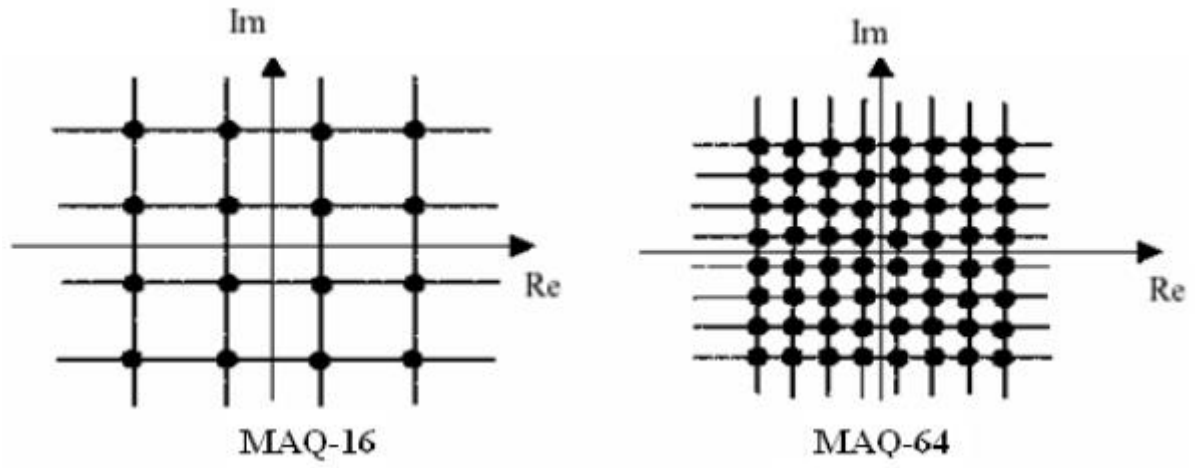


Figure III.9 : Constellation MAQ-16 et MAQ-64

3.6 Avantage de la transmission numérique

L'extraordinaire variété des applications que nous venons d'exposer met en évidence l'importance capitale des différentes techniques de transmission numérique sur onde porteuse. Un intérêt majeur des transmissions numériques réside dans la possibilité de leur insertion harmonieuse dans les réseaux intégrés numériques qui se développent de jour en jour. Un autre avantage réside dans la possibilité de conserver l'intégrité de l'information à transmettre, ce qui est tout à fait impossible avec une transmission analogique. Cependant, la simplicité d'utilisation des modulations analogiques traditionnelles fait qu'elles ne sont pas encore reléguées au musée des techniques désuètes.

Les systèmes modernes de communication numérique sont complexes et requièrent des circuits de modulation et de démodulation de plus en plus sophistiqués. Nous avons examiné un certain nombre de modulations qui sont aujourd'hui utilisées. Il s'avère que le choix d'un type de modulation est toujours déterminé par les contraintes de l'application. Le développement des transmissions numériques s'est appuyé sur les progrès rapides réalisés dans le domaine des circuits intégrés de traitement des signaux. Ainsi, l'utilisation de solutions intégrées devient indispensable au fur et à mesure que le niveau de complexité des systèmes s'accroît et que le prix consenti par le consommateur diminue.

3.7 Conclusion

La modulation QAM c'est une technique dans laquelle l'information est transportée à la fois en amplitude et en phase du signal porteur. Elle est largement utilisée par les modems pour leur permettre d'offrir des débits binaires élevés. Ces porteuses appelées en phase porteuses (I) et porteuses en quadrature (Q). L'ensemble des combinaisons d'amplitudes sont souvent

représentées sur un diagramme en (x, y), est un ensemble de points appelé diagramme de constellation, chaque point représente un groupe de bits.

La modulation d'amplitude en quadrature est un schéma de modulation important avec de nombreuses applications pratiques, y compris les technologies sans fil actuelles et futures. Quelques exemples de systèmes de communication qui utilisent QAM sont le Wi-Fi, les modems câblés, la diffusion Vidéo numérique (DVB) et le WiMax.

4.Chapitre 4 : Implémentation d’une chaîne de transmissions de données cryptées sur logiciel LABVIEW

4.1 Introduction :

Une variété de protocoles de communication implémente la modulation d'amplitude en quadrature (QAM).Les protocoles actuels tels que l'Ethernet sans fil 802.11b (Wi-Fi) et la diffusion Vidéo numérique (DVB), par exemple, utilisent tous les deux la modulation 64-QAM. Aussi, les technologies sans fil émergentes telles que Worldwide Interoperability for Microwave Access (WiMAX), 802.11n et HSDPA/HSUPA (une nouvelle norme de données cellulaires) implémentent également la QAM. Ainsi, la compréhension de la QAM est importante en raison de son utilisation répandue dans les technologies actuelles. Dans ce chapitre une étude sur l'implémentation d'une chaîne de transmissions de données cryptées sera présentée en utilisant le logiciel LabVIEW qui va être présenté dans ce chapitre.

La première partie de cette application permet de chiffrer un message avec le chiffrement AES. Il est possible d'entrer un texte dans la partie Message envoyé, puis on applique un algorithme AES sur le message.

La deuxième partie on implémente une chaine de transmission numérique de données de type QAM (émetteur, canal de transmission, récepteur).On peut aussi voir l'influence de changement des paramètres de modulation (rapport signal sur bruit, l'ordre de modulation M..) sur les performances de transmission numérique QAM. De plus, en observant le diagramme de constellation.

La troisième partie c'est la partie déchiffrage, le déchiffrement devrait retourner le message d'origine et l'afficher sur la partie Message reçu.

4.2 Présentation de logiciel LABVIEW

LabVIEW (Laboratory Virtuel Instrument Engineering Workbench), est un logiciel de développement d'applications d'instrumentation. Développé par la société américaine National Instrument, le logiciel est utilisable dans un grand nombre de domaines, spécialement conçu pour l'acquisition de données et le traitement du signal.

En effet, il offre de nombreuses possibilités de communication avec l'ordinateur et le monde physique, ainsi que des bibliothèques mathématique importantes qui permettent de réaliser des traitements sur les signaux.

Les programmes LabVIEW sont appelés instruments virtuels ou VIs car leur apparence et leurs fonctions sont généralement similaires à celles d'instruments réels, tels que les multimètres et les oscilloscopes. LabVIEW comprend un ensemble d'outils pour collecter, analyser, Visualiser et enregistrer des données, ainsi que des outils pour nous aider à développer des programmes.

Lors de la création d'un nouveau VI, deux fenêtres apparaissent : la fenêtre de face-avant et la fenêtre du diagramme.

4.2.1 Environnement LABVIEW

4.2.1.1 Face-avant

Lorsque vous ouvrez un nouveau VI ou un VI existant, sa face-avant s'affiche. La face-avant est l'interface utilisateur où l'on dessine et on place tous les éléments Virtuels, comme les contrôles d'entrée : bouton, interrupteur, potentiomètre.

La Figure IV.1 montre un exemple de fenêtre de face-avant :

