UNIVERSITE SAAD DAHLEB DE BLIDA

Faculté des sciences de l'ingénieur

Département d'aéronautique

MEMOIRE DE MAGISTER

Spécialité : Aéronautique

ETUDE D'UNE CHAINE DE TRANSMISSION DE DONNEES CRYPTEES SUR UN CANAL BRUITE

Par

Azine Houria

Devant le jury composé de :

S. BOUKRAA	Professeur, U.S.T.B., Blida	Président
H. SALHI	Maître de conférences, U.S.T.B. Blida	Examinateur
M. GUESSOUM	Professeur, U.S.T.B., Blida	Examinateur
H. TAHRAOUI	Docteur C.R.D.A.T, Alger	Rapporteur
S. BERGHEUL	Chargé de cours, U.S.T.B., Blida	Examinateur
B. SLIMANI	Chercheur, C.R.D.A.T., Alger	Invité

Blida, septembre 2006

RESUME

Ce document de thèse s'attache à l'étude d'une chaîne de transmission de données cryptées sur un canal bruité. Le codage en général relève de la théorie de l'information. La correction d'erreurs et le chiffrement sont des aspects importants de la protection de l'information. Il s'agit d'une part de résister au bruit et d'autre part de lutter contre les fraudes.

Donc le travail s'est focalisé sur deux aspects importants, le premier aspect est celui de la théorie d'information avec l'étude des performances associées à des modulations à haute efficacité spectrale (MDP8, MAQ16) ainsi qu'à la correction des erreurs et le deuxième aspect est celui de la sécurité d'information « cryptage », nous avons opté pour l'algorithme IDEA qui a une clé de 128 bits sur un mot de 64 bits. IDEA est aujourd'hui un algorithme considéré comme très robuste, et qui a remarquablement résisté à toutes les tentatives de cryptanalyse.

هذا البحـــث خاص بدراسة سلسلة توصيل المعلومات المشفرة في قناة مشوشة حيث أن التشفير مأخوذ عموما من النظرية المعلوماتية.

تصحيح الأخطاء و الترقيم يعتبر جانب مهم لحماية المعلومة, من ناحية يقاوم التشويش و من ناحية أخرى يصد القرصنة.

هذا العـــمل يتركز على وجهين مهمين, الوجه الأول حول النظرية المعلوماتية و مزاياها, والوجه الثاني على تامين المعلومات (التشفير).

اخترنا لوغـــــريتم (IDEA) بمفتاح 128 بايت على كلمة ب64 بايت حيث يعتبر هذا البرنامج مقاوم لقرصنة التشفير

ABSTARCT

This document of thesis studies the coded data link chain on a sound-effected cannel. The error correction and encryption are important aspects for protecting the information. It consists of resisting to the noise, and on the other hand, fighting against frauds. These two contradictory methods, reveal against hide are often complementary.

So, this work is based on these two important aspects. The first one which is from the theory of information with the study of performances associated to high spectral modulations effectiveness.(MDP8, MAQ16) and the error correction. The second aspect is of the security of information ‘’ encoding’’.

We opted for the algorithm IDEA which has a key of 128 bits on a word of 64 bits. IDEA is a reliable algorithm which has resisted against many encoding attempts**.**

REMERCIEMENTS

Lors de la rédaction de mon rapport de thèse, les seules lignes qui me venaient naturellement à l'esprit, fréquemment de surcroît, étaient celles qui auraient doit constituer ces remerciements. Malheureusement, toute l'énergie mobilisée jadis a été consommée, et me voilà presque devant l'angoisse d'une page blanche au moment de les rédiger. Presque, puisque j'ai quand même un grand nombre de personnes à remercier, inconditionnellement, et donc de la matière à travailler ; le seul frein est la mise en forme de ces lignes, qui sera loin, très loin croyez-moi, de celles que j'avais mentalement rédigées, il y a quelques mois. Tout s'est bien terminé ; allons donc à l'essentiel, et efforçons-nous de n'oublier personne.

Ce travail n'aurait pu se faire seul, ce sont les compétences, la disponibilité, et la bonne humeur de chacun, qui m'ont permis de poursuivre mes études et surtout d'achever cette thèse dans les meilleures conditions. C'est pourquoi je tiens chaleureusement à remercier ici toutes personnes qui ont contribués de loin comme de prés à ce travail.

Tout d'abord,

Je tiens à remercier chaleureusement le directeur d'institut d'aéronautique, Mr. BERGHEUL et Mr. REZZOUG pour m'avoir accueillie, encouragé, guidé et qui ont rendu mon rêve réalité merci infiniment

Un hommage aux personnes qui m'ont suivi lors de ces trois années, sans qui tout ceci n'aurait pas été possible leur passion et leur rigueur.

Je commence par le Directeur du CRDAT Monsieur « TEBOUDELETTE » pour son soutien inconditionnel et ses conseils avisés, il a été un frère, un ami, une oreille dans les moments difficiles, pour lui la vie continue.

Au Directeur de Thèse le Docteur « TAHRAOUI Hocine », Chef de Département Informatique au niveau du CRDAT, qui a tenté de m'inculquer la rigueur nécessaire à l'achèvement de ce travail (on y arrive doucement...) et qui a su me donner les conseils et l'aide nécessaire pour l'aboutissement de ce projet et surtout pour son entière disponibilité.

Aux Ingénieurs du CRDAT « AMINE, TAREK, BRAHIM, ABDEKARIM, MAJDID et ADAA » pour leurs aides précieuses.

Je remercie très sincèrement les membres du jury d'avoir accepté d’examiner cet humble travail. Qu'ils sachent tous que c'est pour moi un grand honneur de pouvoir leurs présenter cette thèse.

Ma vie aurait par ailleurs été bien terne sans toutes les personnes qui m’ont offert leur amitié et leur aide.

Tout ceci n’aurait évidemment pu être possible sans ma mère, mon père, qui m’ont apporté soutien et réconfort dans les moments de doute et sans qui toutes ces années auraient été bien fades, merci ma **CHIRAZ** pour ton amour, soutien, tu as été ma mère, ma sœur, ma confidente, ma complice et ma fille à la fois, malgré ton jeune âge dans les moments de faiblesses, eh! Oui les rôles se sont inversés pardon ma fille.

Merci à mes sœurs (Djamila, Kenza, Yamanda, Assia et Nadjet sans oublier la grande Ghizléne) pour leurs soutiens durant toute cette période de difficultés et de problèmes, je leur dis chapeau mes anges,Je ne saurais être qu’infiniment reconnaissante quant aux sacrifices qu’elles ont consentis.

Merci à mes frères, mes belles sœurs et leurs enfants, à mes beaux-frères (Riad, Sofiene et Ahmed).

Un grand merci à Lila, Zineb et Kahina pour leur soutien.

A mes amis (ies) Djamel, Youcef , Nawel, Aliéléve, tante Fatiha , Samira, à Mr Hadji et à toute ma promotion sans oublié Dalila responsable du centre de calcul .

Enfin merci à ceux que je n’ai pu citer mais qui ont toutes mes amitiés et mes remerciements.

TABLE DES MATIERES

LISTE DES ILLUSTRATIONS, GRAPHIQUES ET TABLEAUX

“Rien n’est plus pénible à surmonter que les
Difficultés que l’on croyait surmontées.”

Alexis de Tocqueville

INTRODUCTION GENERALE

Il y a deux siècles, naissaient les premières télécommunications. A cette époque les premiers modes de transmission de l'information peuvent être divisés en deux grands groupes:

- Les signaux visuels: le premier outil pour transmettre des informations fut le feu. Sa fumée indiquait la présence d'un groupe humain ou d'un individu isolé. Un peu plus tard, des feux allumés de relais en relais permettaient la transmission d'une information. De même, on se servait des feux prés des cotes pour signaler les récifs aux bateaux au travers des phares.

- Les signaux sonores: les Gaulois utilisaient des trompes, cors ou encore transmettaient des messages par des cris codes. Dans certaines contrées des pyrènes, on utilisait des langages siffles, une pratique encore utilisée aujourd'hui. D'autres moyens comme les cloches d'églises ont également été employées jusqu'au debut du siècle.

Il va sans dire que la rapidité de ces communications ne permettait pas un dialogue très complet ni rapide comparé à ce que nous connaissons aujourd'hui. Depuis toujours, les hommes ne cessent de faire des découvertes qui concourent toutes à accélérer le délai d'acheminement de l'information.

Les progrès considérables établis au XX siècle ont été le facteur essentiel dans le développement des télécommunications et tout cela ne serait rien sans le concours providentiel de certains hommes qui ont révolutionné le domaine des télécommunications sans fil.

De nos jours, la technologie permet d'envoyer de plus en plus d'informations de plus en plus vite. Nous avons donc vu tout naturellement apparaître les communications numériques via les ondes hertziennes.

La transmission de données dans le domaine de l'aéronautique n'était pas vraiment développée, car dans l'aviation civile, il n'y a pas de secret, la transmission de données était courante mais, Elle a connu un développement après les avènements du 11 septembre 2001 (les États-Unis ont adopté le 19 novembre 2001 un règlement), l'aviation and transportation security act imposant aux compagnies aériennes opérant des vols à destination de leur territoire, de leur transférer des données relatives aux passagers et aux membres d'équipage (passenger manifest information). Le transfert doit être effectué par voie électronique et terminé avant le décollage de l'avion, au plus tard dans les 15 minutes après le départ, pour les passagers [1].

Toutes les données doivent être transmises à une base de données centralisée exploitée conjointement par les douanes U. S et l'immigration and naturalization service. Les données seront alors partagées avec d'autres autorités fédérales et ne bénéficieront plus d'une protection spécifique.

L'objectif de cette thèse est d'introduire le concept des communications numériques et les généralités qui serviront à la bonne compréhension de l'ensemble de cette thèse.

- Le premier chapitre est consacré à la propagation des ondes ainsi qu'aux différentes fréquences mises en jeux ainsi que les différents supports.
- Le deuxième chapitre propose quelques généralités sur la théorie de l'information car c'est la base de la transmission d'information, et pour la compression des données, nous avons utilisé le code de HUFFMAN sans pertes « est appelée souvent codage source », en compressant les données, on se rapproche plus au premier critère de Shannon puis nous avons fait l'étude de la capacité d'un canal (qui est le deuxième théorème de SHANNON) et nous terminerons ce chapitre par le codage canal. Comme il n'existe pas de système de diffusion parfait, que ce soit par onde ou-bien par fil, les données peuvent donc être légèrement altérées lors d'une transmission, mais une légère modification dans un programme peut le rendre totalement inutilisable, et un changement dans des données peut les fausser entièrement. Il faut donc trouver un moyen de détecter ces erreurs au fur et à mesure.
- Le troisième chapitre propose quelques généralités sur les communications numériques, il décrit brièvement le fonctionnement d'une chaîne de transmission. Nous commencerons par la transmission en bande de base avec ces différents codes

dans le cas d'une liaison filaire puis la transmission numérique avec porteuse (modulation QAM, PSK, FSK). Cette étude a été faite pour pouvoir choisir la modulation adéquate car le critère le plus important dans une transmission est l'efficacité spectrale et le taux d'erreurs binaire.

- Le quatrième chapitre est celui du cryptage, l'objectif classique de la cryptologie est d'assurer la confidentialité d'un texte transmis. La tache de la cryptographie est de transformer, grâce à une clé de chiffrement, un texte en clair en un texte chiffré, de telle sorte que la transformation inverse ne soit possible qu'avec la connaissance de la clé de déchiffrement, comme les données sont souvent piratées, les différentes raisons rendent aujourd'hui incontournable le cryptage des informations stockées ou transmises.

Après avoir fait l'étude de toute la chaîne de transmission nous passerons à la simulation de cette chaîne pour pouvoir valider nos résultats

- Le cinquième chapitre, évalue les performances d'une chaîne de transmission de données, une simulation a été réalisée à cet effet dans le premier lieu, il montre les caractéristiques du point de vue élargissement de spectre, puis dans un deuxième lieu, les performances de transmission en probabilité d'erreurs pour un canal bruité, une correction du signal reçu à l'aide d'une réception optimale basée sur le critère de maximum de vraisemblance « code de VITERBI » et en dernier lieu le cryptage « IDEA » pour assurer nos données. Et en dernier lieu une réalisation d'une chaîne de transmission de données cryptées entre deux postes.
- Enfin, ce mémoire est achevé par une conclusion générale.

CHAPITRE 1

GENERALITES SUR LES PROPAGATIONS DES ONDES

1.1 Introduction

L'immense développement des communication a seulement été possible parce qu'un phénomène physique, le champ électromagnétique, pouvait se propager avec un affaiblissement très inférieur à ceux des autres phénomènes connus auparavant (gravité, champ électrostatique).

Il n'est pas question, dans le cadre restreint de cette thèse, d'étudier la propagation des ondes mais nous indiquerons seulement les caractéristiques qui peuvent influencer la qualité d'une transmission de données.

Nous allons appeler voie de transmission le chemin suivi par l'onde radioélectrique pour aller de l'émetteur vers le récepteur, cette voie peut avoir un support matériel comme un coaxial ou un guide d'onde, au contraire elle peut être constituée par une portion de l'espace où se déplace l'énergie de l'onde.

Historiquement ce sont les raffinements des techniques qui ont fait évoluer la perception des problèmes de propagation. Ce qui est important, c'est la possibilité pour le récepteur de recouvrer sans erreurs l'information que l'émetteur avait l'intention de lui transmettre. Deux phénomènes vont gêner l'accomplissement de cette tache: d'une part le signal transmis, subit des altérations au cours de sa propagation (affaiblissement, distorsions diverses…) et d'autre part les perturbations électromagnétiques d'origine naturelle (bruit cosmique) ou anthropique (bruit industriel) viendront s'y superposer.

Connaître un canal de propagation, c'est donc être capable d'une certaine manière de déduire le signal reçu en fonction du signal émis. Le cas le plus courant et le plus simple est celui où le canal peut être considéré comme constant. On distingue deux types de propagation: la propagation en visibilité et la propagation en non-visibilité.

1.2 La propagation en visibilité:

Elle concerne les liaisons pour lesquelles la propagation est de type « optique » ou « quasi-optique ». Ces liaisons utilisent des fréquences élevées dans le domaine des ondes

« centimétriques »ou« millimétriques ». Bien que l'émetteur et le récepteur soient en visibilité l'un par rapport à l'autre, des perturbations, induites par la présence du sol ou de l'atmosphère peuvent intervenir. Deux grandes familles de liaisons appartiennent à cette classe:

- Les liaisons sol-sol, de type faisceaux hertziens.
- Les liaisons sol espace, utilisées par les systèmes de transmissions par satellites.

La plupart des services qui utilisent les VHF-UHF dans le domaine professionnel (radiodiffusion, taxis, police,...) se limitent à la porté géométrique ou à la portée radio encore appelé « line of sight » en anglais. La portée géométrique vaut [20] :

$$D = \sqrt{2R}\left(\sqrt{h1} + \sqrt{h2}\right) \qquad (1.\ 1)$$

L'atmosphère réfracte légèrement les ondes et celles-ci vont donc légèrement plus loin que la portée géométrique, c'est-ce que l'on appelle l'horizon radioélectrique. Dans ce cas nous ne considérons pas encore les phénomènes de propagation troposphérique qui entraînent « de bonnes conditions de propagation », mais simplement une propagation normale que l'on peut obtenir grâce à une atmosphère bien « stabilisée ».

1.3 La propagation en non- visibilité:

Elle concerne des liaisons pour lesquelles un obstacle est interpose entre l'émetteur et le récepteur. Le signal émis va alors se propager grâce à différents phénomènes:

- La diffraction (angle de diffraction): se produit lorsque la ligne de visée (angle. Line of sight: los) entre l'émetteur et le récepteur est obstruée par un obstacle opaque dont les dimensions sont plus grandes que la longueur d'onde du signal émis.
- La diffusion (angle de scattering): se produit dans le même cas que la diffraction mais lorsque les dimensions des obstacles sont comparables à la longueur d'onde.
- La réflexion (angle de réflexion): se produit lorsque l'onde émise rencontre un obstacle dont les dimensions sont très largement supérieures à la longueur d'onde. La réflexion peut avoir pour effet une augmentation ou une diminution du niveau du signal reçu. Lorsqu'il y a un grand nombre de réflexions le niveau du signal reçu peut devenir instable.
- La transmission (angle de transmission): se produit lorsque l'obstacle est en partie « transparent » vis à vis de l'onde émise
- La réfraction (angle de réfraction): provient du fait que la variation de l'indice atmosphérique entraîne une propagation « courbée » de l'onde émise.

1.4 Propagation en espace libre

Lors de la définition d'un système de communications, il est nécessaire de déterminer le type et la taille des antennes d'émission et de réception, la puissance d'émission, l'ensemble des pertes et affaiblissements que va subir l'onde émise et enfin le rapport signal à bruit nécessaire pour pouvoir effectuer la transmission avec la qualité requise. Effectuer cet ensemble de déterminations constitue l'établissement du bilan de liaison.

Il existe d'innombrables types d'antennes avec des caractéristiques très différentes et chaque type d'antenne corresponde à un besoin bien défini. De plus, leur coût est souvent proportionnel à leurs performances.

Les caractéristiques principales sont:

- Le diagramme de rayonnement: antennes omnidirectionnelles, bidirectionnelles, directives, etc.
- Le gain: les antennes directives ont généralement un gain plus important que les omnidirectionnelles,
- La bande passante: les antennes à bande étroite ont généralement un gain plus important que les antennes a large bande,
- La polarisation: rectiligne (horizontale, verticale, etc.) ou circulaire (droite ou gauche)

1.5 Propagation des ondes radio

Les ondes radio (notées RF pour radio frequency) se propagent en ligne droite dans plusieurs directions. La vitesse de propagation des ondes dans le vide est de $3.\ 10^8$ m/s.

Dans tout autre milieu, le signal subit un affaiblissement dû à :

- La réflexion
- La réfraction
- La diffraction
- L'absorption

1.6 Réflexion des ondes radio

Un paramètre d'une importance primordiale dans le choix de la méthode à utiliser pour traiter un problème de propagation est le rapport entre la longueur d'onde considérée et les dimensions caractéristiques du milieu de propagation.

Lorsqu'une onde radio rencontre un obstacle, elle est réfléchie en totalité ou en partie, avec une perte de puissance. La réflexion est telle que l'angle d'incidence est égal à l'angle de réflexion.

Par définition une onde radio est susceptible de se propager dans plusieurs directions. Par réflexions successives, un signal source peut être amener à atteindre une station ou un point d'accès, en empruntant des chemins multiples (on parle de multi-path ou en français cheminements multiples).

La différence de temps de propagation (appelées délai de propagation) entre deux signaux ayant emprunté des chemins différents peut provoquer des interférences au niveau du récepteur car les données reçues se chevauchent.

Ces interférences deviennent de plus en plus importantes lorsque la vitesse de transmission augmente car les intervalles de temps entre les données sont de plus en plus courts. Les chemins de propagations multiples limitent ainsi la vitesse de transmission dans les réseaux sans fil.

1.6.1 La réflexion sur un obstacle

Lorsque le rayon de courbure de l'obstacle est grand par rapport à la longueur d'onde, il est possible de remplacer la surface réfléchissante par son plan tangent au point de réflexion. Le champ incident est peut être représente par une onde localement plane. On peut alors assimiler le phénomène de réflexion sur l'obstacle à la réflexion d'une onde plane sur une surface plane. Les lois de la réflexion et de la réfraction, établies précédemment s'étendent alors à la réflexion sur un obstacle et on peut appliquer les formules de Descartes.

1.6.2 Réfraction des ondes radio

Les formules développées jusqu'à maintenant ont considéré que les différents milieux étaient homogènes et isotropes.

En propagation radio cette hypothèse ne peut s'appliquer à l'atmosphère dont l'indice de réfraction « n » varie de manière continue en fonction de la pression, de la température et de la composition de l'air.