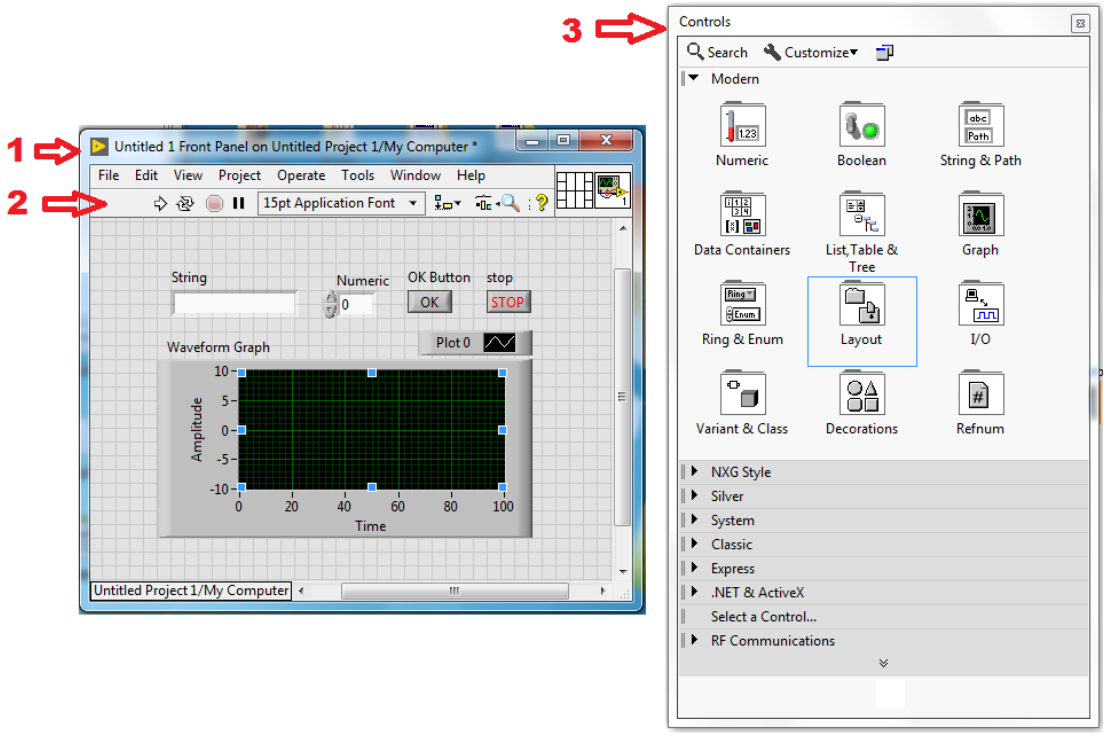


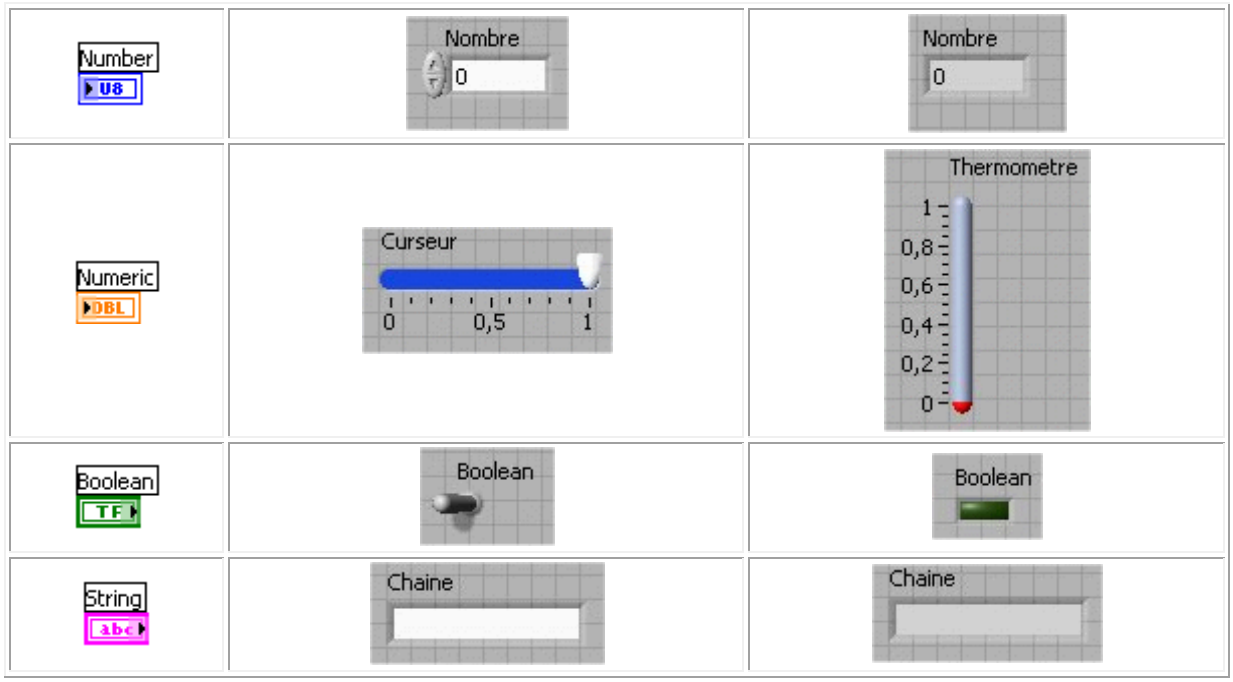
Figure IV.1 : Exemple de face-avant

(1) Fenêtre de la face-avant | (2) Barre d'outils | (3) Palette des commandes

Sur la face avant présentée plus haut, nous avons choisi de disposer 4 terminaux, le premier pour une chaîne de caractère, le second est un nombre de mesures, le troisième c'est un Botton, et le dernier un graphe XY nommé Waveform Graph. Les 3 premiers terminaux sont des terminaux de contrôle, c'est à dire qu'il permette à l'utilisateur de saisir les données de ces variables depuis la face-avant. Le quatrième c'est un indicateur : un graphe XY.

4.2.1.2 Les variables

Le langage G ou langage graphique disponible dans LabVIEW utilise deux types de terminaux, le terminal "contrôle" et le terminal "instruction". La différence entre les deux est que le premier est utilisé pour l'écriture, et le deuxième sert pour l'affichage. LabVIEW propose quatre types de variables. Le type U8 qui représente un entier non signé codé sur 8 bits (on peut spécifier d'autres codages), le type DBL qui représente un nombre flottant, le type TF qui est une valeur booléenne (Vrai – Faux) et enfin le type intitulé ABC servant à représenter les chaînes de caractères. Le tableau suivant donne un exemple sur les quatre types de variables.



4.2.1.3 Palette des commandes

La palette de commandes contient les commandes et indicateurs utilisés pour créer la face-avant. On peut l'accéder à la palette de commandes sur la fenêtre de la face-avant en

choisissant Affichage "Palette de commandes" ou en cliquant avec le bouton droit de la souris sur une zone VI de la face-avant. La Figure IV.2 présente une palette Commandes.

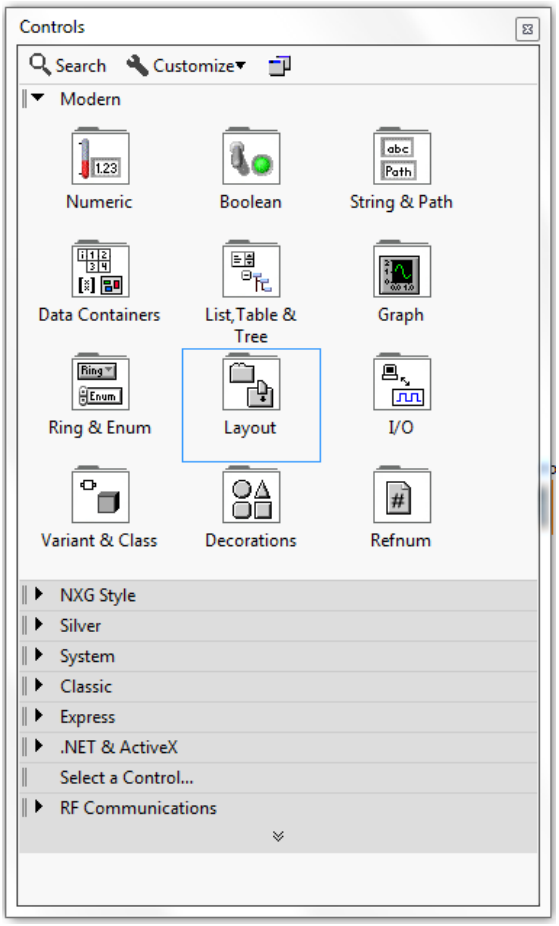


Figure IV.2: Palette des commandes

4.2.1.4 Le diagramme

Le diagramme sert à représenter le code de notre application à l'aide du langage Graphique. Les objets de diagramme sont des terminaux, des sous-VIs, des fonctions, des constantes, des structures et les fils de liaison qui transmettent des données à d'autres objets de diagramme. L'exemple suivant représente un diagramme qui permet de calculer la somme de valeur a et b on utilise deux terminaux de commande pour entrer la valeur de a et b, un indicateur pour afficher le résultat, des fils de liaison, et une fonction d'addition de deux valeurs.

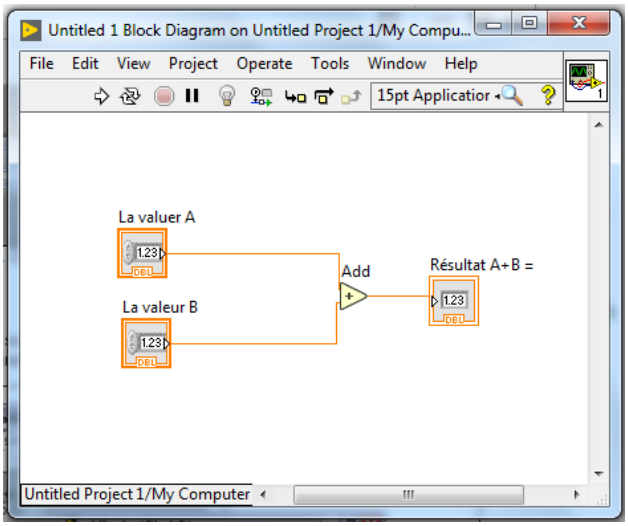


Figure IV.3: Exemple d'un diagramme permet de calcule la somme A+B

4.2.1.5 Palette des fonctions

La palette Fonctions contient les VIs, les fonctions et les constantes que l'on peut utiliser pour créer le diagramme. La palette de fonction ci-dessus va nous permettre d'accéder à l'ensemble des fonctions défini par LabVIEW. Ces fonctions sont regroupées par catégories. La Figure IV.4 présente une palette des Fonctions avec toutes ses catégories Visibles et la catégorie Programmation développée.