On rappelle que: $n=\sqrt{\frac{\varepsilon.\mu}{\varepsilon_0.\mu_0}}$ et que pour l'air $\mu=\mu_0$. (1. 2)

On admettra que la variation de cet indice en fonction de l'altitude peut être résumée par la formule suivante [20]:

$$n(h) = 1 + 315.10^{-6}.e^{-0,136h} \quad (1.\ 3)$$

Expression dans laquelle l'altitude h est exprimée en km.

Compte tenu des faibles variations de cet indice on introduit souvent le co-indice n définit de la manière suivante:

$$N=(n-1)10^{6} \qquad (1.4)$$

Compte tenu de la formule précédente on obtient: $N(h) = 315.e^{-0,136h}$

Cette variation de l'indice à pour effet d'infléchir la trajectoire des ondes électromagnétiques. Ainsi la trajectoire est réfléchie vers le sol lorsque l'indice de réfraction augmente quand on se rapproche du sol. La trajectoire s'éloigne du sol lorsque l'indice diminue quand on se rapproche du sol.

1.7 Absorption des ondes radio

Lorsqu'une onde radio rencontre un obstacle, une partie de son énergie est absorbée une deuxième partie continue à se propager de façon atténue et une autre partie peut éventuellement être réfléchie.

L'atténuation augmente avec l'augmentation de la fréquence ou de la distance. De plus lors de la collision avec un obstacle, la valeur de l'atténuation dépend fortement du matériau composant l'obstacle. Généralement les obstacles métalliques provoquent une forte réflexion, tandis que l'eau absorbe le signal.

1.8 Atténuation par les gaz

Pour les fréquences élevées et plus particulièrement au-delà de $3\,\text{GHz}$, l'absorption moléculaire peut jouer un rôle non négligeable car il existe des pointes de résonances qui donnent lieu à des absorptions énormes.

Ainsi, l'oxygène présente une absorption importante aux environs de $60\ \text{GHz}$ et nul à $118.75\,\text{GHz}$, la vapeur d'eau donne lieu à une absorption importante sur $22.2\,\text{GHz}$, sur $183\,\text{GHz}$ et sur $325\,\text{GHz}$. [20]

1.9 Diffusion des ondes radio

L'encombrement du spectre hertzien et le développement de nouveaux services de télécommunications conduit les opérateurs soient:

- A utiliser des fréquences de plus en plus élevées
- A utiliser dans une même bande de fréquence de deux polarisations orthogonales

Il est alors très important de prendre en compte les imperfections du canal de propagation. Au-dessus de 1GHz ce canal à plusieurs effets.

Le milieu atmosphérique est constitue de gaz qui ont des propriétés d'absorption particulières en fonction de la fréquence. Le milieu est aussi constitué de particules en suspension, ces dernières pouvant être des gouttes d'eau, des poussières, des grains de sable,... Etc.

Toutes ces particules ont pour effet d'atténuer l'onde électromagnétique mais aussi de la déphaser et de modifier sa pureté de polarisation. Tous ces effets sont regroupés sous le terme d'effets de diffusion.

1.9.1 Aspects macroscopiques

- Diffusion troposphérique

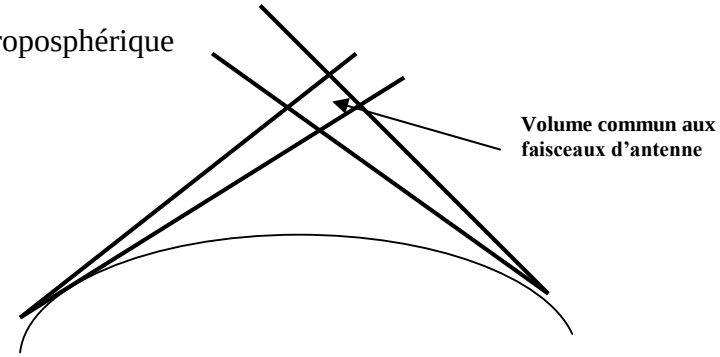


Figure. 1.1 : Diffusion troposphérique

Le niveau moyen reçu est lie principalement aux valeurs moyennes du gradient vertical de l'indice de réfraction dans le volume commun aux faisceaux des antennes.

1.10 Les milieux de propagation:

1.10.1 Les nuages

Constitués de plusieurs centaines de particules d'eau par cm^3, ils provoquent dans certaines gammes de fréquence des atténuations importantes sur les ondes radioélectriques. Les particules d'eau sont généralement de petite taille (diamètre<100 μm).

1.10.2 La pluie

La pluie est le phénomène le plus perturbant du point de vue de la propagation. Les gouttes d'eau sont en général considérées comme sphérique et leur dimension peut atteindre un diamètre de 2 mm. Elles ont pour effet d'atténuer, de diffuser et d'alterner la polarisation des ondes.

La pluie est décrite au moyen de la distribution des tailles des gouttes. On utilise en général la distribution de Marshall et palmer [20]:

$$N(r)=N_0 e^{-\alpha.r} \qquad (1.5)$$

N (dr) : est le nombre de gouttes d'eau par unité de volume dont le rayon est compris entre (r et dr + r). N0 est une constante expérimentale et α est aussi une constante expérimentale en mm^{-1}.

$nombre(r \le R \le r + dr)$

On prend en général: $N_0=16.10^{3} mm^{-1}$ et $\alpha=8,2R^{-0,21} mm^{-1}$

R représente l'intensité de pluie exprime en mm/heure.

Pour des fréquences entre 30 MHz et 1000 GHz et pour des températures de –4°c à +30°c, la permittivité relative de la pluie en fonction de la fréquence f s'écrit:

$$\varepsilon_r = \varepsilon_0 - \frac{\varepsilon_0 - \varepsilon_p}{f - if_p} f + \frac{\varepsilon_p - \varepsilon_s}{f - if_s} f \qquad (1.6)$$

Avec: ε_0=77. 6+103. 30, ε_p= 5. 48, ε_s=3.51

f_p= 20. 09-1420+294θ^2 ， f_s = 590-1500θ

$$\theta = \frac{300}{273,15+T} - 1 \qquad (1.7)$$

T: température en °c

L'atténuation subie par une onde traversant un rideau de pluie homogène est proportionnelle à la distance parcourue et peut-être caractérisée par une atténuation linéique. Il a été montré, par des calculs approches, que l'atténuation linéique « γ » en dB/km pouvait s'écrire en fonction de l'intensité de pluie R en mm/h par la relation:

$$\gamma = aR^b \qquad (1.8)$$

Les coefficients a et b dépendent de la fréquence et de polarisation.

1.10.3 Le sol

A chaque fois que les ondes électromagnétiques passent au voisinage du sol celui ci intervient sur la propagation. L'effet est particulièrement important dans le cas des liaisons terrestres dont l'ensemble du trajet est au voisinage du sol. Il est particulièrement important dans le cas des liaisons terrestres dont l'ensemble du trajet est au voisinage du sol. Il est aussi important pour les liaisons satellites pour la partie concernant la station terrienne. La caractéristique principale du sol est sa permittivité diélectrique « ε ». En général, on considère le sol comme non magnétique.

La permittivité dépend grandement du taux d'humidité du sol considéré.

Le sol intervient dans les études de propagation à travers deux phénomènes:

- La réflexion sur le sol
- La diffraction par le sol

1.10.4 Réflexion sur la le sol

Il a été vu, lors du paragraphe sur la réflexion, que des rayons réfléchis par le sol peuvent venir interférer avec l'onde directe. Il faut alors distinguer les réflexions diffusantes et les réflexions spéculaires. Pour que ces dernières, qui sont les plus significatives, aient lieu il faut que la surface plane réfléchissante couvre la première zone de Fresnel et que le trajet réfléchi ne soit pas affaibli par diffraction par le relief de la liaison.

1.10.5 La diffraction par le sol

La recherche des obstacles diffractant se fait également à partir du profil de la liaison. [20].

1.11 Les supports de transmission

1.11.1 Les fibres optiques

Les fibres optiques véhiculent des ondes électromagnétiques lumineuses ; en fait la présence d'une onde lumineuse correspond au transport d'un « 1 » et son absence au transport d'un « 0 » ; les signaux électriques sont transformes en signaux lumineux par des émetteurs ; les signaux lumineux sont transformes en impulsions électriques par des détecteurs...

1.11.2 Les faisceaux hertziens

Ils assurent une transmission radioélectrique avec les caractéristiques suivantes:

- Fréquence porteuse comprise entre 1 et 40 GHz .
- Utilisation d'antennes directives (Yagi, parabole).
- Liaison à vue directe.
- Antennes portées par des pylônes.
- Portée variant de 10 à 60 km.

1.11.3 Les câbles coaxiaux

Le câble coaxial est employé pour véhiculer des signaux hautes fréquences.

Il possède une bande passante élevée et une faible atténuation pour les fréquences <100 MHz . Au-delà de 100 MHz , l'atténuation devient plus importante et il faut prévoir des câbles coaxiaux hyperfréquences (1 à 20 GHz).

1.12 Utilisation des différentes gammes de fréquences

Une bonne manière de classifier les canaux de transmission est de les répertorier en fonction de la bande de fréquence dans laquelle ils sont exploitables.

Tableau. 1.1 : Utilisation des différentes gammes de fréquences.

Canaux guidés	
Paire torsadée (téléphone)	300 Hz – 300 KHz
Paire torsadée (ADSL)	26 KHz – 1 MHz
Câble coaxial (éther net)	300 KHz – 1 GHz
Guide d'onde	1 GHz – 300 GHz
Fibre optique	30 THz – 1000 THz
Canaux sans fil	
VLF	3 KHz – 30 KHz
LF	30 KHz – 300 *KHz*
MF	300 KHz – 3 MHz
HF	3 MHz – 30 MHz
VHF	30 MHz – 300 MHz
UHF	300 MHz – 3 GHz
SHF	3 GHz – 30 GHz
EHF	30 GHz – 300 GHz
Optique	30 THz – 1000 THz
Acoustique sous-marine	
ULF	150 Hz – 1, 5 KHz
LF	1, 5 KHz – 15 KHz
MF	15 KHz – 150 KHz
HF	150 KHz – 1, 5 MHz
VHF	1, 5 MHz – 15 MHz
UHF	15 MHz – 150 MHz
SHF	150 MHz – 1, 5 GHz

1.13 Les voies radioélectriques

Les transmissions de données par voies radioélectriques ne sont pas très fréquentes en dehors du domaine militaire. Elles posent des problèmes particuliers, difficiles qui limitent l'intérêt, en effet la propagation des ondes joue un rôle très important et le matériel de transmission doit être adapté avec beaucoup de soin à la voie.

1.14 Défauts des voies radio électriques

Nous allons maintenant étudier les principales imperfections des voies radioélectriques. Nous commencerons par le bruit de fond des équipements, puis les bruits atmosphériques, industriels, les défauts dus aux équipements et nous terminons par le fading. [46]

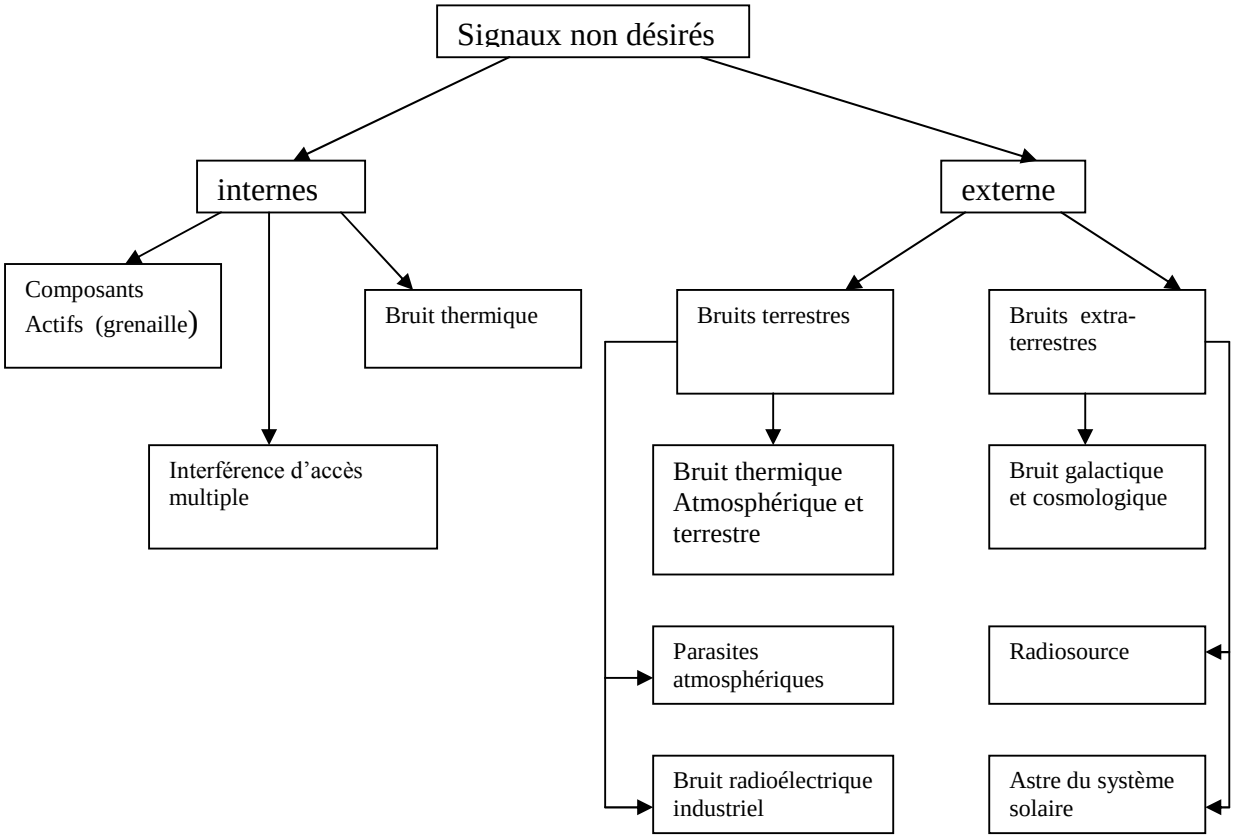


Figure.1.2 : Les sources physiques des signaux non désirés

1.14.1 Bruit de fond

Il est en général lie à la sensibilité de l'installation de réception. L'antenne de réception collecte un certain bruit thermique, les premiers étages de réception ont un facteur de bruit qui augmente ce bruit par rapport au signal.

En fait dans les liaisons radioélectriques, les performances sont rarement limitées par le bruit de font des récepteurs.

1.14.2 Bruits atmosphériques

Les voies radioélectriques peuvent être brouillées par des ondes créées à grandes distances par des orages ou d'autres phénomènes dus à l'ionosphère.

Ces ondes se manifestent par des impulsions en général très brèves et de haut niveau. La statistique de ces bruits est très différente de la loi de Poisson qui s'applique dans le cas d'un canal gaussien, et l'amplitude ne suit pas une loi normale.

1.14.3 Bruit blanc

D'autres sources de bruit ont les mêmes propriétés que le bruit thermique, à savoir une distribution gaussienne et une densité spectrale de puissance constante. On parle dans ce cas de bruit blanc par analogie à la lumière blanche qui contient toutes les couleurs. Un bruit blanc est caractérise par sa température équivalente de bruit t_n qui est similaire à la temperature en cas du bruit thermique.

1.14.4 Bruit en 1/f

Aux fréquences supérieures à quelques KHz, le bruit de fond des composants électriques ou electroniques est essentiellement blanc et dépend pratiquement uniquement de l'effet thermique et de l'effet grenaille. Aux fréquences inférieures, on observe toute fois que la densité spectrale « DSP » croit en fonction inverse de la fréquence. On constate expérimentalement la relation suivante:

$$G_n(f)=\frac{\text{constante}}{\left|f^{\alpha}\right|^2} \qquad \text{Avec } \langle 0\alpha\langle 2 \quad [v^2/Hz] \tag{1. 12}$$

1.14.5 Bruits industriels et brouillage

Une source importante de difficultés provient des parasites industriels, ces bruits sont peu importants lorsque la fréquence dépasse quelque méga hertz.

1.14.6 Le fading

Le fading est un défaut typique des voies radioélectriques, il est dû aux chemins multiples que peuvent suivre les ondes radio entre l'émetteur et le récepteur. Ces chemins multiples sont occasionnés par les réflexions sur l'ionosphère et la terre, ce défaut est surtout marqué en HF ou on utilise beaucoup la réflexion ionosphérique.

Le résultat du fading en transmission de données est d'entraîner une interférence entre les symboles successifs si les vitesses de transmission sont élevées (voir IES).

1.15 Influence du bruit sur la transmission des signaux binaires

Nous allons maintenant aborder le problème essentiel de l'étude des signaux en transmission des données, c'est celui d'erreur minimum que l'on peut obtenir par un traitement optimum des signaux.

Dans les problèmes de transmission on appelle bruit toutes les perturbations qui affectent la voie de transmission bien que l'origine et les caractéristiques des phénomènes puissent être très différents.

Ce qui caractérise fondamentalement le bruit c'est qu'il est inconnu, on ne peut absolument pas prédire la puissance du bruit à un instant future t où on veut émettre un signal x.

1.15.1 Perturbations du signal

Un canal de transmission dégrade inévitablement les signaux qu'il transmet en y provoquant des perturbations qu'on peut classer en deux catégories.

1.15.1.1 Les perturbations indépendantes du signal

Leurs caractéristiques (amplitude, spectre, statistique) ne sont pas liées au signal lui-même, mais seulement au canal. Elles apparaissent même s'il n'y pas de signal utile. Les principales sont:

- le bruit de fond : les perturbations électromagnétiques
- la diaphonie (perturbation par d'autres signaux par couplages inductifs et capacitifs)

Le bruit de fond est difficilement réduit. Les perturbations E/M et la diaphonie peuvent être minimisées par un câblage et/ou un blindage approprie.

1.15.1.2 Les perturbations dépendantes du signal et du canal

Ces perturbations sont présentes seulement si le signal est aussi présent. Ces perturbations varient en fonction des caractéristiques du signal: amplitude, spectre, etc.

- La distorsion (d'amplitude et de phase).
- Le bruit d'inter modulation.
- L'écho.
- Le bruit de quantification (approximations de codage).

CHAPITRE 2
THEORIE D'INFORMATION

2.1 Introduction

La théorie de l'information est née dans un contexte bien particulier, celui de la théorie statistique des communications. La première tentative de définition de la « quantité d'information » remonte à 1928:l'Américain « Hartley » suggéra que « de l'information » apparaisse au cours de sélection successif de symboles distincts

Mais ce n'est qu'à partir de 1948, grâce aux travaux de Shannon, que la théorie de l'information a pris sa forme actuelle.

L'américain C. Shannon, dans deux articles désormais classiques [2], introduisit le nouveau concept de quantité d'information de façon mathématique et en déduit les principales conséquences.

Lorsqu'on parle de codage de source et de codage de canal, on pense naturellement au nom de Shannon, qui a donné les limites fondamentales pour ces deux problèmes ; on pense aussi au fait que les deux domaines sont, depuis des décennies, bien distincts: deux communautés différentes, avec chacune ses propres méthodes, problématiques, conférences et revues.

En fait, on peut affirmer que c'est précisément Shannon qui a provoqué cette séparation dans les années cinquante, à cause de son « théorème de séparation ».

2.2 Nature des informations transmises

La nature des informations échangées peut être très variée:

- Parole humaine;
- Données alphanumériques, textes et autres données structurées en un ensemble de caractères. Images fixes en noir et blanc ou en couleur ;
- Images animées, images de télévision par exemple ;
- Informations multimédia qui intègrent plusieurs moyens de représentation de l'information ;

2.3 Définition à la théorie de l'information

Donner une définition précise et complète de la théorie de l'information est une tache difficile. Pour simplifier on peut énoncer l'assertion suivante; la théorie de l'information est une discipline fondamentale qui s'applique dans le domaine des communications.