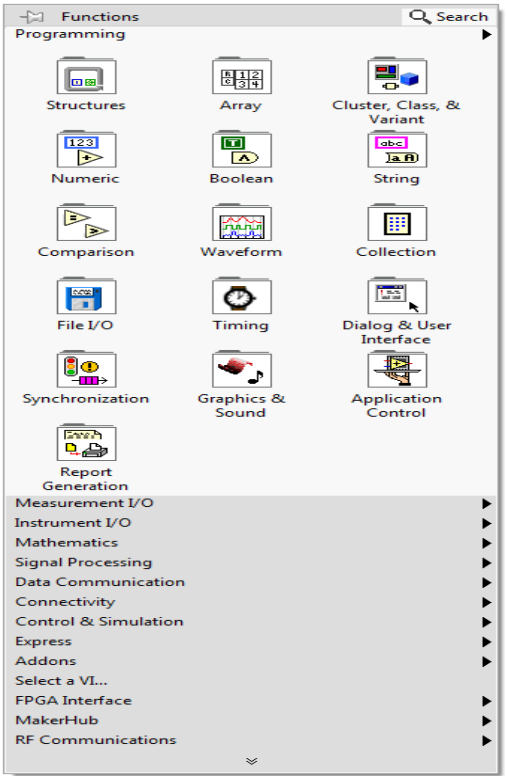


Figure IV.4: Palette des fonctions

4.3 Les logiciels utilisés :

Pour réaliser cette implémentation, il a fallu disposer des logiciels suivant :

- LabVIEW 2020
- NI-Modulation toolkit 20.0
- Bibliothèque : String_to_Bistream.VI Bitstream_to_String AES.VI AES Algorithm.VI

4.4 Chaine de transmission d'un texte modulé en QAM sous LabVIEW :

Dans ce modèle nous simulons une chaine de transmission modulée en QAM. Ce modèle se compose de deux parties :

4.4.1 Face avant:

L'interface utilisateur qui permet l'action sur les paramètres de modulation, le message a envoyé, les paramètres de cryptage. (figure IV.5)

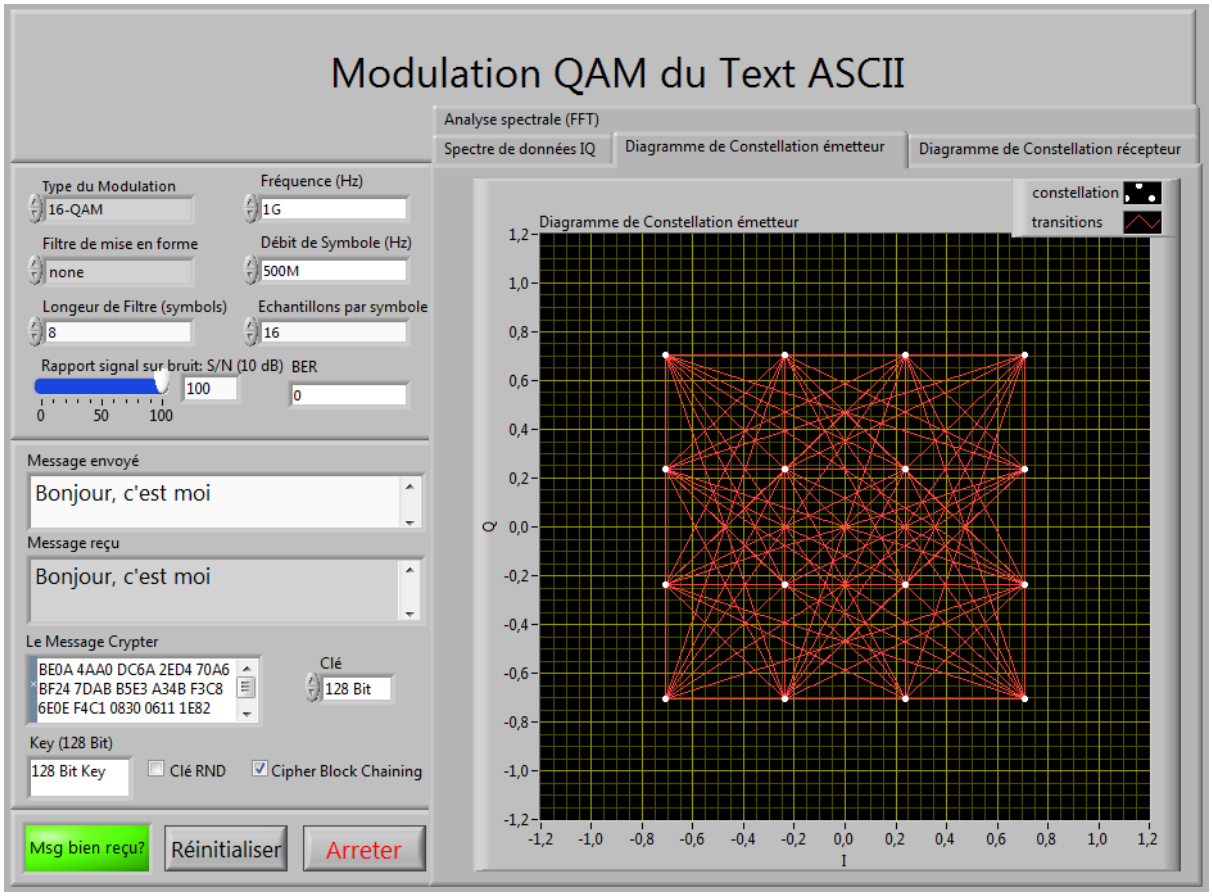


Figure IV.5 : Face avant d'une chaine de transmission QAM crypté

4.4.1 Le diagramme:

L'interface de programmation graphique similaire à celle de simulink dans matlab, consiste à relier les blocs entre aux afin d'assurer le transfert des données entre ces derniers et les réglages nécessaires entre les blocs.

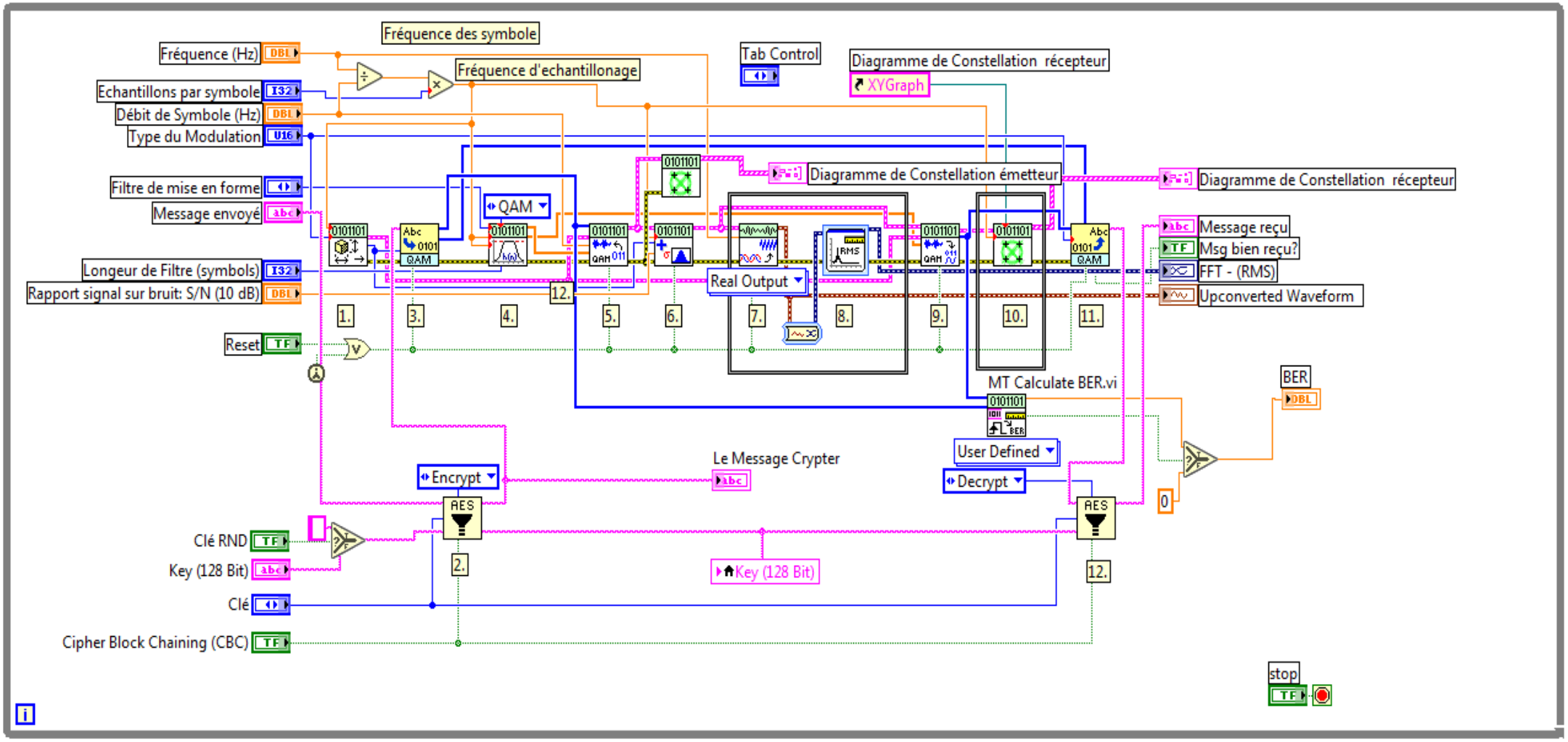


Figure IV.6 : Diagramme d'une chaine de transmission QAM cryptée

4.5 Paramètres de la chaîne QAM et de cryptage AES

Les paramètres primordiaux utilisés pour la simulation sont les suivants :

Paramètres de la chaîne QAM	
Type de Modulation	16-QAM
Fréquence(Hz)	1G
Débit de Symbole (Hz)	500M
Filtre de mise en forme	Aucun
Longueur de Filtre (symboles)	8
S/N (dB)	100
Message a envoyé	Bonjour, c'est moi

Tableau IV.1 : Les paramètres de la chaine de transmission

Type de modulation : dans ce paramètre on peut choisir le type de modulation 4-QAM, 8-QAM, 16-QAM, 32-QAM, 64-QAM, 128-QAM, 256-QAM.

Fréquence : La fréquence utilise pour la transmission de signal.

Débit de symbole : Spécifie le débit de symboles, en hertz (Hz).

Filtre de mise en forme : Spécifie le type de filtre à générer.

Longueur de Filtre : Spécifie la longueur du filtre de mise en forme.

Echantillons par symbole : spécifie un nombre d'échantillons dédiés à chaque symbole. Multipliez cette valeur par la fréquence des symboles pour déterminer la fréquence d'échantillonnage.

Le rapport S/N : Spécifie la valeur de signal sur bruit en dB.

Paramètres de cryptage AES	
Clé	128 Bit
La Clé RND	Non Utilisé
Cipher Block Chaining	Utilisé

Tableau IV.2 : Les paramètres de cryptage AES

Clé : Spécifie la **taille de clé de cryptage : 128, 192 ou 256 bits.**

Cipher Block Chaining : CBC est une forme avancée de chiffrement par bloc. Cela ajoute un niveau supplémentaire de complexité aux données chiffrées.

4.6 Les blocs utilisés

Le modèle est basé sur une boucle While infinie qui permet de tourner en permanence le programme qu'elle contient. Nous citons ci-dessous les 9 composants de ce dernier (7 du modèle et 3 pour les mesures) :

MT Generate système paramètres : Ce VI génère les paramètres de modulation et démodulation.

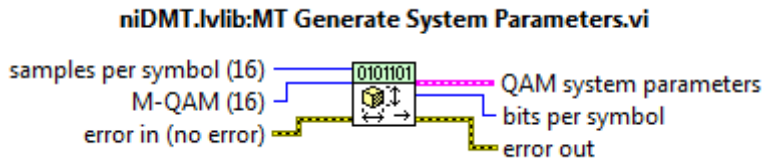


Figure IV.7 : MT Generate système paramètres

String to Bitstream : Ce VI convertit les caractères en séquence binaire.

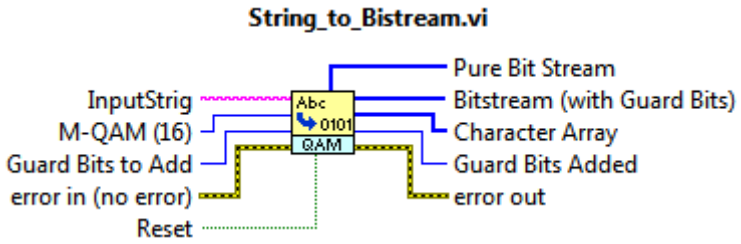


Figure IV.8 : String to Bitstream

Generate Filter Coefficients : Ce VI générera des coefficients de filtre qui seront utilisés pendant la modulation pour réduire la bande passante du signal modulé et pendant la démodulation pour réduire les interférences inter-symboles.

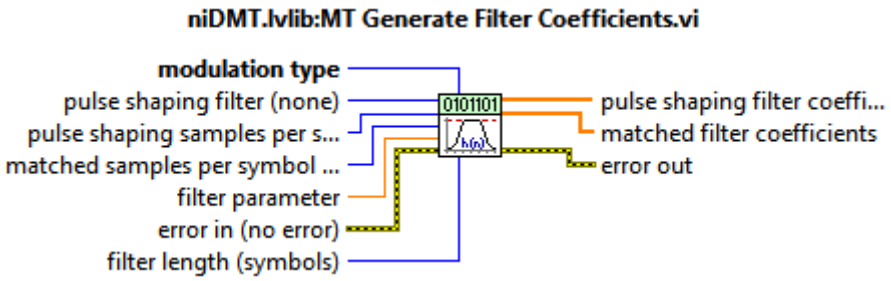


Figure IV.9 : Generate Filter Coefficients

MT Modulate QAM : Ce VI reçoit une séquence de bits de données, effectue une modulation QAM et renvoie sous la forme d'onde de bande de base complexe modulée.

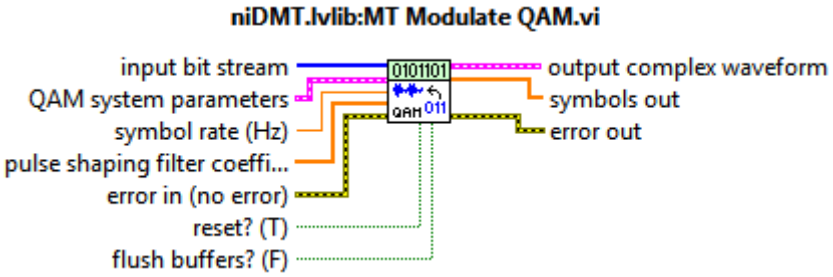


Figure IV.10 : MT Modulate QAM

MT Add AWGN : Ce VI sert à ajouter du bruit blanc au signal modulé à transmettre, le rapport signal sur bruit S/N est spécifié par l'utilisateur, où S représente l'énergie par bit et N représente la variance du bruit.

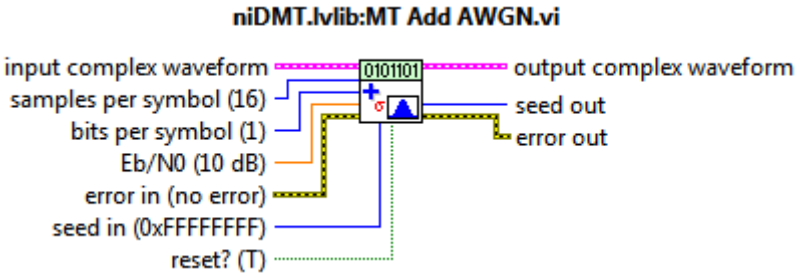


Figure IV.11 : MT Add AWGN

MT Demodulate QAM : ce VI Convertit un signal modulé en séquence de bits binaire.

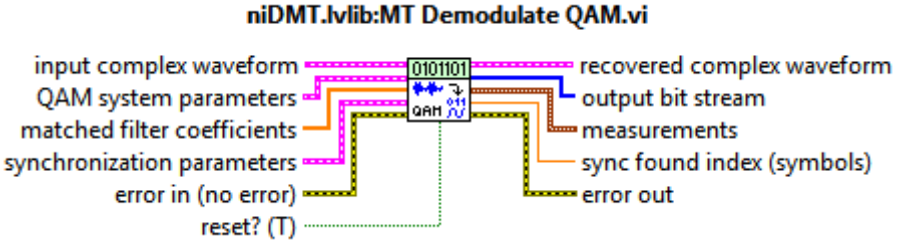


Figure IV.12 : MT Demodulate QAM

MT Format Constellation : Prépare un signal pour la présentation sur un graphe qui montre les emplacements de symboles détectés et les transitions entre ces symboles.

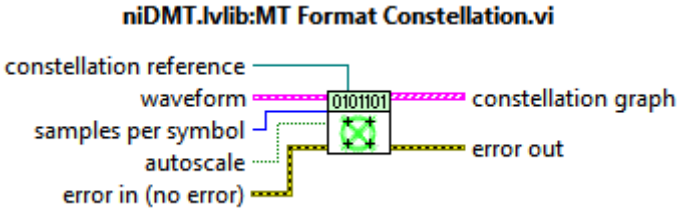


Figure IV.13 : MT Format Constellation

Bitstream to String : ce VI sert à convertir les bits des données en format caractère.

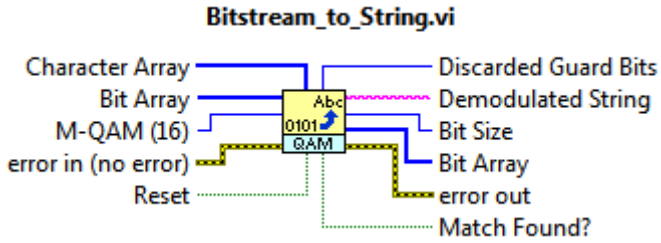


Figure IV.14 : Bitstream to String

AES Algorithm : ce VI est utilisé pour crypter et décrypter les données émis dans le canal en utilisant l'algorithme AES.

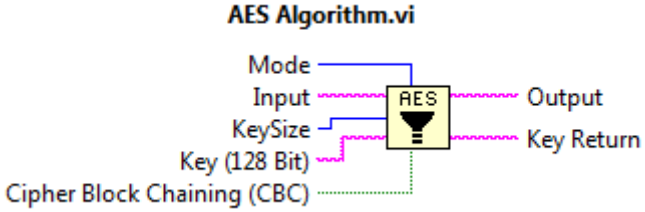


Figure IV.15 : AES Algorithm

4.7 Description détaillé sur le programme :

4.7.1 Processus de chiffrement :

Le bloc de cryptage (AES Algorithm) se former de deux bloc. Le premier bloc pour générer la clé de cryptage. Le deuxième bloc utilise cette clé pour crypter le message qu'on désire chiffrer.

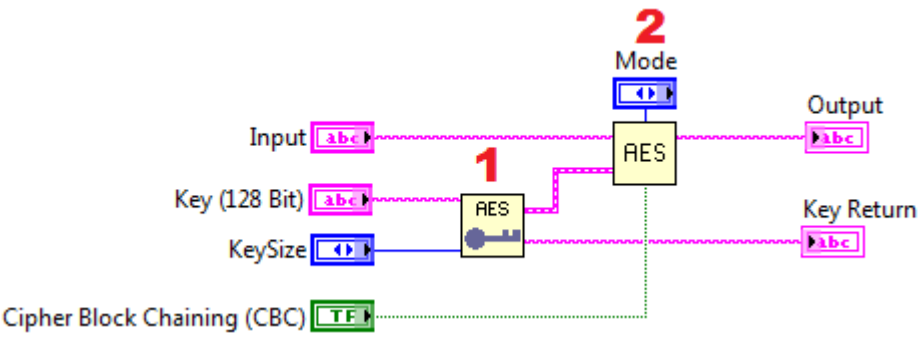


Figure IV.16 : Le bloc de cryptage (AES Algorithm)

Génération de la clé de cryptage :

Le digramme suivant présente l'étape KeyExpansion.