Son objectif consiste d'une part à déterminer les limites imposées par les lois de la nature lorsqu'on doit stocker ou transmettre le contenu d'une source (d'information), d'autre part à proposer des dispositifs permettant d'atteindre ou d'approcher ces limites. La théorie de l'information ne cesse de se développer car les exigences actuelles s'orientent vers une augmentation constante de l'information à stocker ou à transmettre.

2.4 Quelques rappels sur la théorie de l'information

En pratique, pour s'assurer de l'efficacité et de la fiabilité d'un système les opérateurs s'attardent principalement sur deux paramètres : la capacité du canal, qui doit être aussi élevée que possible, et le taux d'erreurs « TEB » que l'on cherche à minimiser. Mais avant de pouvoir appréhender ces deux paramètres, quelques rappels de la théorie de l'information, développée principalement par C. Shannon, sont nécessaires.

Pour cela, introduisons une variable aléatoire x de densité de probabilité p(x). On définit la quantité d'information liée à la réalisation de l'avènement x comme entropie.

2.4.1 Quantité d'information « entropie »

On considère une source s qui produit des mots aléatoires indépendants les uns des autres et qui peuvent prendre k valeurs possibles m_k avec pour chacun d'entre eux une probabilité $p(m)$ avec $k=(1,.....K)$.

On définit la quantité d'information liée au mot m comme :

$$I(m)=-\log_2 [p(m)] \qquad (2.1)$$

C'est une quantité positive ou nulle. Elle montre la diminution de l'incertitude apportée par la réalisation d'un avènement m (l'occurrence d'un avènement peu probable est plus informative que l'occurrence d'un évènement probable). A un évènement certain correspond une quantité d'information nulle. L'entropie « notion définie au départ par les spécialistes de la thermodynamique, comme Clausius qui a inventé ce concept et Boltzmann qui a établi le lien avec la théorie des probabilités », est la moyenne de la quantité d'information :

$$h(s)=-\sum_k p(m_k)\ \log_2\ [p(m_k)] \tag{2.2}$$

Les notions utilisées sont fondées sur les probabilités. Ici, on s'intéresse plus particulièrement aux probabilités conditionnelles, en particulier la probabilité que le mot « A entrée » émis sachant que c'est le mot « B » qui a été reçu. Nous supposerons que la source émet des messages x qui prennent une des valeurs possibles A_k avec (k=1.....,K) avec une probabilité P(A_k). Le récepteur reçoit des messages y qui prennent une des valeurs possibles.

B_l avec (l=.1.....L) avec une probabilité p(B_l).

La probabilité d'avoir émis A_k et reçu B_l est p(A_k , B_l).

La probabilité conditionnelle d'avoir émis A_k et reçu B_l est :

$$p(A_k/B_l)=\frac{p(A_k,B_l)}{p(B_l)} \tag{2.3}$$

2.4.2 Entropie conjointe

On appelle entropie conjointe de X et Y l'espérance :

$$H(X,Y)=-\sum_{k,l} p(A_k,B_l)\log_2 p(A_k,B_l) \tag{2.4}$$

L'entropie conditionnelle relativement à la valeur de Y est :

$$H(X/Y=B_l)=-\sum_k p(A_k/B_l)\log_2 p(A_k/B_l) \tag{2.5}$$

L'entropie conditionnelle de X connaissant Y est :

$$H(X/Y)=-\sum_l p(B_l)H(X/Y=B_l) \tag{2.6}$$

Appelée aussi ``équivoque'', qu'on peut aussi écrire :

$$H(X/Y)=-\sum_{k,l} p(A_k,B_k)\log_2 \frac{p(A_k,B_l)}{\sum_k p(A_k,B_l)} \tag{2.7}$$

Si h(X) caractérise l'incertitude sur X , h(X/Y) caractérise l'incertitude sur X lorsqu'on a Y comme entrée, on a les propretés suivantes :

$$H(X,Y)=H(Y)+H(X/Y) \tag{2.8}$$

$$H(X)\geq H(X/Y) \tag{2.9}$$

Qui signifie que l'incertitude sur « X » est plus faible une fois qu'on connaît « Y ». Il y a égalité si « X » est indépendant de « Y » : alors la mesure de « Y » n'apporte aucune information sur « X ». C'est le cas lorsque le canal de transmission est si bruité qu'il ne permet pas de mesurer la moindre information utile sur « X ». [6], [24].

2.5 Premier théorème de Shannon

On suppose que la source émet un mot par unité de temps. « C. Shannon » a montré qu'il est possible de trouver un codage des données de manière à réduire le débit de transmission. On peut par exemple calculer l'entropie d'une source qui émet le mot « 0 » avec la probabilité « p » et le mot « 1 »avec la probabilité « 1-p ».

$$H(p)=-p\log_2 p-(1-p)\log_2(1-p) \qquad (2.\ 10)$$

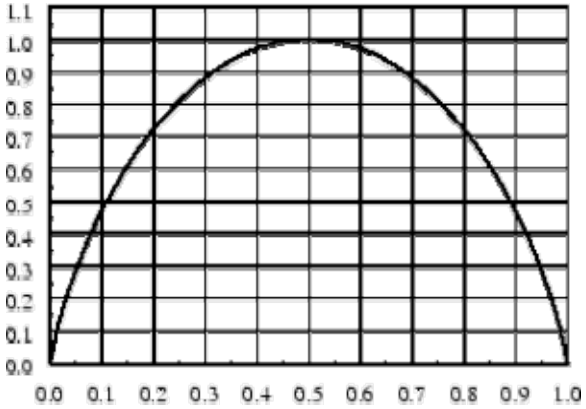


Figure.2.1 : Entropie d'une source émettant deux symboles avec la probabilité p et 1-p

On voit sur la figure (2.1) [4] que l'entropie est maximum et vaut « 1 » pour p = 0.5. Dans ce cas on ne peut pas réduire le débit de la source. D'après le premier théorème de Shannon, la réduction est possible lorsque p est proche de « zéro » ou de « un ». Par exemple lorsque p = 0. 1, on peut réduire la longueur des messages de moitié.

2.6 Efficacité d'un code

Si une source a une entropie « h » et qu'on code les mots émis par cette source sous la forme de « k » séquences de longueur : « l(k) ». Chaque mot à la probabilité p(k) la longueur moyenne des messages correspondant à l'émission d'un mot sera :

$$e(l)=\sum_k p(k)l(k) \quad \text{Avec } k=(1.....K) \qquad (2.\ 11)$$

Et l'efficacité du code est égale à : $\eta=\frac{h}{e(l)}$

2.7 Codage d'une source

La compression est l'action utilisée pour réduire la taille physique d'un bloc d'information.

En compressant des données, on peut placer plus d'informations dans le même espace de stockage ou utiliser moins de temps pour le transfert au travers d'un réseau.

L'information à transmettre ou à stocker, modélisée par le processus aléatoire $x(n)$, prend ses valeurs dans un ensemble fini, l'alphabet d'entrée : A_k, et on désire représenter (coder) les différents éléments de cet ensemble de façon adaptée aux caractéristiques du canal de transmission et de façon efficace.

- De façon adaptée aux caractéristiques du canal de transmission veut dire que la représentation de chaque symbole d'entrée, un mot du code, peut être construit à partir d'éléments d'un autre alphabet, adapté au canal. On supposera par la suite que cet alphabet est composé de deux éléments $A_c = (a^1, a^2)$, par exemple les deux symboles binaires habituels 0 et 1.
- De façon efficace veut dire que l'on cherche à représenter la source en utilisant le minimum de bits, c'est à dire en minimisant la longueur moyenne des mots du code.

2.8 Compression

La compression a pour but la réduction du volume des informations ; cette réduction peut être effectuée :

- Sans perte d'informations (réduction de la redondance), permettant de reconstituer de façon exacte le fichier.
- Avec perte d'informations, utilisée principalement pour les images et les sons, permettant de reconstituer de façon approximative le fichier original.

2.9 Le codage de HUFFMAN

Le codage d'entropie est une méthode de compression « statistique » de données qui permet de réduire la longueur du codage d'un alphabet. Il substitue à un code de longueur fixe un code de longueur variable. [6] [25]

2.9.1 L'algorithme

- Evaluer les fréquences d'occurrence des symboles du fichier.
- Classer les symboles en ordre décroissant des fréquences d'apparition.

- Regrouper de façon séquentielle les paires de symboles de plus faible probabilité, en reclassant symboles et groupes si nécessaires.
- Calculer les codes avec retour en arrière en ajoutant, dans chaque point de regroupement, un « 0 » a une branche et un « 1 » a l'autre branche.

2.9.2 Exemple d'algorithme /logique de Huffman

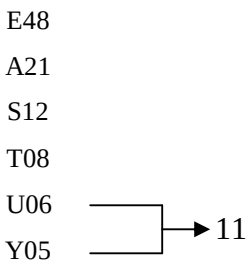
- Lecture complète du fichier et création de la table des symboles.

E	0.48
A	0.21
S	0.12
T	0.08
U	0.06
Y	0.05

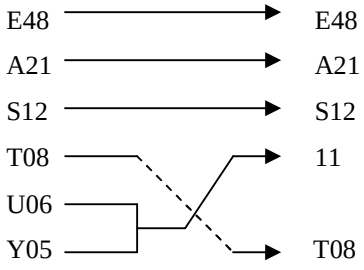
- Classement des symboles par ordre des fréquences décroissantes.

E48
A21
S12
T08
U06
Y05

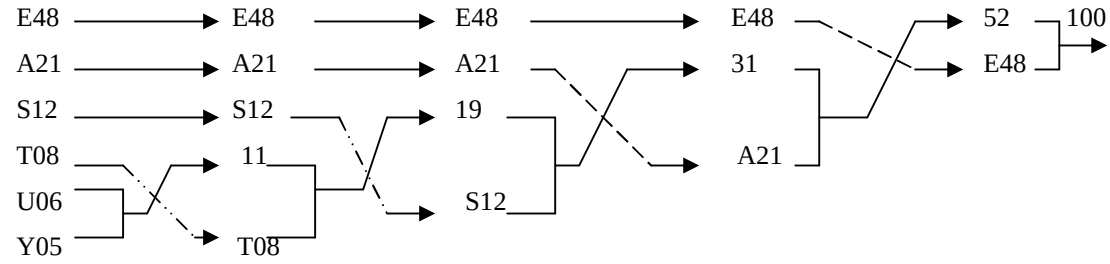
- Réductions successives en rassemblant en une nouvelle occurrence les 2 occurrences de plus petites fréquences.



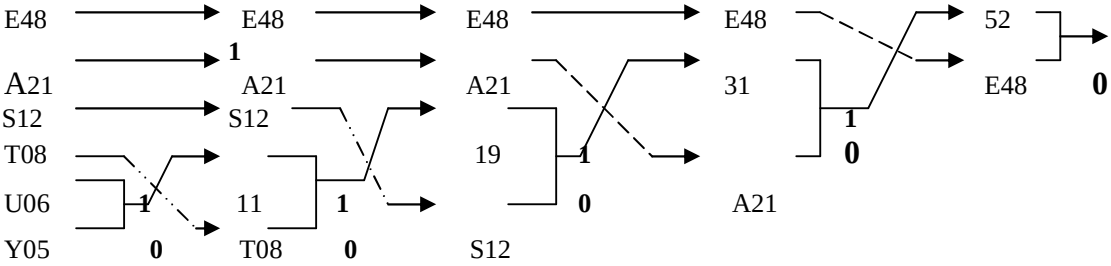
- La nouvelle occurrence obtenue est insérée dans la table et celle-ci à nouveau trié par ordre de croissant.



- Les réductions se poursuivent jusqu'a ce qu'il n'y ait plus d'élément et construction de l'arbre binaire en reliant chaque occurrence à la racine.



- Le codage consiste à lire l'arbre du sommet aux feuilles en attribuant par exemple la valeur 0 aux branches basses et 1 aux branches hautes.



- Et voici le résultat du codage de Hauffman:

E	0
A	10
S	110
T	1110
U	11111
Y	11110

2.10 Codage du canal

Le canal de transmission est le support physique utilisé pour envoyer l'information de l'émetteur au récepteur, et il diffère selon le type d'application envisagée.

2.10.1 Canal de transmission idéalisé

Un canal est discret si les deux alphabets x et y sont discrets nous avons considéré jusqu'ici que le canal pouvait transmettre tous les m symboles de l'alphabet x de la source, ce qui en général n'est pas le cas. Supposons que l'alphabet du canal, note *z*, est composée de d symboles, avec d < m. Il faut alors intercaler un codeur entre la source et le canal, codeur qui fera correspondre de façon biunivoque à chaque message x_k émis par la source une séquence Z_K de longueur n_k de symboles appartenant à *z*.

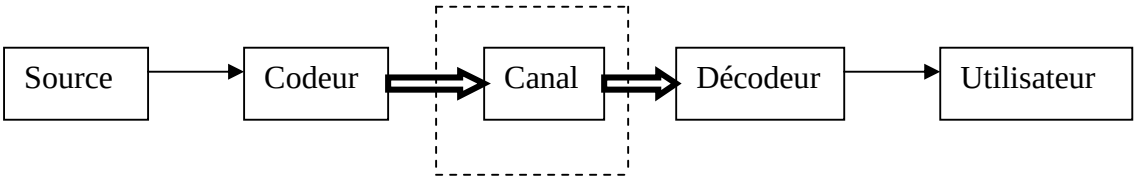


Figure.2.2 : Codage canal

Nous avons ainsi adapté la source au canal. Soit *n* la longueur moyenne des séquences :

$$\overline{n} = \sum_{k=1}^{M} n_k \cdot p(x_k) \qquad (2\ 13)$$

Dans le cas d'un canal idéal, nous désirons trouver un codeur qui assure une valeur minimale pour $\overline{n}$.

L'entropie de la source est h(t), qui sera aussi l'entropie du codeur par messages ; l'entropie du codeur par symboles sera: $\frac{H(X)}{\overline{n}}$

L'entropie maximale du codeur est $\log_2$ d, donc l'efficacité du codeur est :

$$E = \frac{\frac{H(X)}{\overline{n}}}{\log_2 D} \qquad \text{Et} \qquad E\langle 1$$

Le principe de base du codage de canal consiste à remplacer le message à transmettre par un message plus long qui contient de la redondance. Sans redondance, chaque donnée du message est indispensable à la compréhension du message entier. Toute erreur dans une partie du message est donc susceptible de changer la signification du message. L'objectif de la redondance est de faire en sorte que les erreurs ne compromettent pas la compréhension globale du message.

Du fait de l'adjonction d'une redondance, le message effectivement transmis est plus long. Un code se caractérise par son rendement R. Si le codeur génère n bits à partir de k bits d'information, le rendement R vaut k/n.

Les données générées par le codeur sont appelées des symboles. Lors du décodage, les symboles reçus peuvent être des bits ou des mots binaires. Dans le premier cas, le système est dit à décision dure, dans le second à décision douce. Un système à décision douce présente de meilleures performances qu'un système à décision dure, mais au détriment d'une complexité plus grande du décodeur de Viterbi.

2.10.2 Capacité d'un canal

L'information apportée sur X par la mesure Y est la ``transformation".

$$I(X,Y)=h(X)-h(X/Y) \qquad (2.14)$$

Si la connaissance de « X » est équivalente à la connaissance de « Y » (pas d'erreurs de transmission), et on aura : $I(X/Y)=h(X)$

Par exemple dans le cas d'un canal binaire symétrique sans mémoire de la figure (2.11), où « X »prend les valeurs « 0 » et « 1 »et où « Y » prend la valeur de « x » avec les probabilités $(1-p)$ « pas d'erreur de transmission » et la valeur complémentaire avec la probabilité (p) « erreur de transmission », On a:

$$I(X,Y)=h(X)+p\log_2 p+(1-p)\log_2(1-p) \qquad (2.15)$$

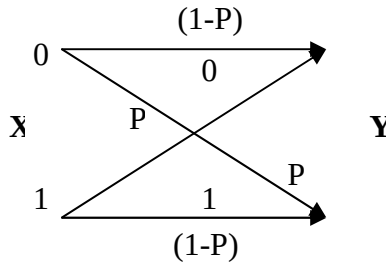


Figure.2.3 : Canal binaire symétrique

La capacité du canal de transmission est le maximum de $I(X,Y)$ pour toutes sources possibles x.

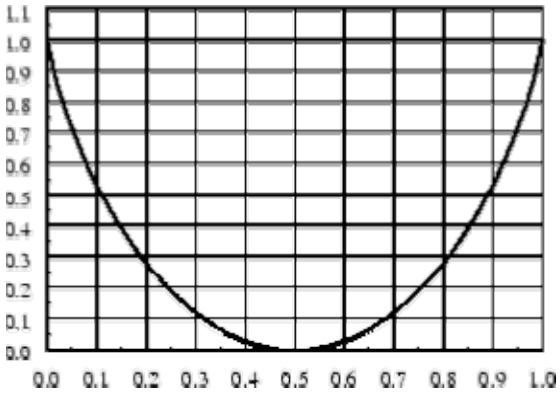


Figure.2.4 : Capacité d'un canal obtenue lorsque les deux valeurs de x (0 et 1) sont équiprobables en fonction de la probabilité d'erreur

On remarquera que la capacité du canal est maximum lorsqu'il n'y a pas d'erreur de transmission (p=0) mais aussi lorsque le canal remplace systématiquement la donnée par son complémentaire (p=1). Il est alors possible de reconstituer le message simplement. La

capacité est nulle lorsque p=0. 5, c'est à dire lorsque la donnée a une chance sur deux d'être erronée. Dans ce cas la donnée reçue est indépendante de la donnée émise.

2.11 Deuxième théorème de Shannon

On considère une source S d'entropie $h_\infty(s)$ délivrant ses symboles au débit : D_s, *et* un canal de capacité par symbole C a un débit : D_c. [6], et le débit d'entropie est $h=h_\infty(s)\times D_c$.

$\forall\varepsilon>0$ il existe un code pour transmettre le contenu de la source sur le canal tel que p{erreur après décodage}<ε.

En d'autres termes, cela signifie que si le débit d'entropie d'une source est inférieur à la capacité par unité de temps d'un canal, alors on peut transmettre le contenu de la source sur le canal avec une probabilité d'erreur aussi petite que souhaitée.

A posteriori, ce théorème donne tout son sens à la notion de capacité. Définie initialement comme une quantité d'information susceptible d'être fournie, la capacité apparaît comme une aptitude à transmettre de l'information.

Soit un canal de capacité « C » transmettant « S » symbole par unité de temps d'une source x d'entropie h(X) dont le débit est un mot par unité de temps. Shannon a montré qu'il existe une méthode de codage qui garantit une transmission quasi parfaite (probabilité d'erreur arbitrairement faible) si :

$$h(X) \langle S{\cdot}C \qquad (2.16)$$

On peut interpréter ce résultat de la manière suivante: si un canal de transmission génère des erreurs de transmission, il est tout de même possible de trouver une manière de coder les messages émis en leur rajoutant suffisamment de redondance de sorte qu'on puisse retrouver le message émis sans erreur.

2.12 Canaux de transmission

2.12.1 Canal binaire symétrique

Le canal binaire symétrique (CBS) est un canal discret dont les alphabets d'entrée et de sortie sont finis et égaux. On considère dans ce cas que le canal comprend tous les éléments de la chaîne compris entre le codeur de canal et le décodeur correspondant (Fig. 2.5).