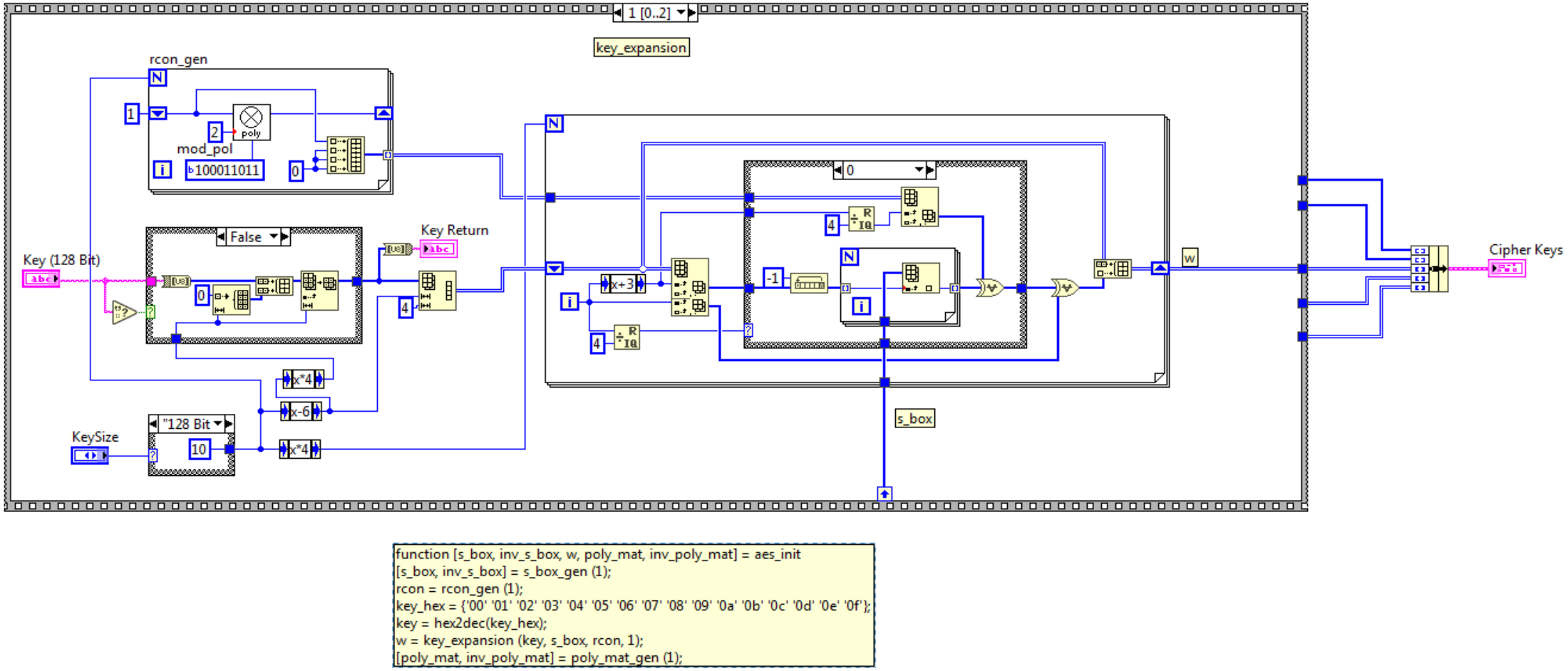


Figure IV.17: Diagramme de bloc qui génère la clé de cryptage KeyExpansion

Chiffrement de texte avec l'algorithme AES :

Le digramme suivant présente les étapes de cryptage AES (SubByte, ShiftRows, MixColumns, AddRoundKey).

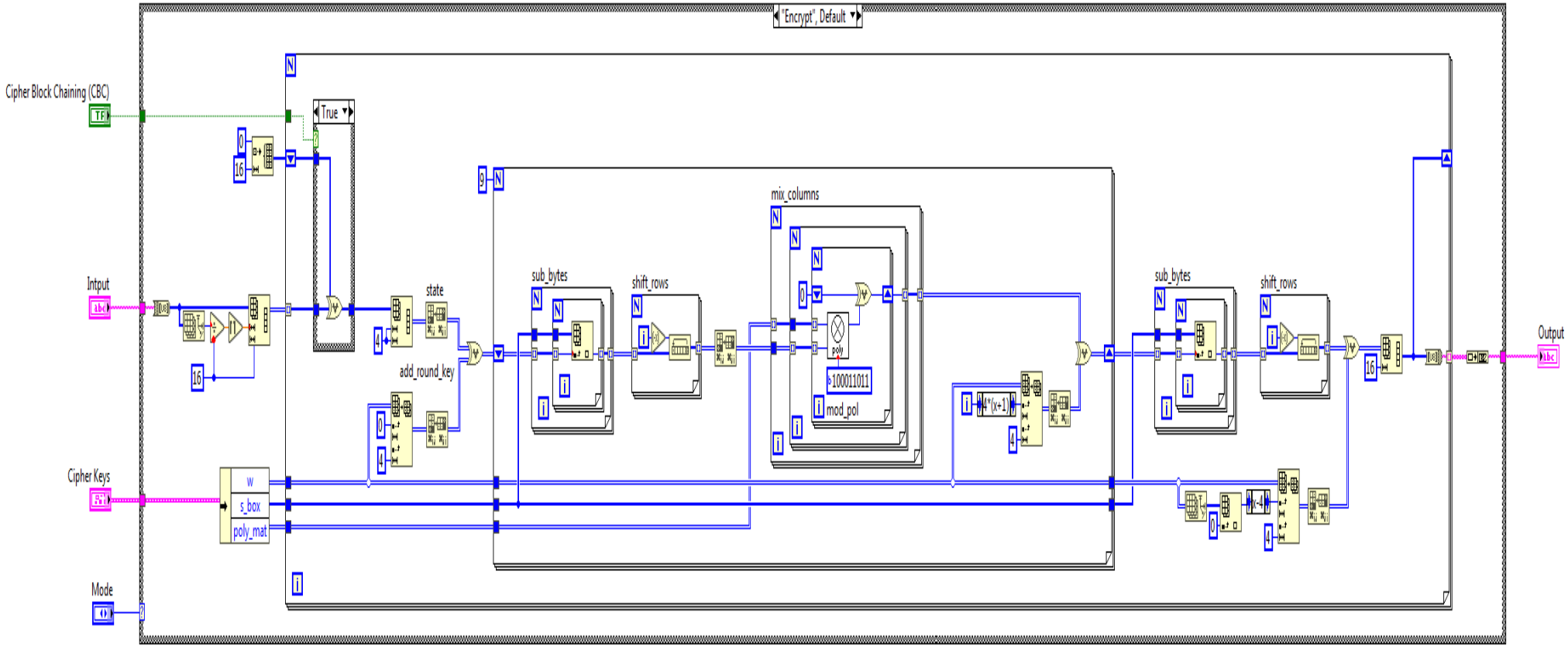


Figure IV.18: Diagramme de bloc d'algorithme de cryptage

L’application permet de crypter un message avec le chiffrement AES (128 bits). Il est possible d’entrer un texte dans la partie Message envoyé. Pour lui appliquer l’algorithme AES pour cela, il faut d’abord convertir chaque lettre du message en hexadécimale, puis stocker chaque deux chiffre hexadécimaux dans un tableau de 4 lignes et 4 colonnes, qui s’appelé un bloc ou state. Comme AES est un chiffrement par blocs, chaque bloc chiffré doit avoir 16 octets (chaque lettre est codée sur 8 bits, ce qui donne un total de 128 bits). Si le nombre de caractères entré ne permet pas d’avoir le dernier bloc restant de 16 caractères, une fonction a été codée afin d’ajouter x nombres de fois le caractère « 0 » pour compléter le dernier bloc à chiffrer.

Exemple le message : LE CHIFFREMENT AES

Texte	L	E	C	H	I	F	F	R	E	M	E	N	T	A	E	S
Hexadécimale	6c	65	63	68	69	66	66	72	65	6d	65	6e	74	61	65	73

6c	69	65	74
65	66	6d	61
63	66	65	65
68	72	6e	73

Figure IV.19: State pour le mot : LE CHIFFREMENT AES

4.7.2 Processus d’émission :

Le processus d’émission commence par la déclaration des paramètres de la chaine de transmission, et les paramètres de filtre de mise en forme. La deuxième étape consiste à appliquer l’algorithme de cryptage AES sur le message entré, ensuite le bloc (String_to_Bistream) convertit ce message crypté en séquence binaire.

Modulation :

Le modulateur reçoit cette séquence binaire sur laquelle il effectue une modulation QAM et renvoie le signal modulé.

Effet canal :

Dans cette partie on génère un bruit et l'additionne avec notre signal qui identifie le bruit blanc gaussien (AWGN) additif.