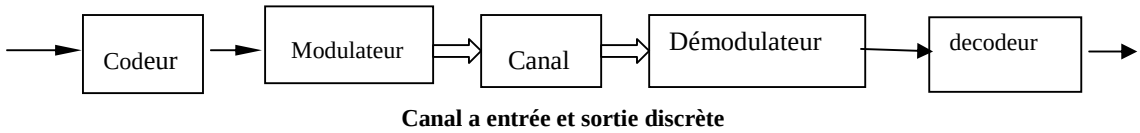


Figure.2.5 : Description d'un canal binaire symétrique

2.12.2 Canal à bruit additif blanc gaussien (BBAG)

Le modèle de canal le plus fréquemment utilisé pour la simulation de transmissions numériques, qui est aussi un des plus faciles à générer et a analyser, est le canal à bruit blanc additif gaussien (BBAG). Ce bruit modélise à la fois les bruits d'origine interne (bruit thermique dû aux imperfections des équipements...) et le bruit d'origine externe (bruit d'antenne...). Ce modèle est toutefois plutôt associe à une transmission filaire, puisqu'il représente une transmission quasi-parfaite de l'émetteur au récepteur. Le signal reçu s'écrit alors: $r(t)=s(t)+v(t)$

Où v(t) représente le BBAG, caractérisé par un processus aléatoire gaussien de moyenne nulle, de variance :σ_v^2 et de densité spectrale de puissance bilatérale : $\varphi_{XY}=\frac{n_0}{2}$. La densité de probabilité conditionnelle de « r » est donnée par l'expression: [11]

$$p(r/s)=\frac{1}{\sqrt{2\pi\sigma_v}}e^{\frac{-(r-s)^2}{2\sigma_v^2}} \qquad (2.17)$$

2.12.3 Canal à évanouissements

Les communications radio ont souvent besoin d'un modèle plus élaboré prenant en compte les différences de propagation du milieu, appelées encore atténuations ou évanouissements, qui affectent la puissance du signal.

Cette atténuation du signal est principalement due à un environnement de propagation riche en échos et donc caractérisé par de nombreux multi trajets, mais aussi au mouvement relatif de l'émetteur et du récepteur entraînant des variations temporelles du canal. Le phénomène de multi- trajets s'observe lorsque l'onde électromagnétique portant le signal modulé se propage par plusieurs chemins de l'émetteur au récepteur.

2.13 Les choix des codes

- Problèmes pouvant se poser lors du cheminement d'une information sur une ligne de télécommunication ou dans un ordinateur:
    - Validité de l'information à l'arrivée: il faut pouvoir vérifier que l'information reçue est bien l'information qui avait été émise.

- Correction d'une erreur éventuelle.

- Pour cela, on utilise des codes qui possèdent un nombre de bits supérieur à celui strictement nécessaire pour transmettre l'information. Ces bits permettent de contrôler la validité de l'information reçue.
- Deux types de codes dits redondants (ayant plus de bits que strictement nécessaires):
  - Codes auto vérificateurs*:* les bits supplémentaires permettent de détecter d'éventuelles erreurs de transmission,
  - Codes auto correcteur*:* les bits supplémentaires permettent de détecter et de corriger d'éventuelles erreurs de transmission,

2.14 Classification des codes

Il y a deux grandes familles de code :

2.14.1 Le codage en bloc

Le message décomposé en blocs de k bits, est remplacé par un bloc de n bits comprenant directement les k bits d'information et n-k bits de redondance calculés à partir des bits d'information, le codage d'un bloc se faisant indépendamment des précédents.

2.14.2 Les codes en treillis

La figure (2.14) donne un simple résumé de la grande famille de codage. Dans la première classe à droite de la figure, citons les codes les plus célèbres comme les codes BCH, Reed Solomon, Goppa, Golay et Hamming. La deuxième classe à gauche de la même figure est moins riche en variété, mais présente beaucoup plus de souplesse surtout dans le choix des paramètres et des algorithmes de codage disponible. Une troisième classe dite codes concaténés est obtenue par concaténation série, parallèle ou hybride de codes convolutifs et de codes en blocs. Ainsi, les turbo-codes classiques sont construits par concaténation parallèle de codes convolutifs récursifs. Les codes dits produits sont le résultat de la concaténation de deux codes en blocs.

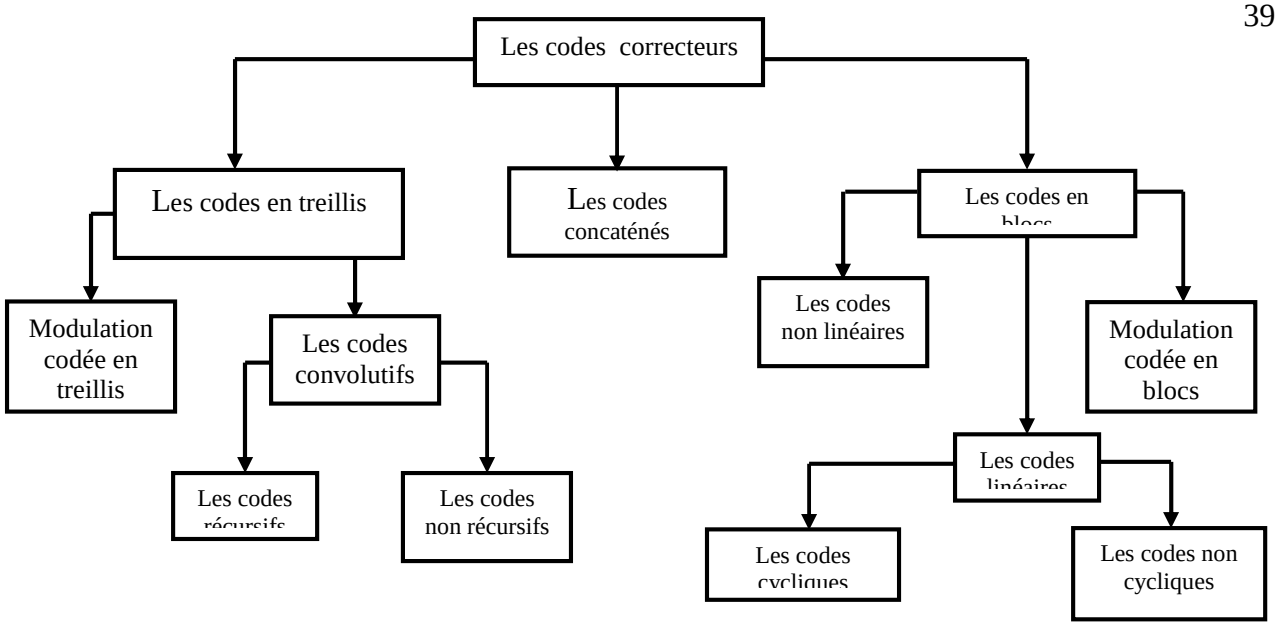


Figure.2.6 : La famille des codes correcteurs

2.14.3 Codes détecteurs

Le plus simple code détecteur d'erreurs est le contrôle de parité :

- Cela revient à ajouter un bit qui prend une valeur telle qu'il y ait un nombre pair de 1 dans l'information finale.
- Technique utilisée si le taux d'erreur est faible (< à 10^{-9}) car il est nécessaire de retransmettre une information erronée (perte de temps si erreur fréquente).
- Type de contrôle utilise dans les PC, au niveau entrée/sortie et en interne.
- Sur le même principe, on peut également réaliser un test d'imparité.

2.14.4 Codes correcteurs d'erreurs

Mettre en œuvre un code correcteur consiste à introduire une redondance dans l'information à transmettre. Ceci permet de détecter et éventuellement de corriger les cas ou la transmission a modifie le message. Il peut sembler paradoxal de compresser un fichier pour éliminer toute redondance puis d'en réintroduire. Un code correcteur est en fait une redondance réfléchie et optimisée pour minimiser le taux d'erreurs non détectées et la longueur des bits ajoutes. [35]

2.14.4.1 Double parité/double impartie

- Utilise quand l'information sous forme matricielle (tableau à deux dimensions), ce qui est le cas pour les bandes magnétiques,

2.14.4.2 Code de Hamming

- S'utilise quand l'information est vectorielle (sous forme d'une liste de bits),
- Fondé sur plusieurs tests de partie à des positions bien déterminées dans l'information,

- On rajoute aux m bits de l'information initiale k bits dits de parité. On a donc une information finale de n = m + k bits.
- Les k bits doivent permettre de coder les n positions possibles de l'erreur, ainsi que le fait (plus probable) qu'il n'y ait pas d'erreur → n+1 possibilités à coder,
- K doit donc être tel que:

  $2^k \geq n + 1 = m + k + 1$

  Soit: $m \leq 2^k - (k+1)$

2.14.5 Code convolutif(algorithme de Viterbi)

L'algorithme de Viterbi, de Andrew Viterbi, permet de corriger les erreurs survenues lors d'une transmission numérique (dans une certaine mesure). Il utilise la distance de Hamming afin de faire ressortir la plus faible métrique entre les différentes valeurs probables, utiliser l'algorithme de Viterbi double la taille de l'information envoyée mais à l'avantage de pouvoir corriger un nombre important d'erreurs.

Celui-ci s'appuie sur le schéma en treillis. Le principe est de chercher une séquence sans erreur la plus proche de celle reçue (et donc la plus probable). On recherche donc une trame qui ait la distance la plus petite avec celle reçue.

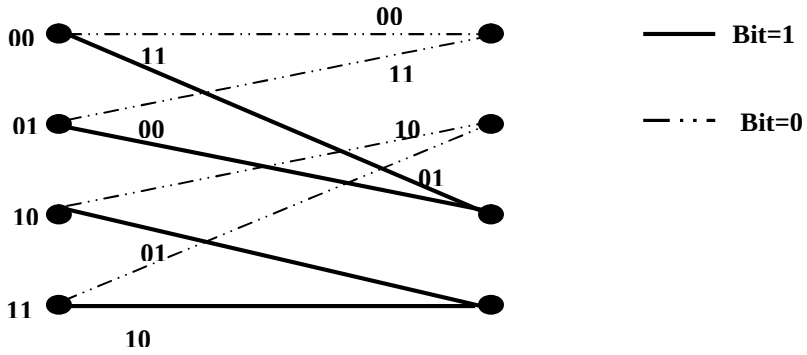
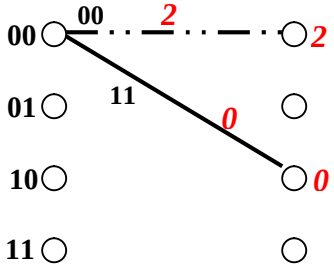


Figure.2.7 : Schéma de treillis

Les étapes : *1ere étape*

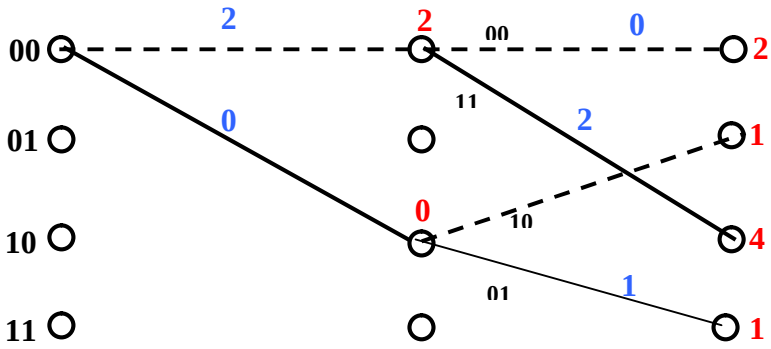
On part de l'état 00.

- On trace toutes les branches possibles à partir de cet état.
- Pour chacune de ces branches, on calcule la distance entre la valeur de la branche et le code reçu (c1).
- On affecte à l'état d'arrivée le poids de la branche rattachée.



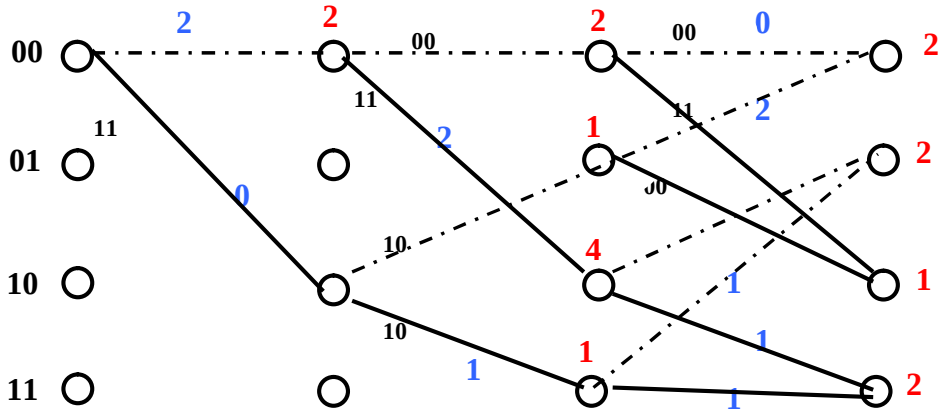
2eme étape.

- A partir des états d'arrivée précédents.
- On trace toutes les branches possibles.
- Comme à l'étape 1, o calcule la distance entre les valeurs des branches et le code reçu (c2).
- Pour chaque état d'arrivée, on effectue la somme entre le poids de la branche et le poids de l'état d'origine.



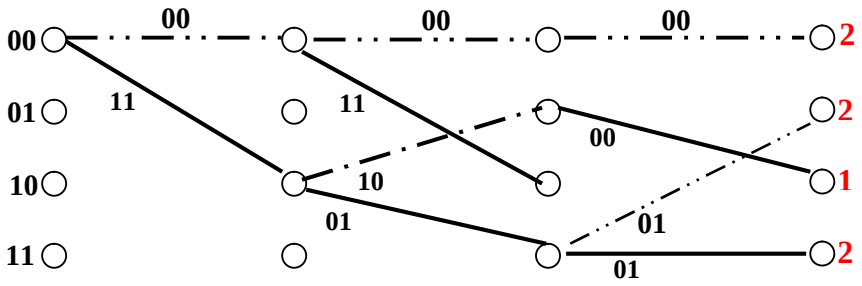
3eme étape

- A partir des états d'arrivée précédents.
- on trace toutes les branches possibles.
- Comme aux étapes précédentes, on calcule la distance entre les valeurs des branches et le code reçu (c3).
- Pour chacune des branches arrivant à un état, on effectue la somme entre le poids de la branche et le poids de l'état d'origine.
- On affecte le résultat le plus petit à l'état d'arrivée.



4eme étape

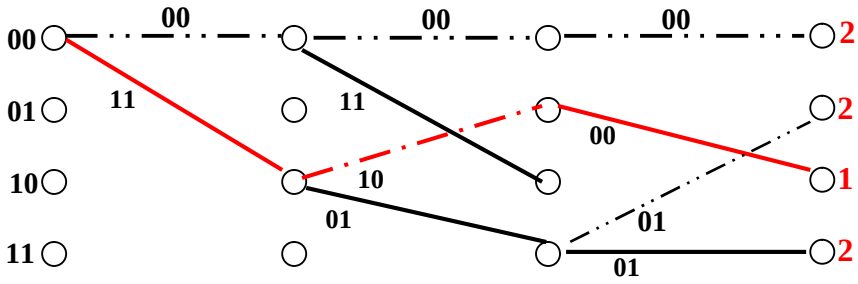
- Une fois ce travail effectue, pour chaque état d'arrivée, on ne garde que la branche qui a permis l'affectation du poids de cet état (c'est à dire celle qui a la somme entre son poids et le poids de l'état d'origine la plus petite).



5eme étape

A cette étape, on regarde les poids d'arrivée, il y a deux cas :

- 1er cas: le poids minimal des états d'arrivée n'est affecté qu'à un seul état. Dans ce cas le décodage peut avoir lieu. Le message est la suite des valeurs des branches (0 ou 1) du seul chemin possible pour atteindre cet état à partir de l'état initial.
- 2eme cas: le poids minimal des états d'arrivée est affecte a plusieurs états. Dans ce cas, le décodage aura lieu lors des étapes suivantes.



6eme étape:

Reprendre à l'étape 3 jusqu'au décodage complet du code.

2.15 Performance et améliorations

2.15.1 Distance libre

Un paramètre important d'un code convolutionnel est sa distance libre. En effet il détermine les performances d'un codage en fonction de la vraisemblance des différentes possibilités de son décodage.

La capacité de correction du code est déterminée par la distance de Hamming entre les différents chemins.

La distance libre est la distance minimale entre deux chemins différents du treillis partant d'un état donne jusqu'à l'obtention à nouveau de ce même état.

On calcule ainsi les poids respectifs de ce trajet. Plus la distance libre est élevée, plus le code sera performant.

La distance libre de notre exemple de treillis est égale à 5.

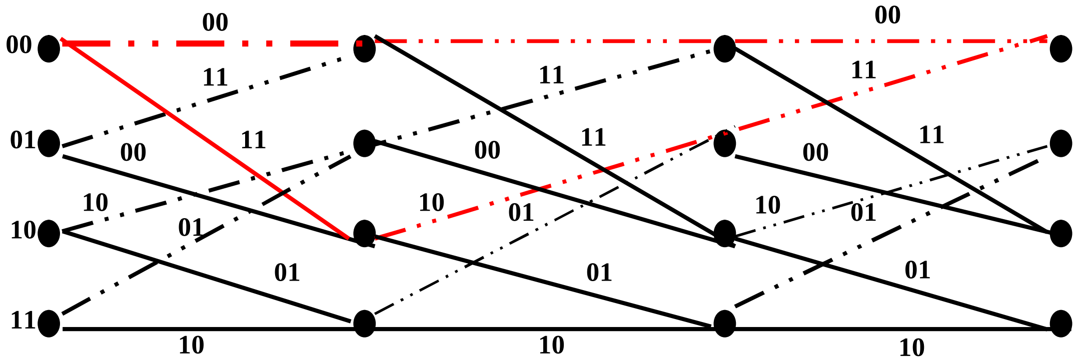


Figure.2.8 : Schéma de codage de viterbi

2.15.2 Rendement

Du fait qu'une redondance a été rajoute, le message alors transmis est plus long. Un codage convolutionnel se caractériser par son rendement R:

$$R=\frac{\text{nombre debits d'information}}{\text{nombre debits du code transmis}} \tag{2.18}$$

Le rendement de notre code convolutionnel utilisé est de 1/2, soit pour 1 bit d'entrée, on obtient 2 bits de sortie.

Contrairement aux codes en bloc (rendement élevé > 0, 9), ce type de rendement est très faible. Le débit après codage est multiplié par deux, ce qui ne peut être satisfaisant dans certaines transmissions. Aussi, il existe des techniques qui permettent d'améliorer cette insuffisance de rendement telles que le poinçonnage.

2.16 Poinçonnage

Le rendement des codes convolutionnels est de la forme 1/n.

Il est extrêmement rare de mettre en place des codes convolutionnels de rendement inférieur à 1/2.Tel quel le rendement ne peut être supérieur à :1/2.

Pour en obtenir un meilleur code, il faut utiliser la technique du poinçonnage.

Le principe est de supprimer périodiquement un bit de sortie. Par exemple si on supprime un bit tous les quatre bits, le rendement deviendra donc 2/3.

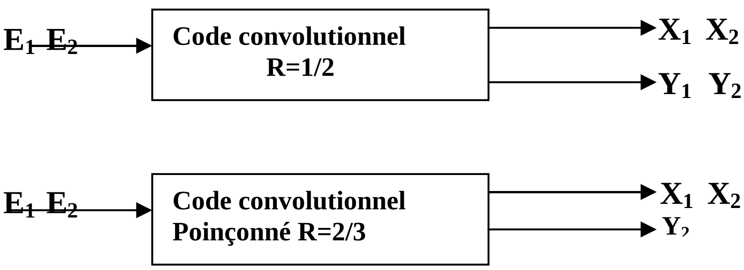


Figure. 2.9 : Poinçonnage

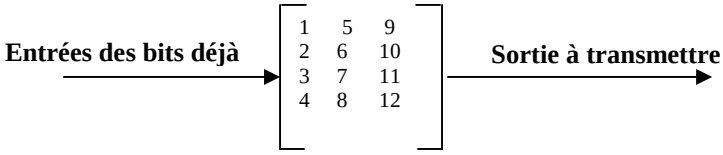
De même, on peut construire un code de rendement 7/8. (7 bits en entrée, 14 en sortie et 8 bits seulement transmis).