4.7.3 Processus de réception :

Démodulation :

Le processus de réception commence par démoduler le signal reçu en forme d'onde est on récupère la séquence binaire du début.

4.7.4 Processus de Déchiffrement :

La dernière étape consiste à décrypter le message reçu. Pour pouvoir décrypter le message, il suffit de coder la matrice inverse nécessaire au décryptage. En principe, puisque AES est basé sur une fonction réversible, il effectue les mêmes opérations que le chiffrement, mais les matrices sont inversées, le déchiffrement doit retourner le message d'origine.

Les fonctions inverses de chaque étape qui sont généralement nommées InvShiftRows, InvSubBytes et InvMixColum

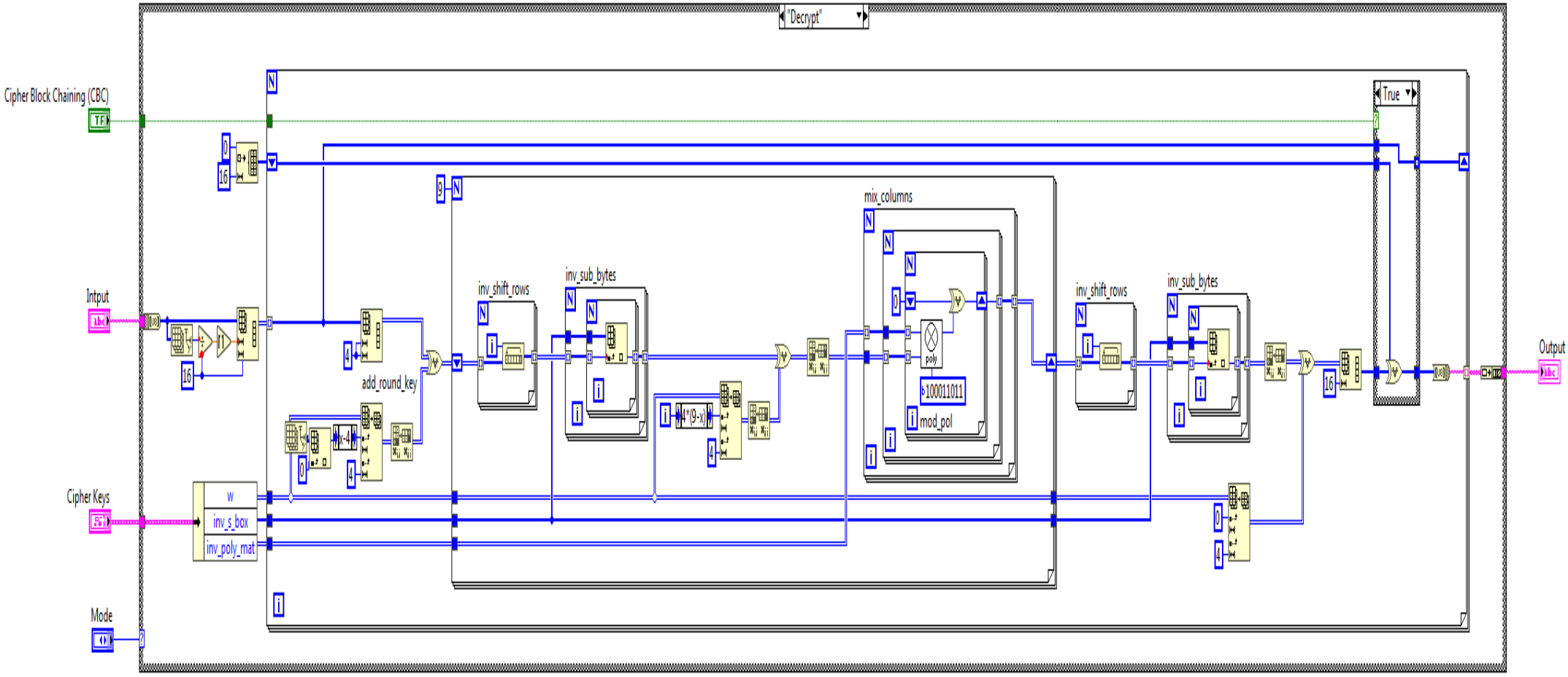


Figure IV.20 : Diagramme de bloc d'algorithme de décryptage

4.8 Résultats :

Il est important de s'assurer que le message reçu est le même que celui qui a été transmis, les résultats de la simulation de ce programme est comme suite :

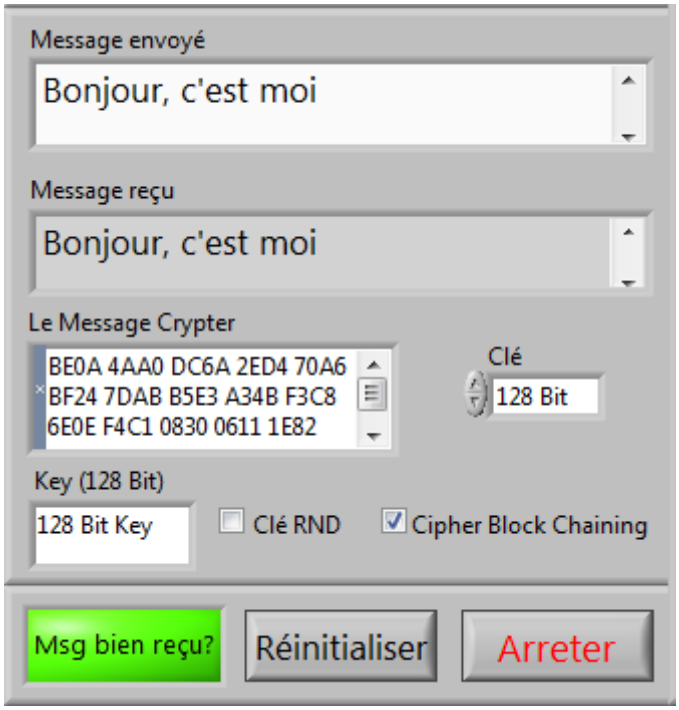


Figure IV.21 : Résultat de message transmis

4.8.1 L’influence de bruite sur le canal :

L'Etude d'un ensemble de cas par changement de paramètre S/N (signal sur bruit) avec la modulation 16-QAM.

Constellation a l’émission :

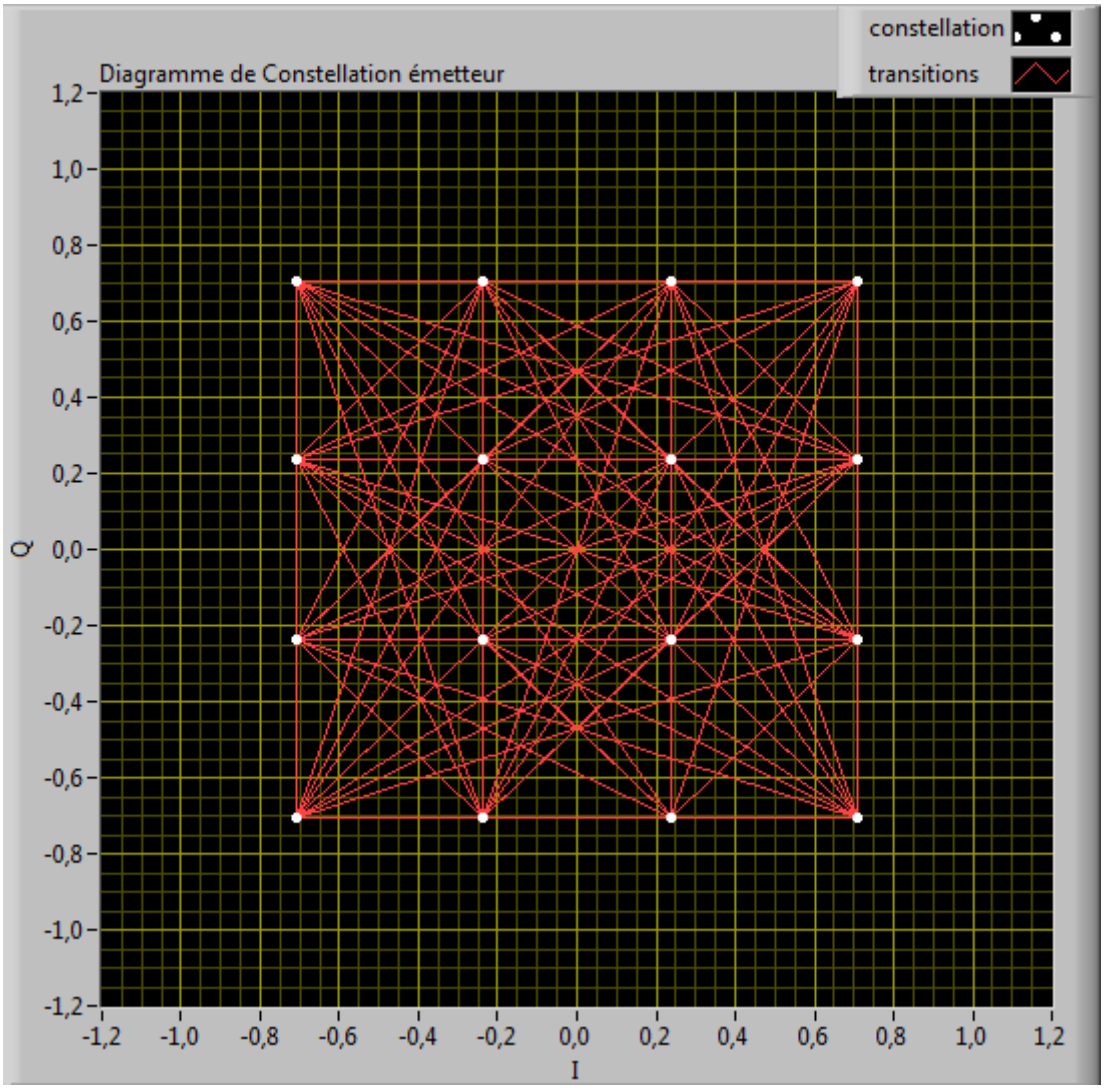


Figure IV.22 : Constellation a l’émission

Le message transmis :

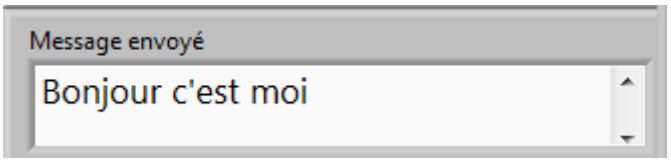


Figure IV.23 : Résultat de la simulation de modulation 16QAM avec un SNR=0 dB.