Le poinçonnage crée bien évidemment des erreurs puisque tous les bits ne sont pas transmis. Pour le décodage via Viterbi, on remplacera ces bits ignores par des zéros.

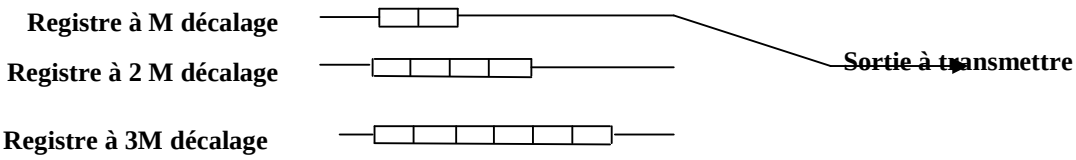
2.17 Entrelacement

Pour diminuer les rafales d'erreurs, on peut effectuer un entrelacement temporel. Il suffit de modifier l'ordre des codes et de les remettre dans le bon ordre avant le décodage. Il existe deux types:

- L'entrelacement en bloc



- L'entrelacement convolutionnel.



➢ Les avantages:

- Capable de coder une infinité de symboles d'information
- Correction de plusieurs erreurs isolées et en paquet d'erreur si l'entrelacement est utilisé.
- Facilite de décodage (algorithme de viterbi)

➢ Les inconvénients:

- Faible rendement
- Nécessite beaucoup de mémoire (registre à décalage)
- Doit être entrelace ou concaténé avec un autre code pour être efficace à la correction des rafales d'erreurs.

2.18 Conclusion

Le code convolutionnel est utilisé de plus en plus dans les nouvelles technologies (GSM, télévision numérique, transmission satellite et terrestre, audio de la compression MPEG-4…).

L'utilisation des codes convolutionnels en association avec les codes cycliques est fréquente, et son efficacité peut être considérablement améliorée par les turbo codes.

CHAPITRE 3
TRANSMISSION NUMERIQUE

3.1 Introduction

Historiquement, la transmission analogique a dominé l'industrie des télécommunications. En analogique, les signaux sont transmis sous forme de tensions électriques d'amplitude variable. Aujourd'hui, les ordinateurs sont présents dans la plupart des réseaux de télécommunications, ce qui conduit à de profond changement des techniques de transmission, qui évoluent vers la transmission numérique.

Un message ne peut pas être envoyer directement sur le canal de transmission car, d'une part, les fréquences des canaux et des messages ne coïncident pas forcement (il faut adapter la fréquence du signal au mode transmission) et, d'autre part, il s'agit surtout de pouvoir transmettre plusieurs messages sur un même réseau.

3.2 Chaîne de transmission numérique classique

Les systèmes de transmission numérique véhiculent de l'information sous formes numériques entre une source et un ou plusieurs destinataires (fig.3.1) 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 tache du système de transmission est d'acheminer l'information de la source vers le destinataire avec le plus de fiabilité possible. Les caractéristiques de l'environnement de transmission sont très importantes et affectent directement la conception des systèmes de communication et leurs fonctions.

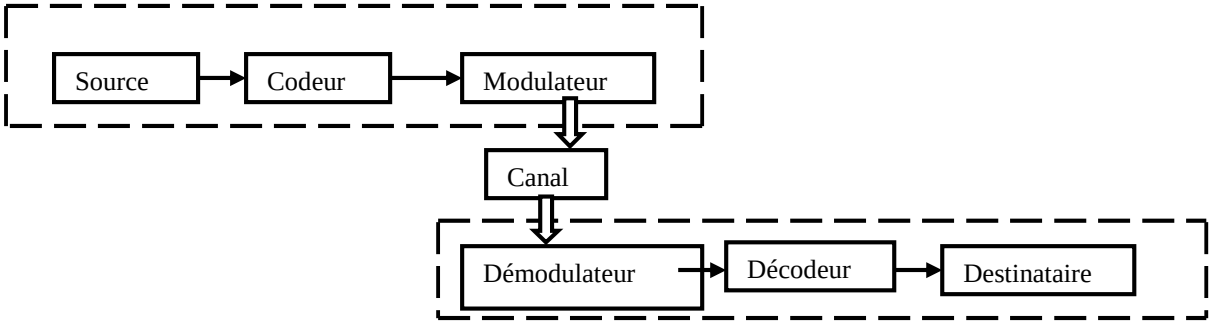


Figure.3.1 : Un système de communication simple

3.3 Model radioélectrique

L'information est codée puis préparée pour son routage entre l'émetteur et le récepteur et enfin mise en forme pour accéder au canal physique.

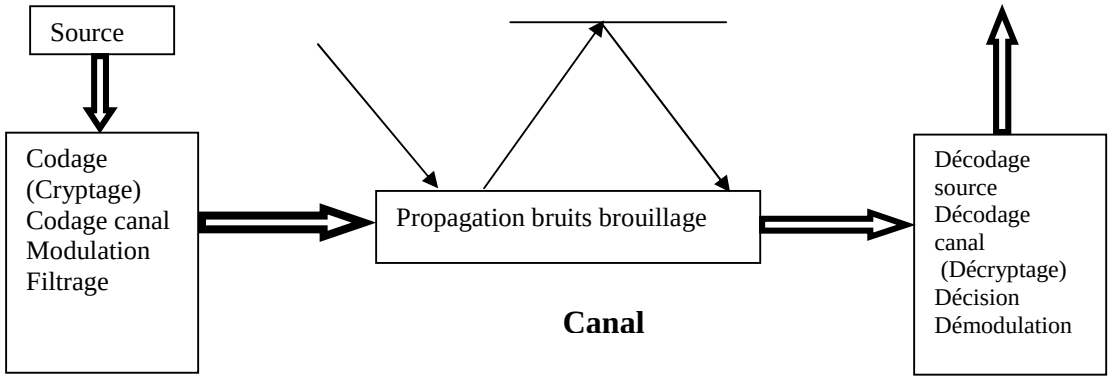


Figure.3.2 : Model de chaîne émettrice canal récepteur

Le schéma synoptique d'un système de transmission numérique est donné à la figure (3.2) où l'on se limite aux fonctions de base [6]:

- La source émet un message numérique sous la forme d'une suite d'éléments binaires.
- Le codeur peut éventuellement supprimer des éléments binaires non significatifs (compression de données ou codage de source, qui a été vue dans le chapitre de la théorie d'information)
- Ou au contraire introduire de la redondance dans l'information en vue de la protéger contre le bruit et les perturbations présentes sur le canal de transmission (codage de canal qui n'est rien d'autre que le code correcteur d'erreurs). Le codage de canal n'est possible que si le débit de source est inférieur à la capacité du canal de transmission (la probabilité d'erreur p tend dans ce cas vers 0 d'après les travaux de Hartley - Shannon).
- Cryptage: afin de sécuriser les données.
- La modulation a pour rôle d'adapter le spectre du signal au canal (milieu physique) sur lequel il sera émis.
- Enfin, du coté récepteur, les fonctions de décompression, décodage, démodulation et décryptage sont les inverses respectifs des fonctions de modulation, codage et décryptage situés du coté émettrice.

3.4 Les caractéristiques principales de techniques de transmission

Les trois caractéristiques principales permettant de comparer entre elles les différentes techniques de transmission sont les suivantes:

- La probabilité d'erreur peut par bit transmis permet d'évaluer la qualité d'un système de transmission. Elle est fonction de la technique de transmission utilisée, mais aussi du canal sur lequel le signal est transmis.
- L'occupation spectrale du signal émis doit être connue pour utiliser efficacement la bande passante du canal de transmission. On est contraint d'utiliser de plus en plus des modulations à grande efficacité spectrale.
- La complexité du récepteur dont la fonction est de restituer le signal émis est le troisième aspect important d'un système de transmission.

3.5 Les modulations numériques

La transmission de données peut se faire de deux manières, soit par le codage en ligne appelé souvent transmission en bande de base ou bien transmission par porteuse.
Il faut distinguer:

- Les liaisons en bande de base, au rythme d'émission des 0 et 1.
- Les liaisons avec changement de fréquence et modulation d'une porteuse radiofréquence ou optique.

3.5.1 Codage en ligne (transmission en bande de base)

La transmission en bande de base consiste à transmettre directement des signaux Numériques sur un support (bande passante limitée, distorsions, etc.) de longueur en principe limitée, cette opération est réalisée par un codeur.

Le codeur transforme une suite de bits {ai} en une suite de symboles { d_k } pris dans un alphabet de q symboles. Les d_k ont en principe toutes la même durée.

Lorsque la transmission s'effectue en bande de base, sans changement de fréquence, un codage binaire en ligne associe un signal électrique e (t) a chaque élément binaire génère "a" avec le débit binaire:

$$D=\frac{1}{T}\ [\text{Bit /s}] \qquad (3.1)$$

Les bits peuvent être regroupes en symboles quaternaires ou m-aires, pour augmenter l'efficacité spectrale.
La rapidité de modulation R, exprimée en bauds vaut:

$$R=\frac{1}{symbole}=\frac{1}{bt\cdot\log_2 m}=\frac{D}{\log_2 m} \qquad (3.2)$$

Ces signaux électriques sont choisis en fonction du milieu de transmission et des conditions qui en résultent sur le spectre des signaux: éviter une composante continue, réduire la bande passante, fournir des informations de synchronisation. [32]

3.5.2 Les codages

Pour l'ensemble des différents codes écrits, nous prendrons la même suite binaire afin de permettre la comparaison: 1 0 0 0 0 1 0 1 1 1 1

3.5.2.1 Cordage NRZ (non return to zero)

Le principe est très proche du codage binaire de base, il code un 1 par +v, un 0 par –v

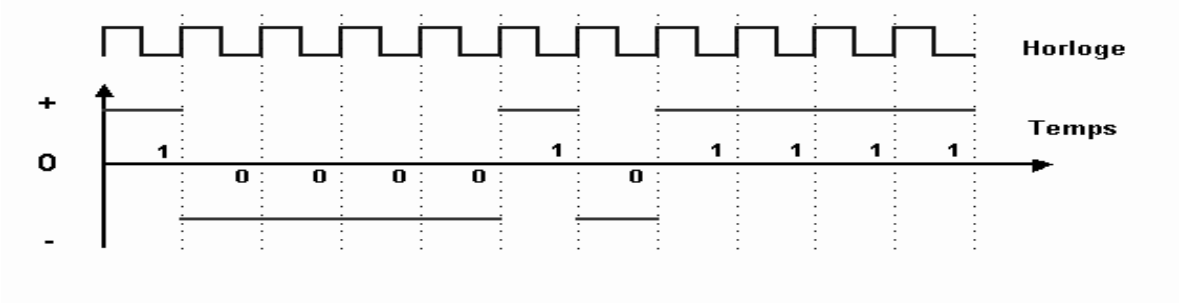


Figure.3.3 : Signal NRZ

Le codage NRZ améliore légèrement le codage binaire de base en augmentant la différence d'amplitude du signal entre les 0 et les 1. Le débit maximum théorique est le double de la fréquence utilisée pour le signal :

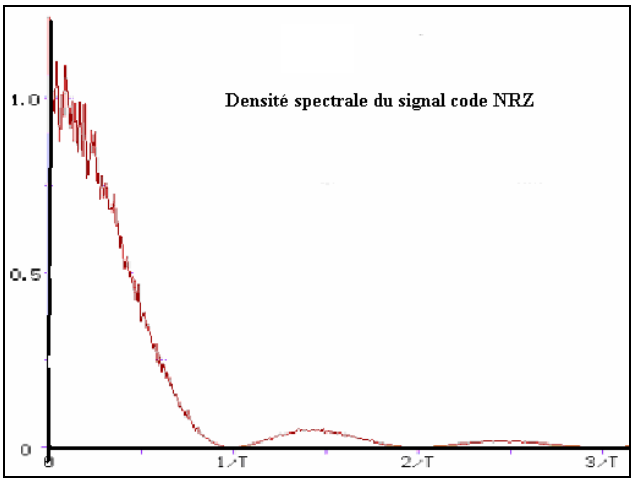


Figure.3.4 : Densité spectrale du signal code NRZ

- Caractéristiques

- Composante Continue : n'est nulle que si les états -a et +a sont équi-répartis.
- La bande passante w =1/Tm.

La densité spectrale de puissance (DSP) d'un signal NRZ est centrée en f=0. Ce mode est donc mal adapté au milieu qui ne passe pas les basses fréquences et le continu. On a:

$$G_v = a^2 . T_m . Sinc^2 (T_m . F) \qquad (3.3)$$

3.5.2.2 Codage MLT3

Dans ce codage, seuls les « 1 » font changer le signal d'état. Les 0 sont codés en conservant la valeur précédemment transmise. Les 1 sont codes successivement sur trois états: +v, 0 et –v.

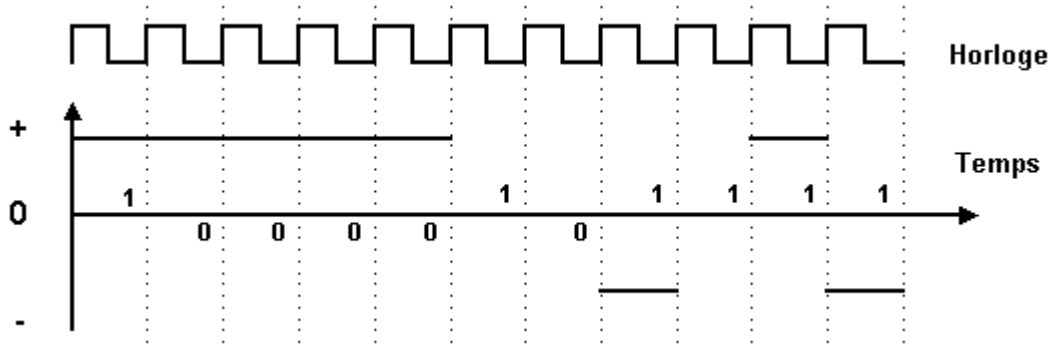


Figure.3.5 : Signal MLT3

Le principal avantage du codage MLT3 est de diminuer fortement la fréquence nécessaire pour un débit donné grâce à l'utilisation de 3 états. Les longues séquences de 0 peuvent entraîner une perte ou un déphasage de l'horloge du récepteur.

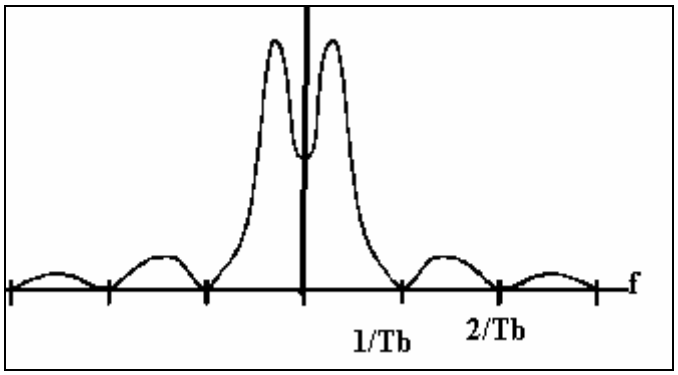


Figure.3.6 : Densité spectrale

3.5.2.3 Codage Manchester

Dans le codage Manchester, l'idée de base est de provoquer une transition du signal pour chaque bit transmis. Un 1 est représenté par le passage de +v à –v, un 0 est représenté par le passage de -v à +v. Le codage Manchester est obtenu par le mélange (opération logique ou exclusif) d'un signal horloge et d'un signal NRZ. Ce codage est illustre par la figure (3 7).

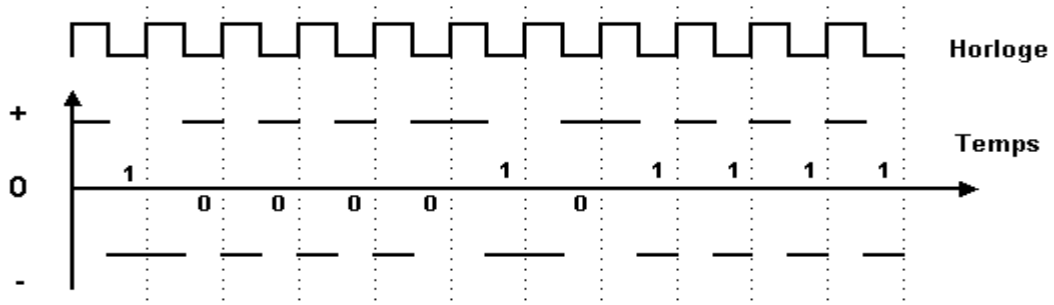
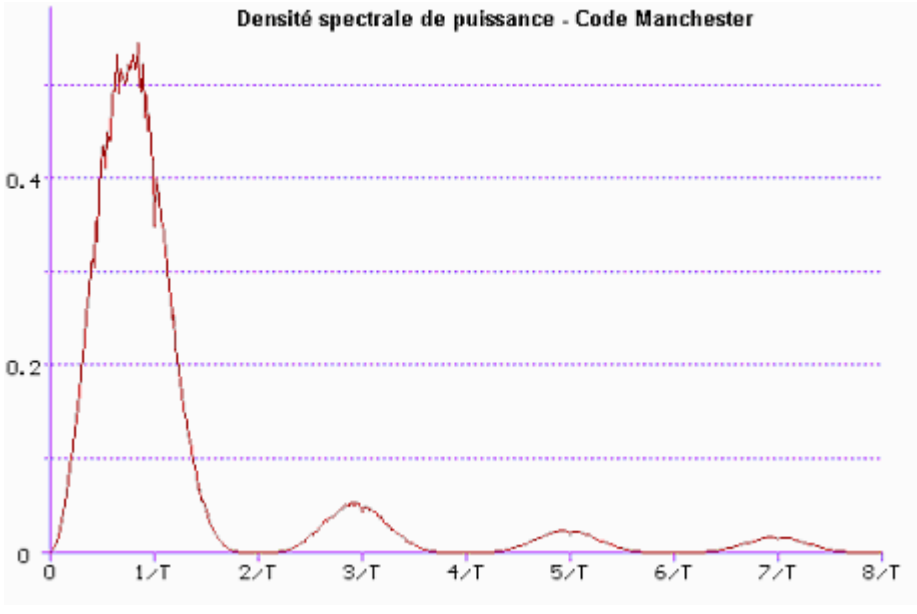


Figure.3.7 : Signal de Manchester

Avantages du code Manchester:

- Valeur moyenne du signal nulle, pas de composante continue et peu d'énergie dans les fréquences basses.
- La densité spectrale du signal présente un maximum vers la fréquence"0, 75/t"

La synchronisation des échanges entre émetteur et récepteur est toujours assurée, même lors de l'envoi de longues séries de 0 ou de 1. Composante continue nulle.



$w=\frac{2}{t_m}$

Figure.3.8 : Densités spectrales de puissance "code Manchester

3.5.2.4 Codage bipolaire ou AMI (alternat mark inversion)

Comme sa désignation anglophone le précise (alternat mark inversion), on alterne les impulsions.[44]

On a la correspondance suivante: "0" =0 v et "1" =a et +a alternativement

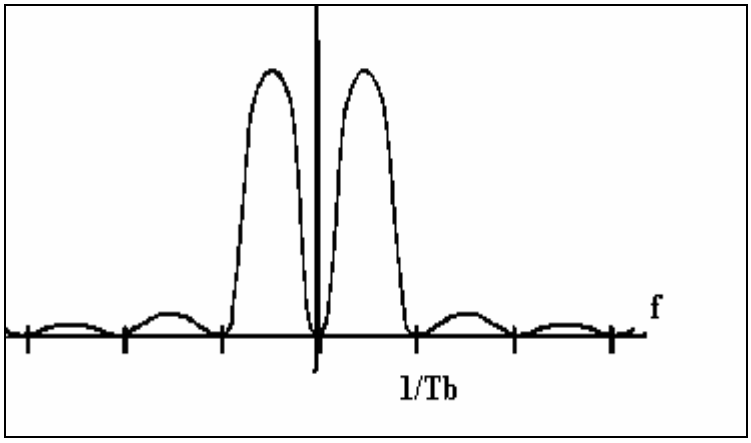


Figure.3.9 : Densité spectrale du code de AMI

- Composante continue nulle.
- Bande passante :w =1/Tm.
- La puissance est bien concentrée entre 0 et 0, 8/t. La composante continue est annulée par le principe d'inversion. On a:

$$G_v = a^2 . T_m . \mathrm{Sinc}^2 (T_m . F) . \mathrm{Sin}^2 (\pi . T_m . F) \qquad (3.5)$$

3.5.2.5 Codage HBDn (haute densité binaire d'ordre n)

Le principe de base est le même que pour le codage bipolaire, mais pour éviter une trop longue série de 0, on introduit un bit supplémentaire au signal pour terminer une série de « 0 » consécutifs. Ce bit supplémentaire est de même phase que le dernier « 1 » transmis pour pouvoir l'identifier, afin qu'il ne soit pas pris en compte dans l'information transmise.

3.5.2.6 Répartition de puissance (spectres) des codes en bandes de base

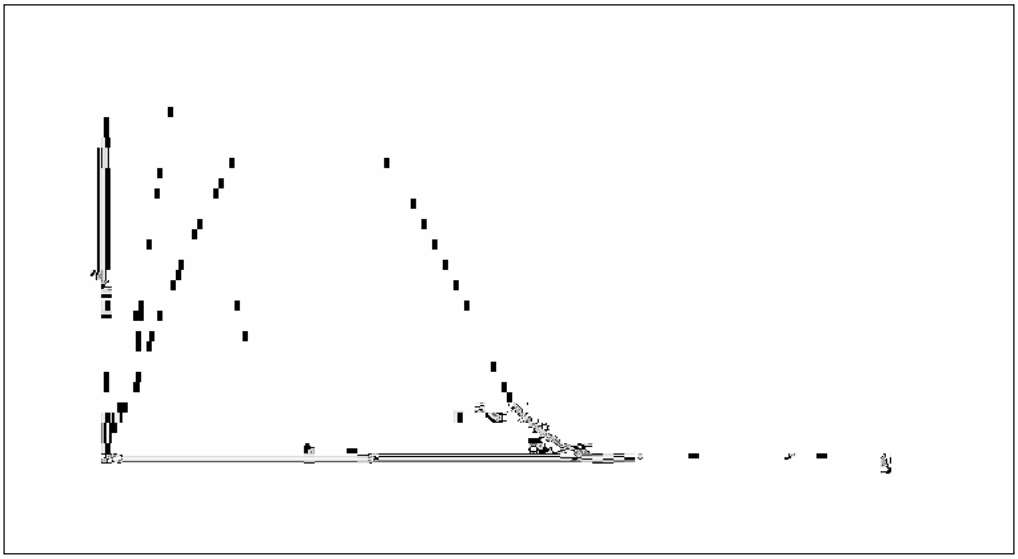


Figure.3.10 : Répartitions de puissance (spectre) des codes en bandes de base

- La densité spectrale de puissance d'un signal « DSP » Manchester est centrée en f=1/tm. Ce mode est donc bien adapté à un milieu qui ne passe pas les basses fréquences et le continu, au prix d'une bande passante doublée par rapport au codage NRZ.
- La densité spectrale de puissance (DSP) d'un signal NRZ est centrée en f=0

3.5.3 Relation de Shannon

Lorsque m bits sont associes à un symbole, le débit de symboles ou rapidité de modulation R, donné en bauds est plus petit que D [18] :

$$R=\frac{d}{\log_2 m} \leq D \qquad (3.6)$$

Le débit de symboles impose les fréquences émises qui sont limitées par la largeur du canal en bande de base avec une largeur totale de bande du canal w, il est possible de transmettre au maximum 2w symboles par seconde. Si ts=1/R est la durée d'un symbole, la période minimale est 2 ts, donc :

$$\frac{1}{2t_s}=\frac{R}{2}\langle w \quad \text{Et} \quad R\langle 2\ w.\frac{1}{2t_s}=\frac{R}{2}\langle W$$

Le nombre de symboles est limité par le rapport des puissances de signal et de bruit S/R ou (Eb/N_0) dans le canal.

$$\log_2\sqrt{\frac{S+N}{N}}=\log_2\sqrt{1+SNR}=\frac{1}{2}\log_2(1+SNR) \quad (3.7)$$

Au total, le débit binaire D est lie à la bande passante w par la relation de Shannon qui donne la capacité binaire théorique maximale C d'un canal de bruit gaussien (en bps) : [18]

$$D\langle C = W\log_2(1+SNR) = W\log_2(1+\frac{P}{WN_0}) = W\log_2(1+\frac{DE_b}{WN_0}) \quad (3.8)$$

3.5.3.1 Caractéristiques d'une voie de communication

- Perturbations

La transmission de données sur une ligne ne se fait pas sans pertes. Tout d'abord le temps de transmission n'est pas immédiat, ce qui impose une certaine « synchronisation » des données à la réception. D'autre part des parasites ou des dégradations du signal peuvent apparaître (voir chapitre 1.)

- Bande passante et capacité

La bande passante d'une voie de transmission est l'intervalle de fréquence sur lequel le signal ne subit pas un affaiblissement supérieur à une certaine valeur (généralement 3db, car 3 décibels correspondent à un affaiblissement du signal de 50%).

- La capacité d'une voie est la quantité d'informations (en bits) pouvant être transmise sur la voie en 1 seconde. Elle se caractérise de la façon suivante :

$$C = W\log_2(1+\frac{S}{N}) \quad (3.9)$$

- La largeur de bande (en Hz) et S/N représente le rapport signal sur bruit de la voie, c'est la bande de fréquence dans laquelle les signaux sont correctement reçus :

$$W = f_{\max} - f_{\min} \quad (3.10)$$

Le spectre du signal à transmettre doit être compris dans la bande passante du support physique.

- Débit maximum d'un canal de transmission :

Nyquist, puis Shannon ont montré que, si un signal quelconque était appliqué à l'entrée d'un filtre passe-bas ayant une bande passante w, le signal ainsi filtré pouvait être reconstitué avec un échantillonnage à 2w par seconde.

$$D_{max}=2W\log_2 V \quad [bit/s] \qquad (3.11)$$

Si le signal comporte v niveaux significatifs (valence). La bande passante limite la rapidité de modulation.

Lorsque des bruits aléatoires apparaissent sur les canaux de transmission, la situation se dégrade rapidement. La quantité de bruit présente sur un canal est exprimée par le rapport de la puissance du signal transmis à la puissance du bruit et est appelé rapport signal sur bruit, (SNR en anglais signal to noise ratio ou S/N en dB).

$$\frac{S}{N}(dB)=\frac{\text{puissance moyenne du signal}}{\text{puissance moyenne du bruit}} \qquad (3.12)$$

3.5.3.2 Temps de transmission et temps de propagation

- Temps de propagation (t_p) = temps mis par le signal pour parcourir une longueur du canal, dépend de la distance, de la nature du support, de la fréquence.
- Temps de transmission (t_t) = temps écoulé entre le début et la fin de la transmission d'un message sur une ligne, dépend de la capacité du canal = n / c).
- Temps d'acheminement d'un message $= t_p + t_t$

3.6 Les modulations de base

La modulation a pour objectif d'adapter le signal à émettre au canal de transmission. Cette opération consiste à modifier un ou plusieurs paramètres d'une onde porteuse.

$S(t) = a\cos(\omega_0 t + \varphi_0)$ Centrée sur la bande de fréquence du canal.

Les paramètres modifiables sont :

- L'amplitude : ***a***
- La fréquence : $f = \frac{\omega_0}{2\pi}$
- La phase : φ_0

A l'instar de la modulation analogique, la modulation numérique est une opération qui transpose le spectre d'un signal numérique pour l'amener autour d'une fréquence porteuse.

3.6.1 Critères de choix de la modulation

Il existe de nombreux critères guidant le choix d'un type de modulation. Il va de soi que l'importance relative d'un critère dépend de l'application envisagée.

Les critères de comparaison sont classes en trois catégories principales [6].

- La résistance aux distorsions et aux interférences

- La résistance au bruit en terme de probabilité d'erreur, celle-ci étant généralement une fonction du rapport énergie sur bruit : $\frac{Eb}{No}$.
- La sensibilité aux interférences dues à des multi trajets.
- La sensibilité aux imperfections des filtres qui produit de l'interférence entre les symboles numériques.
- La sensibilité aux non-linearités.

➢ L'occupation spectrale caractérisée par :

- L'efficacité spectrale exprimée en (bit/seconde) par hertz [b/s/Hz], qui représente le débit binaire que l'on peut transmettre dans un canal large de 1 [Hz] pour un type de modulation,
- Le comportement asymptotique de la densité spectrale de puissance, c'est à dire la rapidité de décroissance de la courbe de densité spectrale de puissance en fonction de la fréquence,

➢ La simplicité d'implémentation

Dans les procèdes de modulation binaire, l'information est transmise à l'aide d'un paramètre qui ne prend que deux valeurs possibles.

Les types de modulation les plus fréquemment rencontrés sont les suivants :

- Modulation par déplacement d'amplitude MDA. (Amplitude shift keying ASK).
- Modulation par déplacement de phase MDP. (Phase shift keying PSK).
- Modulation par déplacement de phase différentielle MDPD. (Differential phase shift keying DPSK).
- Modulation d'amplitude de deux porteuses en quadrature MAQ. *(*quadrature amplitude modulation QAM)
- Modulation par déplacement de fréquence MDF. (Frequency shift keying FSK).

3.6.2 Définition et appellations

Dans les procèdes de modulation m-aire, l'information est transmise à l'aide d'un paramètre qui prend m valeurs. Ceci permet d'associer à un état de modulation un mot de n digits binaires. Le nombre d'états est donc $M=2^n$. Ces n digits proviennent du découpage en paquets de n digits du train binaire issu du codeur. [28]

➢ Un symbole est un élément d'un alphabet. Si M est la taille de l'alphabet, le symbole est alors dit M-aire. Lorsque M=2, le symbole est dit binaire. En groupant, sous forme d'un bloc, n symboles binaires indépendants, on obtient un alphabet de

$M=2^n$ symboles m-aires. Ainsi un symbole m-aire véhicule l'équivalent de $n=\log_2 M$ [bits].

- La rapidité de modulation R se définit comme étant le nombre de changements d'états par seconde d'un ou de plusieurs paramètres modifient simultanément.
- 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.
- La qualité d'une liaison est liée au taux d'erreur par bit :

$$TEB=\frac{\text{nombre de bits faux}}{\text{nombre de bits transmis}} \qquad (3.12)$$

- L'efficacité spectrale d'une modulation se définit par le paramètre η = D/w et s'exprime en « bit/seconde/Hz ». La valeur D est le « débit binaire » et w est la largeur de la bande occupée par le signal modulé. Pour un signal utilisant des symboles m-aires, on aura $\eta = (1/t.w) \log_2 M$ [bit/sec/Hz].

3.7 Principe des modulations numériques

Le message à transmettre est issu d'une source binaire. Le signal modulant, obtenu après codage, est un signal en bande de base, éventuellement complexe, qui s'écrit sous la forme :

$$C(t)=\sum_k c_k \cdot G(t-kt) \quad \text{Et} \quad c_k=a_k(t)+jb_k(t) \ \text{Avec} \ c_k=a_k+jb_k \qquad (3.14)$$

La fonction g(t) est une forme d'onde qui est prise en considération dans l'intervalle [0, t[puisque t doit vérifier la relation : $kt \leq t < (k+1)t$. $g(t)= \{ 1/\sqrt{T}$ pour $t \in [0,T]$ et 0 ailleurs$\}$.
Dans les modulations MDA, MDP et MAQ, la modulation transforme ce signal c(t) en un signal modulé m(t) tel que :

$$m(t)=re[\sum_k c_k(t) \cdot \exp j(\omega_0 \cdot t+\varphi_0)] \qquad (3.15)$$

La fréquence $f_0 = w_0/2\pi$ et la phase φ_0 caractérisent la sinusoïde porteuse utilisée pour la modulation.

S'ils sont réels, la modulation est dite unidimensionnelle, et s'ils sont complexes la modulation est dite bidimensionnelle.
Le signal modulé s'écrit aussi plus simplement :

$$m(t)=\sum_k a_k(t)\cdot\cos(\omega_0\cdot t+\varphi_0)-\sum_k b_k(t)\cdot\sin(\omega_0\cdot t+\varphi_0) \quad \text{Ou encore} \tag{3.16}$$

$$m(t)=a_k(t)\cdot\cos(\omega_0\cdot t+\varphi_0)-b_k\cdot\sin(\omega_0\cdot t+\varphi_0) \tag{3.17}$$

En posant : $a(t)=\sum_k a_k(t)$ et $b(t)=\sum_k b_k(t)$, Le signal $a(t)=\sum_k a_k(t)$) modulé en amplitude, la porteuse en phase : $\cos(\omega_0\cdot t+\varphi_0)$ Et le signal $b(t)=\sum_k b_k(t)$ modulé en amplitude, la porteuse en quadrature : $\sin(\omega_0\cdot t+\varphi_0)$ .Dans la plupart des cas les signaux élémentaires $a_k(t)$ et $b_k(t)$ sont identiques à un coefficient près et ils utilisent la même forme d'impulsion g(t) appelée aussi « formant » :

$a_m(t)=a_k\cdot G(t-kt)$ Et $b_m(t)=b_k\cdot G(t-kt)$

Les symboles a_{ka} et b_k prennent respectivement leurs valeurs dans l'alphabet ($a_1, a_2, \ldots a_m$) et dans l'alphabet ($b_1, b_2, \ldots b_m$).

Le schéma théorique du modulateur est représenté sur la figure (3 11).

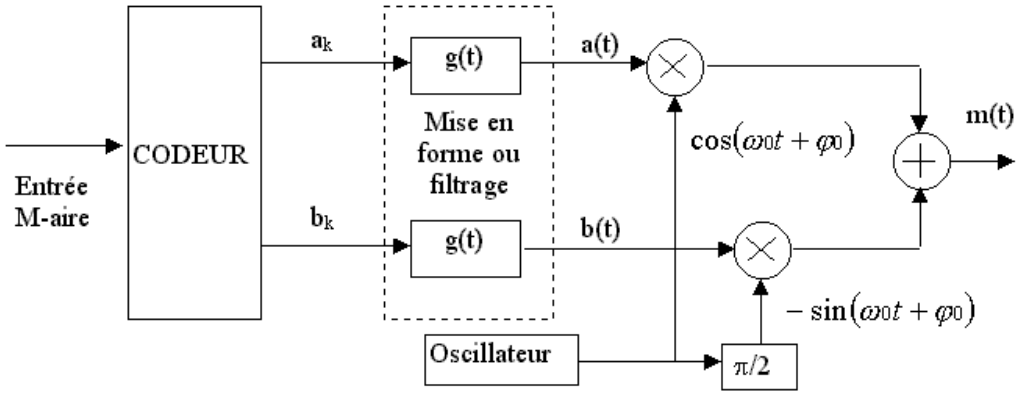


Figure.3.11 : Forme générale du modulateur

Les différents types de modulations sont définis par les alphabets écrits ici dessus et par la fonction g(t).

A chaque symbole émis correspond un signal élémentaire de la forme :

$$m_k(t)=a_k(t)\cdot g(t-kt)\cdot\cos(\omega_0\cdot t+\phi_0)-b_k(t)\cdot\sin(\omega_0\cdot t+\phi_0) \tag{3.18}$$

Qui peut être représentés (voir figure 3.12) dans un espace à deux dimensions dont les vecteurs de base sont : $-g(t-kt)\cdot\cos(\omega_0\cdot t+\phi_0)$ (décomposition de Fresnel). [7]

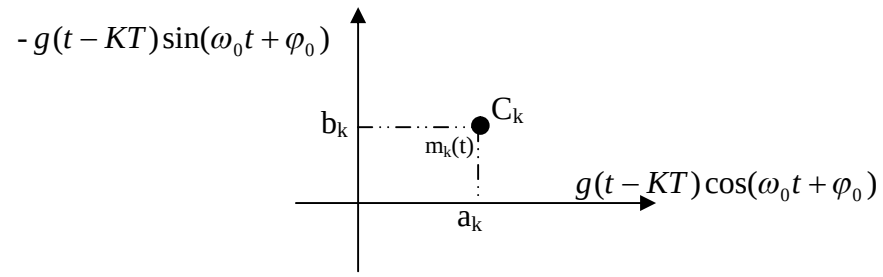


Figure.3.12 : Position d'un symbole dans le plan de Fresnel

Le signal modulé m(t) véhicule des informations distinctes à travers $a_k(t)$ et $b_k(t)$ qui sont deux signaux en bande de base appelée respectivement composante en phase (I en anglais) et composante en quadrature (Q en anglais). La récupération de $a_k(t)$ et $b_k(t)$ sera possible uniquement si ces deux signaux sont de bande limitée à l'intervalle [-b, b] avec $b<f_0$ (condition de Rayhley). [6]

Une représentation dans le plan complexe qui fait correspondre à chaque signal élémentaire un point $c_k=a_k+j\cdot b_k$ permet de différencier chaque type de modulation. L'ensemble de ces points associé aux symboles porte le nom de constellation.

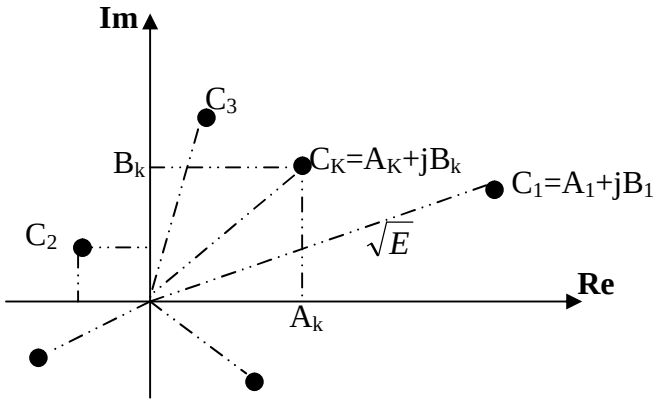


Figure.3.13 : Définition d'une constellation numérique

3.8 Le choix de la répartition des points

Le choix de la répartition des points dépend des critères suivants :

- Pour pouvoir distinguer deux symboles, il faut respecter une distance minimale m_{in}, entre les points représentatifs de ces symboles. Plus cette distance est grande et plus la probabilité d'erreur sera faible. La distance minimale entre tous les symboles est :

$$D\min=\min(d_{i,j}) \quad \text{avec} \quad d_{i,j}=|c_i-c_j|^2 \ (i \neq j) \tag{3.19}$$

Ceci est rapproché avec la définition de la distance de Hamming vue en deuxième chapitre.

- A chaque symbole émis correspond un signal élémentaire $m_k(t)$ et par la même une énergie nécessaire à la transmission de ce symbole. Dans la constellation, la distance entre un point et l'origine est proportionnelle à la racine carrée de l'énergie qu'il faut fournir pendant l'intervalle de temps [kt, (k+1)t] pour émettre ce symbole. La puissance moyenne d'émission des symboles est assimilable à $\Sigma_i |ci|^2$ et la puissance crête à $\max_i |ci|^2$.

Les deux critères évoqués ci-dessus sont antagonistes puisque l'on serait tenté d'une part d'éloigner les symboles au maximum pour diminuer la probabilité d'erreur et d'autre part, de les rapprocher de l'origine pour minimiser l'énergie nécessaire à la transmission. [7]

3.9 Modulation par déplacement d'amplitude (MDA)

Les modulations par déplacement d'amplitude (MDA) sont aussi souvent appelées par leur abréviation anglaise : ASK pour « amplitude shift keying ».