Constellation a la réception :

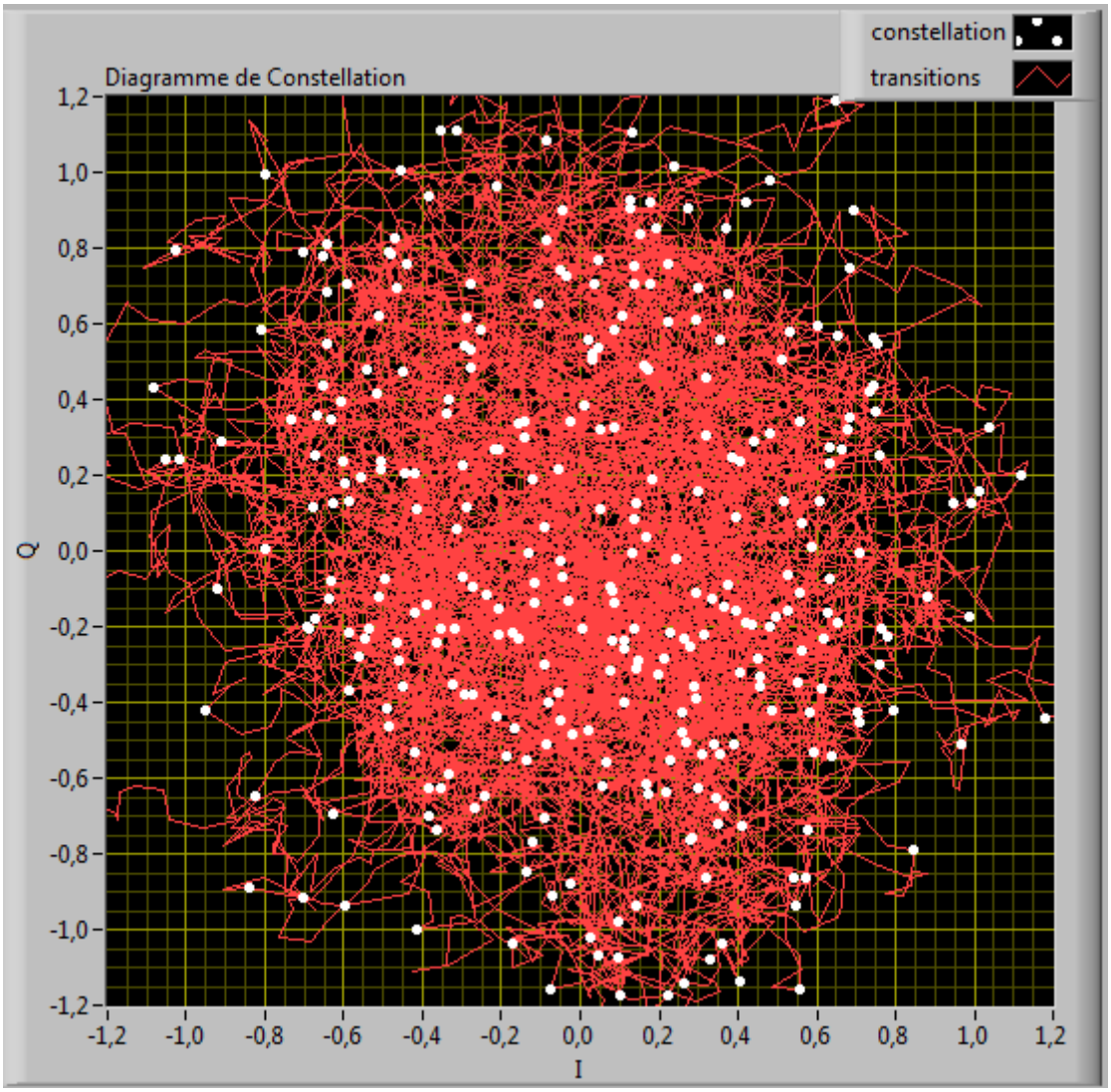


Figure IV.24 : Constellation a la réception pour SNR=0 dB

Le message reçu :

Figure IV.25 : Résultat de la simulation de modulation 16QAM avec un SNR=0 dB.

Constellation a la réception :

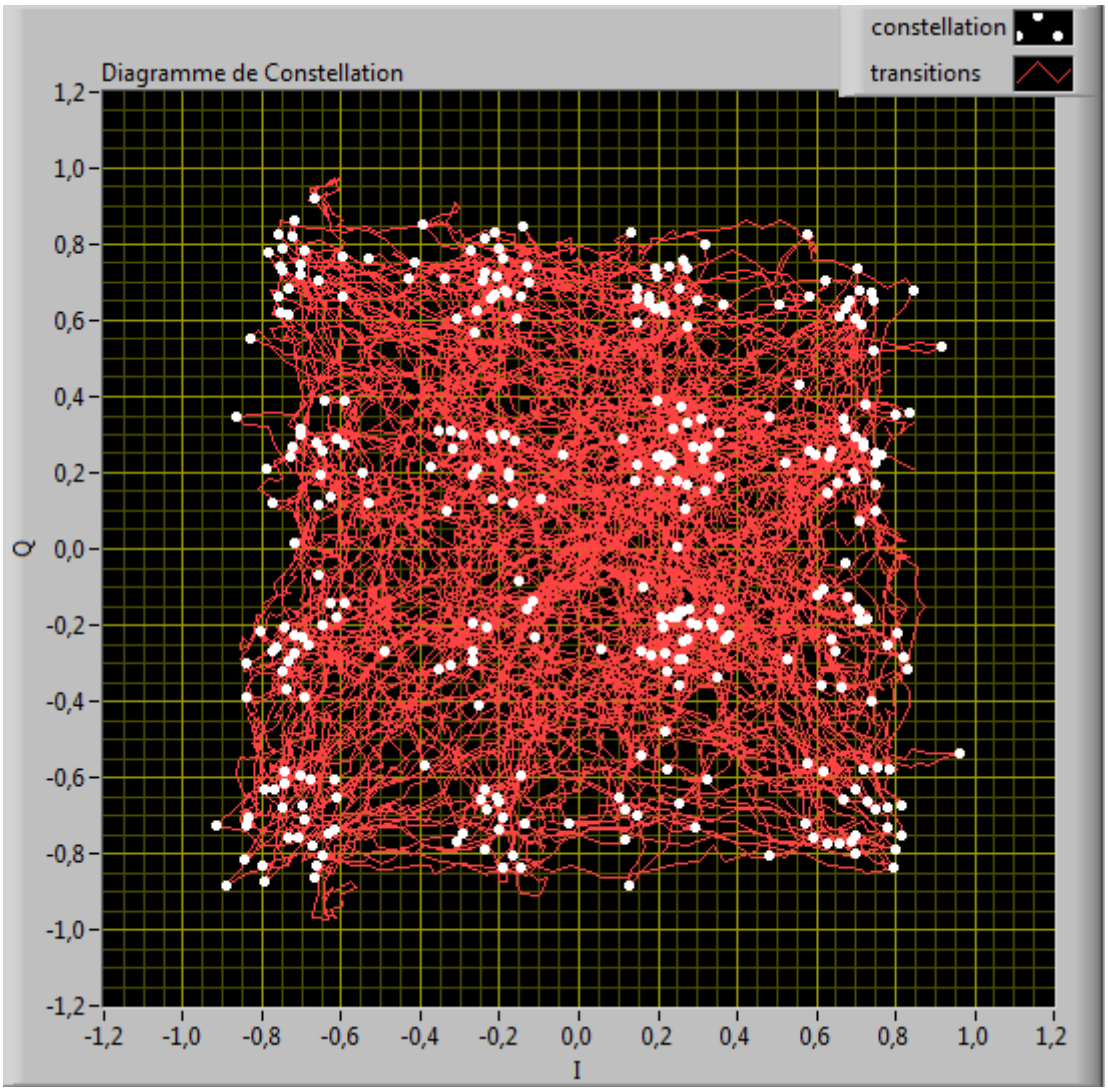


Figure IV.26 : Constellation a la réception pour SNR = 10 dB

Le message reçu :

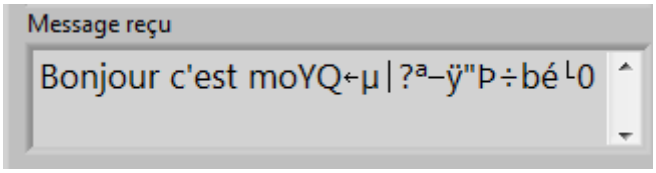


Figure IV.27 : Résultat de la simulation de modulation 16QAM avec un SNR=10 dB.