Dans ce cas, la modulation ne s'effectue que sur la porteuse en phase : $\cos(\omega_0 \cdot t + \varphi_0)$. Il n'y a pas de porteuse en quadrature. Cette modulation est parfois dite mono dimensionnelle [7]. Le signal module s'écrit alors :

$$m(t) = \sum_k a_k(t) \cdot G(t - kt) \cdot \cos(\omega_0 \cdot t + \varphi_0) \qquad (3.20)$$

La forme de l'onde *g(t)* est rectangulaire, de durée t et d'amplitude égale à 1 si *t* appartient à l'intervalle [0, t[et égale à 0 ailleurs.

Le symbole a_k prend sa valeur dans l'alphabet ($a_1, a_2, \ldots a_m$). Autrement dit, cet alphabet met en évidence les $M=2^n$ amplitudes possibles du signal, la valeur n désignant les groupements de n bits ou symboles à émettre. Les changements d'amplitude de la porteuse se produiront au rythme *r* de la transmission des symboles.

3.10 Modulation à « M états »

Dans ce cas on utilise plutôt la modulation symétrique.

Les constellations « MDA M symétrique ». On a toujours $M=2^n$ amplitudes possibles du signal, mais ici les valeurs de l'alphabet sont telles que : $a_i = (2i - M + 1)\, a_0$ avec i = 1, 2, …M.

Suivant les valeurs de n on obtient le tableau suivant :

n	M	Valeurs de l'alphabet
1	2	$-1a_0$, $1a_0$
2	4	$-3a_0$, $-1a_0$, $1a_0$, $3a_0$
3	8	$-7a_0$, $-5a_0$, $-3a_0$, $-1a_0$, $1a_0$, $3a_0$, $5a_0$, $7a_0$

La constellation de la modulation à M états symétriques est donnée figure (3.14).

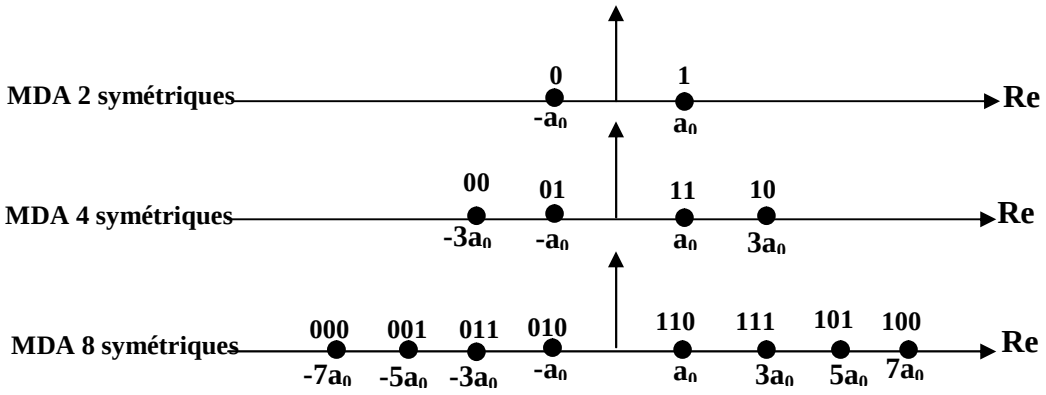


Figure.3.14 : constellation de la modulation d'amplitude à M états

On remarquera que la disposition des symboles M et en œuvre un code de gray de telle sorte qu'un seul bit change lorsque l'on passe d'un point à un autre.

3.11 Modulation par déplacement de phase (MDP)

Les modulations par déplacement de phase (MDP) sont aussi souvent appelés par leur abréviation anglaise : PSK pour « phase shift keying ». [7], [31], [33].

Reprenons l'expression générale d'une modulation numérique :

$$m(t)=re[\sum_k c_k(t)\cdot\exp j(\omega_0\cdot t+\varphi_0)] \text{ Avec } c_k=a_k(t)+jb_k(t) \qquad (3.21)$$

Les signaux élémentaires $a_k(t)$ et $b_k(t)$ utilisent la même forme d'onde g(t) qui est ici une impulsion rectangulaire, de durée t et d'amplitude égale à « *a* » si t appartient à l'intervalle [0, t[et égale à 0 ailleurs.

On a toujours : $a_m(t)=a_k\cdot G(t-kt)$ et $b_m(t)=b_k\cdot G(t-kt)$

$$\text{Soit : } c_k(t)=[a_k(t)+j\cdot b_k(t)]\cdot G(t-kt) = c_k.G(t-kt) \qquad (3.22)$$

Dans le cas présent, les symboles C_k sont repartis sur un cercle, et par conséquent : $C_k = a_k + jb_k = e^{j\varphi k}$ D'où $a_k = Cos(\varphi_k)$ et $b_k = Sin(\varphi_k)$

Avec $a_k(t) = Cos(\varphi_k).G(t-Kt)$ et $b_k(t) = Sin(\varphi_k).G(t-Kt)$

On pourrait imaginer plusieurs MDP-M pour la même valeur de M ou les symboles seraient disposés de façon quelconque sur le cercle. Pour améliorer les performances par rapport au bruit, on impose aux symboles d'être repartis régulièrement sur le cercle (il sera ainsi plus facile de les discerner en moyenne). L'ensemble des phases possibles se traduit alors par les expressions suivantes : $K = \frac{\pi}{M} + \frac{k.2\pi}{M}$ lorsque M > *2*Et : $\varphi_k = 0$ ou π lorsque M = 2.

$$m(t) = a(t)Cos(\omega_0 t + k + \varphi_0) = a(t)Cos(\omega_0 t + \varphi_k)Cos(\varphi_k) - a(t)Sin(\omega_0 + \varphi_0)Sin(\varphi_k) \quad (3.23)$$

Cette dernière expression montre que la phase de la porteuse est modulée par l'argument φ_k de chaque symbole ce qui explique le nom donne à la MDP.

On appelle « MDP-M » une modulation par déplacement de phase (MDP) correspondant à des symboles m-aires. La figure (3.15) montre différente constellation de (MDP) pour M= 2, 4 et 8.

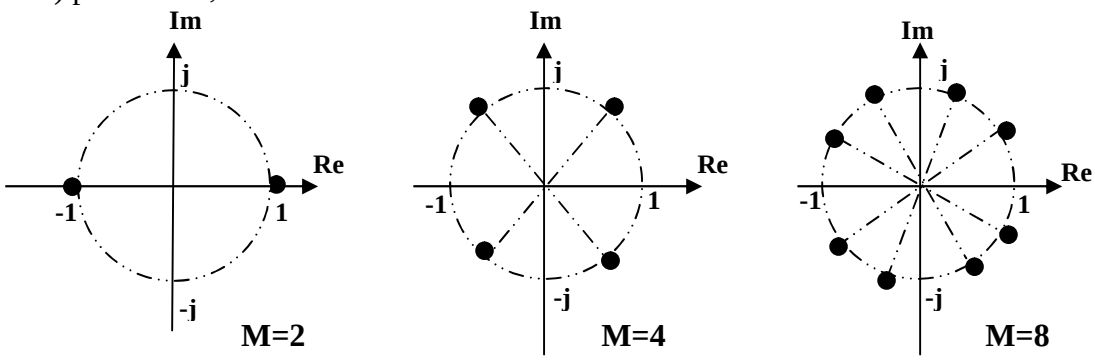


Figure. 3.15 : Constellation des symboles en modulation de phase MDP-M

- Spectre et efficacité spectrale :

L'efficacité spectrale $\eta = D/b$ est multiplie par $n = \log_2 M$.

Tableau.3.1 : le gain obtenu sur le débit binaire et sur l'efficacité Spectrale pour diverse modulation MDP-M

M	Modulation	Débit binaire : *d*	Efficacité spectrale : η
2	MDP-2	*D*	η
4	MDP-4	*2. D*	2η
8	MDP-8	*3. D*	3η
16	MDP-16	*4. D*	4η

Le tableau ci-dessus montre le gain obtenu sur le débit binaire et sur l'efficacité spectrale pour diverse modulation MDP-M, ceci pour une même rapidité de modulation.

3.12 Modulation d'amplitude sur deux porteuses en quadrature (MAQ)

Les modulations d'amplitude sur deux porteuses en quadrature (MAQ) sont aussi appelées par leur abréviation anglaise : QAM pour « quadrature amplitude modulation ». [7], [28] c'est une modulation dite bidimensionnelle.

La MDA et la MDP ne constituent pas une solution satisfaisante pour utiliser efficacement l'énergie émise lorsque le nombre de points M est grand. En effet, dans la MDA les points de la constellation sont sur une droite, et dans la MDP les points sont sur un cercle. Or, la probabilité d'erreur est fonction de la distance minimale entre les points de la constellation, et la meilleure modulation est celle qui maximise cette distance pour une puissance moyenne donnée. Un choix plus rationnel est alors une modulation qui repartit les points uniformément dans le plan.

Pour faire cela, nous avons vu que le signal module m(t) peut s'écrire :

$$m(t)=a(t)\cos(\omega_0+\ _0)-b(t)\sin(\omega_0+\ _0) \qquad (3.25)$$

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

$$a(t)=\sum_k a_k.G(t-Kt) \quad \text{et} \quad b(t)=\sum_k b_k G(t-Kt)$$

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

3.13 Les constellations MAQ-M

Les symboles a_k et b_k prennent respectivement leurs valeurs dans deux alphabets à M éléments (a_1, a_2, … a_m) et (b_1, b_2, … b_m) donnant ainsi naissance à une modulation possédant un nombre $e = M^2$ états. Chaque état est donc représenté par un couple (a_k, , b_k) ou ce qui revient au même par un symbole complexe $c_k = a_k + j\ b_k$.

Dans le cas particulier mais très fréquent où M peut s'écrire $M = 2^n$, alors les a_k représentent un mot de n bits et les b_k représentent aussi un mot de n bits. Le symbole complexe $c_k = a_k + j\ b_k$ peut par conséquent représenter un mot de *2n* bits. L'intérêt de cette configuration est que le signal m(t*)* est alors obtenu par une combinaison de deux porteuses en quadrature modulées en amplitude par des symboles a_k *et* b_k indépendants.
De plus, les symboles a_k et b_k prennent très souvent leurs valeurs dans un même alphabet à m éléments.

Plus généralement lorsque les symboles a_k *et* b_k prennent leurs valeurs dans l'alphabet {± d, ± 3d, ± 5d, …, ± (M-1)d} avec $M = 2^n$, . On obtient une modulation à 2^n états et une constellation avec un contour carrée dont font partie la MAQ-4, la MAQ-16, la MAQ-64 et la MAQ-256.

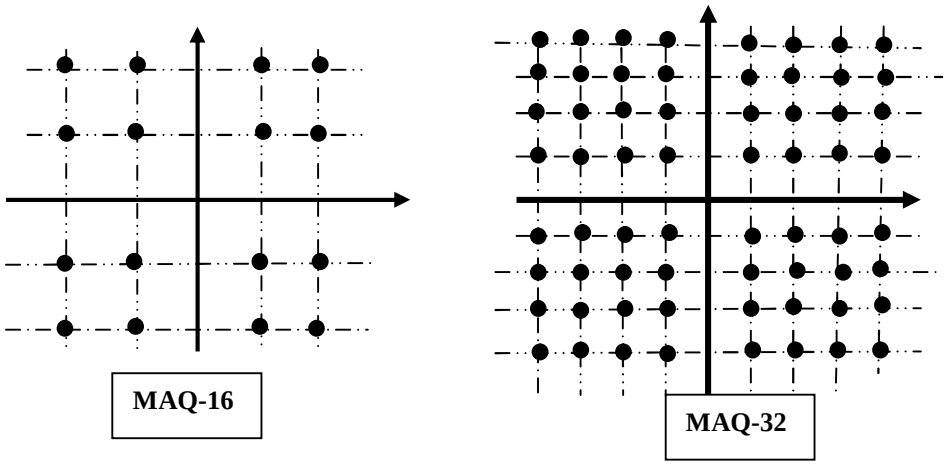


Figure. 3.16 : Constellations MAQ-16 et MAQ-64

- Efficacité spectrale :

Pour une même rapidité de modulation R =1/ t, le débit binaire D= $\frac{1}{Tb}$ de la MAQ-M est multiplie par n=log $_2$ M par rapport celui de la MAQ-2. Autrement dit, pour une largeur de bande *w* donnée, l'efficacité spectrale η = D/b est multiplie par n =log $_2$ M

Tableau. 3.2 : Le gain obtenu sur le débit binaire et sur l'efficacité spectrale pour diverses modulations MAQ-M

N	$M=2^n$	Modulation	Débit binaire: *d*	Efficacité spectrale: η
1	2	MAQ-2	*D*	η
2	4	MAQ-4	*2. D*	*2.* η
4	16	MAQ-16	*4. D*	*4.* η
6	64	MAQ-64	*6. D*	*6.* η
8	256	MAQ-256	*8. D*	*8.* η

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

3.14 Modulation par déplacement de fréquence (MDF)

Les modulations par déplacement de fréquence (MDF) sont aussi souvent appelées par leur abréviation anglaise: FSK pour "frequency shift keying". [7], [28].

Le signal module *m(t)* peut s'écrire: $m(t)=re[e^{j\varphi(t)} \cdot e^{j(\omega_0 + \varphi_0)}]$ (3.26)

Une propriété de la modulation par déplacement de fréquence est d'avoir une enveloppe constante: $e^{j\phi(t)}$ =constante.

L'expression du signal module par déplacement de fréquence s'écrit aussi plus simplement,

Et en prenant $\varphi_0 = 0$, par: $m(t)=Cos(\omega_0+\varphi t))=Cos(2\pi..F_0+\varphi(t))$ (3.27)

3.15 Influence du codage sur l'occupation spectrale

Le premier effet du codage apparaît comme négative puisque le débit numérique transmis

Ou débit code sera: $D_c=\frac{D_b}{R}$ (bits /s) (3.28)

Il est montre que, malgré la corrélation introduite sur les débits, il est nécessaire, pour pouvoir appliquer le codage correcteur, de disposer à priori d'une largeur de bande supplémentaire.

Ainsi on peut dresser le tableau suivant donnant la bande minimale nécessaire au sens du premier critère de Nyquist pour transmettre à un débit d'information de $1/T_b$ avec une modulation MDP-M et un code de rendement R. [42]

Tableau. 3.3 : Largeur de bande minimale occupée par une combinaison d'une MDP-M et Code de rendement R.

Nombre de phase MDP-M	Rendement du code R	Largeur de bande minimale occupée
2	Sans	$1/ T_b$
	1/2	$1 T_b /2$
	2/3	$3/2 T_b$
4	Sans	$1/2 T_b$
	1/2	$1/ T_b$
	2/3	$3/4 T_b$
	3/4	$2/3 T_b$
8	Sans	$1/3 T_b$
	1/2	$2/3 T_b$
	2/3	$1/2 T_b$
	3/4	$4/9 T_b$
16	Sans	$1/4 T_b$
	1/2	$1/2 T_b$
	2/3	$3/8 T_b$
	3/4	$1/3 T_b$

A largeur de bande réellement occupée est 1. 2 fois cette la largeur de bande (théorique)

3.16 Filtre de Nyquist

3.16.1 Transmission en bande de base dans un canal à bande limitée

La bande passante du canal étant limitée, les réponses du canal aux impulsions émises par l'émetteur sont étalées dans le temps et s'additionnent en interférant.

Pour éviter ces interférences entre symboles IES (ou ISI), le premier critère de Nyquist impose des zéros aux temps multiples de la période sur la réponse à une impulsion. De plus, signaux de rapidité R ne peut pas être transmis dans une bande inférieure à R/2 sans IES. [44]

Le filtre de Nyquist va diminuer le débit utile de notre signal en fonction d'un coefficient appel roll off. La largeur de bande occupée sera égale [6], [29], [30] à:

$$W = debit\ \ utile.(1+roll\ \ off) \tag{3.29}$$

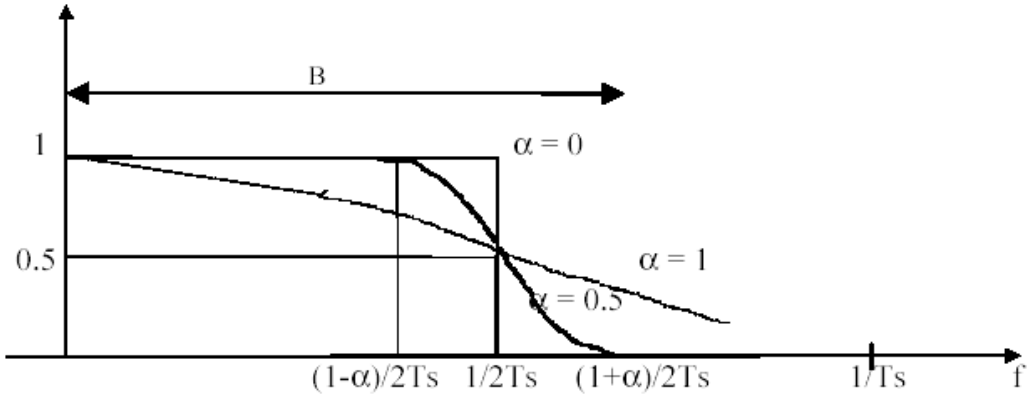


Figure. 3.17 : Transformée de Fourier de l'impulsion en cosinus surélevé pour α = 0 : 0, 5 et 1. En abscisses, l'axe des fréquences est gradué en 1/T.

Le filtre le plus usuel qui satisfait à ce critère, en cosinus surélevé (raised cosinus) ou de nyquist, est caractérisé par son facteur de retombée (roll-off = α) qui définit sa raideur. Le paramètre α s'appelle le facteur de débordement (ou coefficient d'arrondi, roll-off en anglais). Il varie entre 0 et 1. Plus il est grand, plus la bande en fréquence nécessaire pour transmettre est grande. Elle est donnée par:

$$B=\frac{1+\alpha}{2T}=(1+\alpha)\frac{D_b}{2\log_2(M)} \tag{3.30}$$

On voit que la bande occupée est B = (1 + a)/2T.

3.16.2 Calcul du dépit utile

On a vu que, de part le filtrage de Nyquist, le débit du signal binaire que l'on va pouvoir transporter est égal à:

$$\text{Débit binaire}=\frac{largeur\ \ du\ \ canal}{1+Roll\ \ off}$$

Le spectre total du signal après filtrage présente une largeur bande B liée à la fréquence des symboles ou rapidité de modulation R = 1/ts par:

$$B=\frac{(1+\alpha)}{2.t_s}=\frac{(1+\alpha).r}{2} \text{ (si } \alpha=0, B = 1 / 2 \text{ ts: Nyquist)} \qquad (3.31)$$

Sa réponse impulsionnelle, t_f de sa fonction de transfert, s'annule bien pour t multiple de ts. Elle est forcée à zéro si t < 0 pour respecter la causalité.

3.16.3 Interaction entre symboles (IES)

Un canal de transmission ayant toujours une bande passante limitée, chaque symbole transmis est déforme et surtout étalé. A la réception les symboles successifs se trouvent en partie mélangée et leur identification peut devenir difficile.
La détection s'effectue le plus souvent par échantillonnage du signal reçu à un instant de la période jugé favorable.

La limitation de la bande passante conduit inévitablement à un élargissement des symboles émis, mais cet élargissement ne perturbe pas l'identification si les contributions des différents symboles antérieurs sont nulles à l'instant d'échantillonnage.

3.16.4 Le diagramme en oeil

Le diagramme en oeil est une technique de mesure qui permet de déterminer la marge de détection sur un signal avec distorsion et bruit.
La technique du diagramme en oeil consiste à produire avec un générateur pseudo aléatoire toutes les combinaisons possibles de séquences et de les superposer sur un oscilloscope. Une zone sans trace, appelée oeil, doit apparaître entre les transitions. La largeur dt et la hauteur de l'œil en présence de bruit donnent la marge de réserve contre les erreurs de détection.