Constellation a la réception :

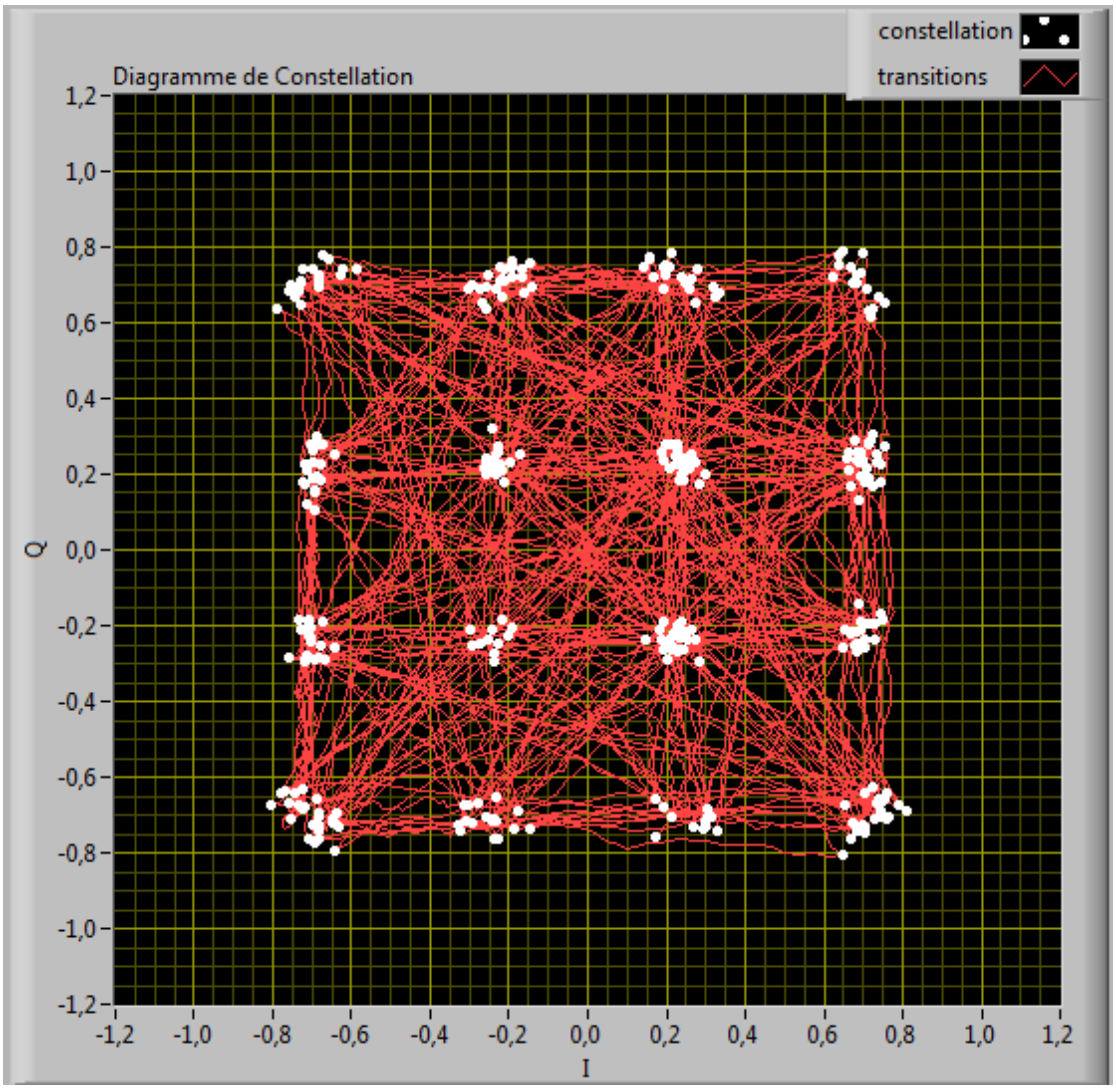


Figure IV.28 : Constellation a la réception pour SNR=20 dB

Le message reçu :

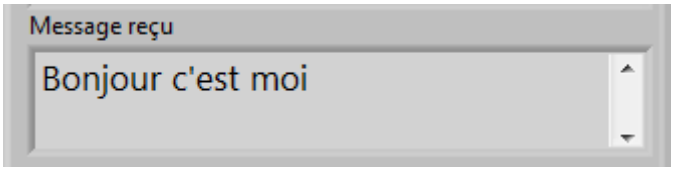


Figure IV.29 : Résultat de la simulation de modulation 16QAM avec un SNR=20 dB

Les figures précédentes représentent une constellation pour la modulation16QAM avec 3 valeurs SNR en émission et réception en présence d'un bruit AWGN.

Dans le cas d'émission le canal de transmission est idéal, sans bruit, tous les symboles sont représentés dans le diagramme de constellation par des points bien définis et concentrés.

Dans le cas de réception le bruit généré agit sur le signal, il a un effet direct sur le diagramme de constellation comme nous le montre les figures. On remarque que les points dans la constellation de réception se dispersent et créent différentes formes sur le diagramme. Cela arrive car le bruit ajouté déforme le signal.

Nous remarquons également un effet direct sur le message sous formes des caractères aléatoires à partir de la variation des valeurs du SNR.

4.9 Conclusion :

LABVIEW est un outil très puissant qui peut être utilisé pour la simulation dans la communication. D'après les résultats de ce chapitre en conclu que le bruit dans la communication est une menace pour la transmission de bits numérique conduisant a plusieurs erreurs au nivaux des bits, ce qui signifie que l'information transmise changera aussi ou perdra son contenu.

Conclusion générale

Par le biais de ce mémoire, nous avons pu réaliser un travail qui consiste à définir les fondements théoriques qui régissent la transmission numérique des informations. En présentant les bases théoriques qui permettent de décrire l'ensemble des fonctions concernées par notre étude.

Puis on a présenté les fondements de la transmission sécurisée, basé sur le chiffrement symétrique. Dans notre chaine de transmission on a utilisé le chiffrement AES qui est l'algorithme de chiffrement le plus utilisé et le plus sûr disponible aujourd'hui.

Nous avons conçu notre chaîne de transmission sur le logiciel LabVIEW. Nous avons d'abord commencé par nous familiariser avec les blocs de communication de la bibliothèque NI Modulation toolkit que nous pouvons mettre en œuvre puis on a simulé la technique QAM

La réalisation de ce projet a énormément contribué à l'enrichissement de nos connaissances dans plusieurs domaines intéressants tant celui d'actualité tel que la cryptographie ou ceux de la conception d'une chaine de transmission sur le logiciel labVIEW.

.

Bibliographie :

[1] : J-C Rolin G Eiffel Dijon, TSi Chaîne d'information Transmission de l'information sous forme numérique, 02/2008

[2] : Genevieve Baudion, Radiocommunications Numériques. Dunod, 2002, ISBN: 978-2-10-059513-6

[3] : A.Fischer', 'COURS DE TELECOMMUNICATION Commutations et systèmes de transmission',' IUTGTR -Université de Paris XIII'.

[4] :http://mediatools.iict.ch/document?url=Cours_de_TelecommunicationsModulations/mod2/Mic.pdf&dpId=15', La modulation par impulsions et codage (PCM, MIC)

[5] : Dominique Seret RESEAUX et TELECOMMUNICATIONS, Université René Descartes – Paris 5UFR de mathématiques et Informatique, 2005,2006

[6] : 'Gérald Arnould',' thèse de doctorat ; Etude et Conception d'Architectures Haut-Débit pour la Modulation et la démodulation Numériques','8Décembre2006'

[7] : Bourennane Hamza ; Douiden Zakaria ; Thèse master; Eude et simulation d'une chaine de transmission numérique, université de blida, 2011.

[8] : Cryptographie. Wiktionary. [Online]. http://fr.wiktionary.org/wiki/cryptographie

[9] : Raphaël Moreau. www.maaars.fr. [Online]. https://maaars.fr/cryptographie-quelques-bases/

[10] : Histoire de la cryptologie. Wikipédia. [Online]. https://fr.wikipedia.org/wiki/Histoire_de_la_cryptologie

[11] : Petite histoire de la cryptologie. Apprendre en ligne. [Online]. https://www.apprendre-en-ligne.net/crypto/histoire/

[12] : Scytale. Wikipédia l'encyclopédie libre. [Online]. http://fr.wikipedia.org/wiki/Scytale

[13] : Le chiffre de César. La cryptographie expliquée. bibmath. [Online]. http://www.bibmath.net/crypto/index.php?action=affiche&quoi=substi/cesar

[14] : Le chiffre de vigenère. La cryptographie expliquée. bibmath. [Online]. http://www.bibmath.net/crypto/index.php?action=affiche&quoi=poly/VIgenere

[15] : L'affaire du télégramme de Zimmermann. bibmath. [Online]. http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debVIngt/zimmermann

[16] : Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, and Sébastien Varrette. (2013) Théorie des codes.

[17] : Chiffrement symétrique. devensys. [Online]. https://blog.devensys.com/chiffrement-symetrique/