Un moyen pratique, très largement utilise, pour évaluer la situation de non interférence entre symboles dans une transmission, est l'observation du diagramme de l'œil.
L'observation du diagramme de l'œil fournit les indications suivantes:

- L'ouverture verticale mesure les performances contre le bruit. Plus l'œil est ouvert en hauteur, plus il est facile de discriminer les symboles en présence de bruit, donc plus la probabilité d'erreur est faible. Si le diagramme manifeste la présence d'une IES (faible), et que l'on souhaite continuer utiliser une détection à seuil (solution sous optimale), il faudra venir échantillonner le signal aux instants où l'œil a une ouverture maximale.

- L’ouverture horizontale indique une résistance à un décalage des instants d’échantillonnage. Ainsi, plus l’œil est ouvert en largeur, plus les lobes secondaires de la réponse en temps seront faibles et plus l’accumulation des interférences dues au décalage des instants d’échantillonnage aura une influence moindre en terme de probabilité d’erreur. C’est le cas pour les fonctions en cosinus surélevé lorsque α augmente.

3.17 Conclusion

L'extraordinaire variété des applications que nous venons d'exposer met en évidence l'importance capitale des différentes techniques de transmission numérique sur porteuse. Un intérêt majeur des transmissions numériques réside dans la possibilité de leur insertion harmonieuse dans les réseaux intègres 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.

CHAPITRE 4
CRYPTAGE

4.1 Introduction

Dés 1949, Claude Shannon tente de donner des fondements théoriques à la cryptologie. Il adopte le point de vue de la théorie de l'information et introduit la notion de sécurité inconditionnelle.

L'objet de cette présentation est de faire un état des lieux des différentes méthodes et procédés de cryptages utilisés à ce jour, ainsi que les moyens de leur mise en oeuvre.

La cryptographie est depuis l'aube des temps liée à l'histoire de la communication. Depuis que les hommes ont commencé à s'échanger des messages, la nécessité de garantir la confidentialité et donc de dissimuler ces messages est apparue.
L'histoire de la cryptographie est donc indissociable de celle des communications. L'évolution des deux va donc s'effectuer en parallèle. Chaque nouvelle évolution des moyens de communication entraînant une évolution des procédés et des moyens de cryptage.

D'abord relativement artisanale et confidentielle au même titre que l'écriture et les moyens de communication. La cryptographie va connaître un brusque essor au XX siècle avec l'apparition des communications radio, du téléphone et bien sûr Internet et l'avènement des réseaux.

Depuis l'apparition de l'écriture, les hommes n'ont cessé de s'intéresser la plupart du temps à des fins militaires aux moyens permettant de transformer un document intelligible en une information incompréhensible.. Au fil du temps, les méthodes de cryptage se sont sophistiquées et adaptées aux innovations techniques de leur époque: les ordinateurs sont par exemple devenus incontournables de nos jours.

Avant d'étudier plus en détail les principaux procédés cryptographiques actuellement utilisés, il convient tout d'abord d'expliquer certains termes fréquemment employés par les spécialistes. La cryptologie est la science des écritures secrètes, qu'il s'agisse d'informations électroniques ou non. Elle englobe la cryptographie - laquelle designé le processus permettant de rendre inintelligible une donnée compréhensible et la cryptanalyse (ensemble de méthodes servant à décoder des données sans connaître préalablement la clé

de codage). Lorsqu'il s'agit de coder des données numériques, on utilise de préférence le terme " chiffrement ". Les informations chiffrées également appelées " cryptogramme " sont dites déchiffrées lorsque la clé de codage appropriée est employée. En revanche, on parle de décryptage lorsque des tiers cherchent à transformer un cryptogramme en texte clair sans connaître la clé.

4.2 Historique

4.2.1 L'antiquité

4.2.1.1 Chine

C'est dans la Chine Antique [38]qu'apparaissent les premiers messages secrets. Il n'est pas encore juste de parler de cryptographie, mais plutôt de stéganographie (stéganos du grec : "caché"). En effet le message n'était pas modifié comme c'est le cas dans la cryptographie. Il était seulement dissimulé. Le message inscrit sur du papier ou de la soie était roulé en boule, puis recouvert de cire. Le porteur dissimulait alors la sphère de cire sur lui ou l'avalait.

4.2.1.2 Grèce

La Grèce antique, avec Sparte la plus guerrière des cités grecques, conçoit le premier procédé de codage. Elle emploie un instrument appelé ″scytale", le premier utilisé en cryptographie et fonctionnant selon le principe de transposition (on garde les caractères d'origine, mais on intervertit l'ordre). [38]

C'est encore en Grèce, qu'apparaît le premier procédé de codage par substitution. Il s'agit d'un système de transmission basé sur un carré de 25 cases. Ce système présente plusieurs caractéristiques intéressantes :

- La conversion des lettres en chiffres.
- La réduction du nombre de symboles.
- Le chiffrement par substitution consiste à remplacer dans un message un ou plusieurs caractères par un ou plusieurs autres caractères.

On distingue généralement plusieurs types de crypto systèmes (systèmes de cryptage) par substitution :

- La substitution mono alphabétique consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet.
- La substitution poly alphabétique consiste à utiliser une suite de chiffres mono alphabétique réutilisée périodiquement.

- La substitution homophonique permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.
- La substitution de poly grammes consiste à substituer un groupe de caractères (poly gramme) dans le message par un autre groupe de caractères.

4.2.1.3 Rome

C'est à Rome, qu'apparaît le système de substitution le plus connu : Le chiffrement de César.

On décale l'ensemble des valeurs de caractères du message d'un certain nombre de position (toujours le même). En définitif, il s'agit de substituer chaque lettre par une autre.

Ce système est dit totalement symétrique, dans le sens où il suffit de faire l'opération inverse avec la bonne clé pour obtenir le message initial.

4.2.2 Le moyen age

Le cryptage des données évoluera très peu entre l'antiquité et le Moyen-âge. Ceci s'explique par le faible volume des communications et aussi par le fait que la lecture et l'écriture étaient très peu répandues. De par le fait, leur utilisation même pouvait s'apparenter à un code.

4.2.2.1 Tri thème

En 1518 Jean TRITHEME, moine bénédictin conçoit un système poly alphabétique utilisant un tableau qu'il intitule "Tabula Recta". Il chiffrait la première lettre avec le premier alphabet, la deuxième lettre avec le deuxième alphabet, etc.…

4.2.2.1.1 Bel Aso

La substitution poly alphabétique progresse encore sous l'impulsion de Giovanni Batista Bel Aso. Il invente la notion de clé littérale qu'il appelle "mot de passe".

4.2.2.1.2 Vigenère (le "carre de vigenere"

Qui utilise un tableau du type trithème). Le système consiste à coder un texte avec un mot (et non plus une lettre comme avec le chiffrement de César). On ajoute à chaque lettre du message la valeur de la lettre du mot clé se trouvant en vis à vis. Le mot clé étant répété sur toute la longueur du message. Conséquence, un caractère du texte codé ne renvoie pas toujours à la même lettre.

Jusqu'en 1917, ce procédé est réputé in-décryptable, notamment par des revues scientifiques américaines. Ce qui n'était pas vraiment le cas, mais les méthodes de décryptage étant quasiment inexistantes. Il fut très rarement "cracké" (décodé).

4.2.3 Le xx siècles

En 1948 et 1949, deux articles de Claude Shannon,le premier est : « a mathematical theory of communication » [3] et le second : « the communication theory of secrecy systems » donnèrent des assises scientifiques à la cryptographie en balayant espoirs et préjuges. Shannon prouva que le chiffrement de Vernam introduit quelques dizaines d'années plus tôt, encore appelé « one-time pad » était le seul système inconditionnellement sure.

4.2.3.1 Première guerre mondiale

C'est avec la première guerre mondiale qu'apparaissent les premiers services de chiffre et de décryptement, qui vont marquer l'essor de la cryptologie (science qui regroupe la cryptographie et la cryptanalyse). L'utilisation massive de la radio pendant les conflits comporte une faille d'importance. N'importe qui peut intercepter les messages. D'où la nécessité de coder les communications. L'utilisation intensive de la radio et la nécessité d'assurer la confidentialité des correspondances va donc faire de la cryptanalyse pendant la guerre une arme de première importance.

4.2.3.2 Deuxième guerre mondiale

Le chiffrement manuel des messages se mécanise pendant la seconde guerre mondiale avec l'utilisation de la machine ENIGMA par l'armée allemande.
Malgré son haut niveau de cryptage, les messages codés par ENIGMA furent régulièrement déchiffrés. Ces décryptements furent l'œuvre essentiellement de mathématiciens (Alan Turing). A partir de ce moment, ce qu'on pourrait appeler la cryptologie moderne va se faire exclusivement sur la base de formules mathématiques.

4.3 . La cryptographie

4.3.1 Les domaines d'application

4.3.1.1 La cryptographie dans le passé

Autrefois la cryptographie est très peu répandue. Elle est surtout utilisée par les gouvernements, l'armée ou encore les services secrets. C'est une discipline confidentielle, secrète.

4.3.1.2 La cryptographie actuelle

Aujourd'hui avec l'essor d'Internet, des communications et du commerce en ligne, l'usage de la cryptographie est devenu incontournable. Elle est principalement utilisée par les réseaux bancaires pour assurer la confidentialité de leurs transactions, par l'aviation surtout à prés le 11 septembre, par les sites commerciaux pour sécuriser les achats en ligne. Et également pour protéger les données privées.

L'importance qu'à pris la cryptographie dans les réseaux a été grandement facilitée par le fait que les données transitant sur les réseaux sont des données chiffrées, binaires (suite de 0 et de 1). Elle a été également facilitée par la place qu'ont prise les mathématiques dans la cryptologie moderne pendant les deux premières guerres comme on l'a vu précédemment.

4.3.2 Les attaques

Les nombreuses attaques que peut subir un réseau démontrent que le cryptage des données ne résulte pas d'un acte de paranoïa, mais bien d'une politique de prévention incontournable. Parer les attaques externes est aujourd'hui une obligation. Le type d'attaque auquel est soumis un réseau est de deux types : Les attaques passives et les attaques actives.

4.3.2.1 Attaques passives

Faire une attaque passive, c'est tenter de décrypter un document dans le but unique d'en prendre connaissance, sans l'altérer. Ce type d'attaque porte atteinte à la confidentialité des données.

4.3.2.2 Attaques actives

Faire une attaque active est le fait de tenter de décrypter un document dans le but de pouvoir en prendre connaissance d'une part, et dans le but de le modifier d'autre part ou d'en modifier la signature pour le falsifier, en général dans son intérêt. Une attaque active nuit à l'intégrité des données.

4.4 Les objectifs

La sûreté d'un système de cryptage repose sur:

- La qualité du brouillage opère par le cryptage: si le brouillage est trop faible, des techniques de cryptonyme (parfois même une simple analyse en fréquence) permettent de reconstituer le message en clair, sans connaître la clé ou l'algorithme

de cryptage. Le cryptage opère de préférence sur des blocs de taille différente de l'octet et fait appel à des transformations fortement non linéaires.

- Le nombre de solutions possibles: si la cryptanalyse est impuissante mais l'algorithme de cryptage est connu, il ne reste que le choix entre essayer toutes les solutions possibles (crypto systèmes conventionnels) ou tenter de calculer la clé de décryptage à partir de la clé de cryptage (crypto systèmes à clé publique). Ces calculs doivent donc être suffisamment complexes pour que le temps de calcul soit prohibitif, même avec la puissance de calcul maximale disponible.

Devant cette multitude d'attaque, le cryptage des données dans le cadre de la sécurité dans les réseaux est censé garantir quatre catégories de services.

4.4.1 L'intégrité des données

Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle). Les données doivent donc entre protégées de manière efficace.

4.4.2 La confidentialité des données

La confidentialité consiste à rendre l'information inintelligible à des personnes autres que les acteurs de la transaction. C'est à dire qu'il faut s'assurer que seuls les destinataires seront détenteurs de l'information.

4.4.3 L'authentification

L'authentification consiste à garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

4.4.4 La non répudiation

La non répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

4.5 Comparaison des forces relatives des algorithmes de cryptage

Il existe de multiples algorithmes et applications, ceux que nous vous présentons ci-dessous sont considérés comme les standards du genre car ils ont été révisés et vérifiés par la communauté internationale.

Tableau 4.11 : Comparaison des forces relatives des algorithmes de cryptage

Type	Degré de sécurité *	Implémentation	Vitesse
IDEA	De type militaire	128 bits secrets partage	Rapide
Blowfish	De type militaire	256 à 448 bits secrets partagés	Très rapide
DES	Bas	40 à 56 bits secrets partage	Rapide
RSA	De type militaire	2048 bits clé publique	Très lent
MD5	Elevé	128 bits message digest	Lent
SHA	Elevé	160 bits message digest	Lent

4.6 Notions de base en cryptologie

Le processus de cryptage est basé sur deux éléments: une clé et un algorithme.

- La clé est une chaîne de nombres binaires (0 et 1).
- L'algorithme est une fonction mathématique qui va combiner la clé et le texte à crypter pour rendre ce texte illisible.

4.6.1 Définition

Soit K une clef de k bits appartenant à un sous-ensemble P de l'ensemble des vecteurs de k bits V_k. Un algorithme de cryptage par bloc est une fonction inversible E_K :
$Vn \times K \rightarrow Vn$ transformant un bloc $xi \in Vn$ de n bits de texte en clair en un bloc $yi \in Vn$ de n bits de texte crypté.
La fonction de décryptage est dénotée par E_{K-1} et $E_{K-1}(yi) = xi$.

4.6.2 Crypto systèmes conventionnels. (le cryptage symétrique)

Les deux interlocuteurs doivent connaître la clé permettant de crypter et de décrypter les messages échangés à travers un canal de communication non secret (réseau de transmission). Cette clé doit être échangée à travers un canal de communication secret (comme un porteur prive). La confidentialité est assurée ainsi que l'authentification car seules les deux parties possèdent la clé [20].

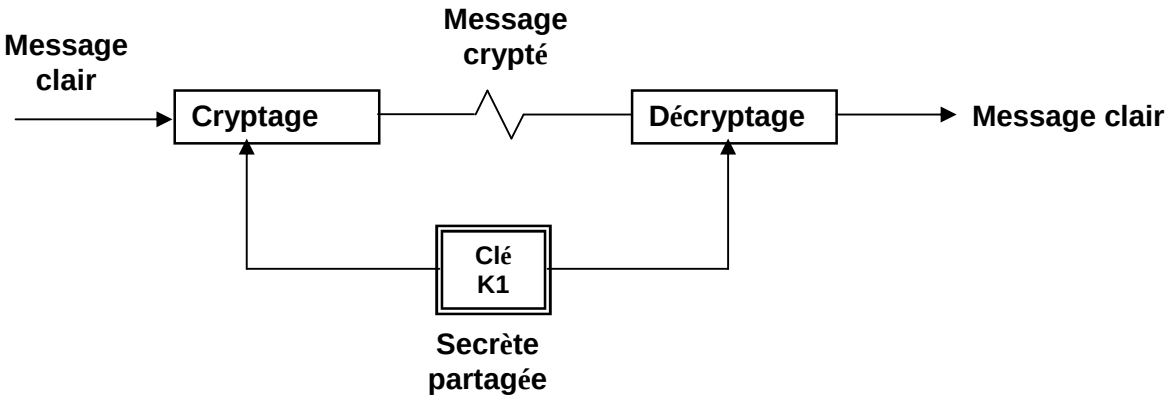


Figure. 4.1 : Le cryptage symétrique

- Si le récepteur a réussi à décoder c'est qu'il possède la clé K, il est donc parfaitement authentifié.
- Si le récepteur a réussi à décoder c'est que l'émetteur a codé avec la clé K, c'est donc qu'il la possède. L'émetteur est donc parfaitement identifié.

Inconvénients:

- Il faut autant de paires de clés que de couples de correspondants
- La non répudiation n'est pas assurée.
- Il faut pouvoir se transmettre la clé au départ sans avoir à utiliser le media à sécuriser.

Les algorithmes utilisant ce système sont: DES, IDEA, RC5, RC4

4.6.3 Crypto systèmes à clé publique. (le cryptage asymétrique)

Le cryptage et le décryptage utilisent deux clés distinctes ; la clé de cryptage est publiée, en revanche la clé de décryptage est connue uniquement par le destinataire du message. La clé de décryptage ne peut pas être calculée, du moins en l'état actuel des connaissances mathématiques, à partir de la clé de cryptage en un temps raisonnable.

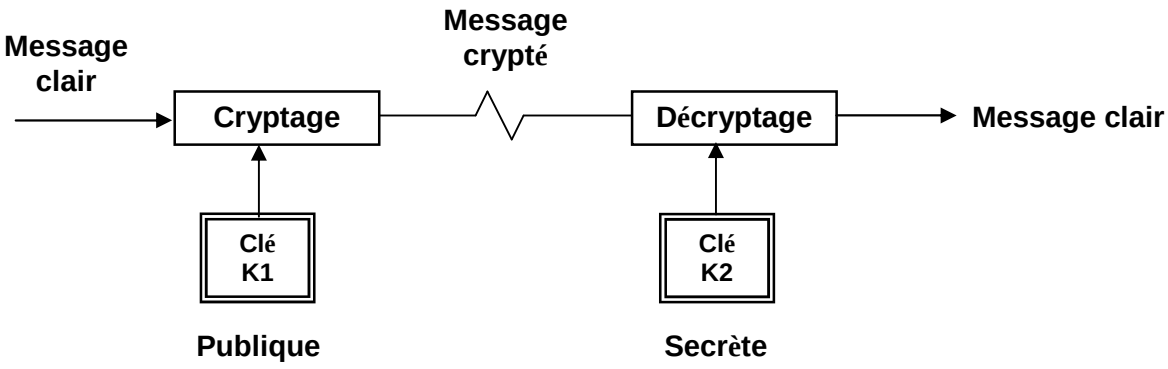


Figure. 4.2 : Le cryptage asymétrique

En employant des techniques similaires, les crypto systèmes à distribution de clé publique laissent deux interlocuteurs aboutir à une clé commune (utilisable par la suite dans un crypto système conventionnel), tout en échangeant sur un canal non secret des informations ne permettant pas à une tierce personne de retrouver la clé.

Celui-ci est né dans les années 70. Le concept a été décrit par W. Diffie et M.E Hellman et repose sur le fait qu'il existe des calculs simples dont la démarche à contre sens. Cette technique repose sur l'existence de deux clés pour chaque utilisateur. Chacun dispose d'une clé privée qui est gardée secrète et d'une clé publique qui est destinée à être divulguée. Ces clés sont liées entre elles. Un document encrypté avec l'une ne peut être décodée qu'avec l'autre. Toutefois, la possession de l'une des clés ne permet pas d'en déduire l'autre.

Il faut bien distinguer deux fonctions différentes:

- La confidentialité :

  Pour ce faire, il suffit de récupérer la clé publique p du destinataire, puis de crypter le message avec cette clé publique et d'envoyer le résultat au destinataire.

  Le destinataire n'a qu'à décoder le message à l'aide de sa clé privée S. Seul la clé privée S correspondant à la clé publique P peut décoder un message en crypté avec cette clé publique p. Comme le destinataire est seul à posséder cette clé privée (secrète), on est sur de la confidentialité du message.

  - L'authentification :

  Le procédé expliqué ci-dessus ne permet pas d'identifier l'émetteur du message. Pour ce faire, on envoie une signature.

  L'émetteur va encrypter le message avec sa clé privée. Le destinataire pourra alors vérifier l'identité de l'émetteur en décryptant le message avec la clé publique de l'émetteur. Comme seul le détenteur de la clé privée P est capable de crypter un message déchiffrable par la clé publique, on est sur de l'identité de l'émetteur.

Avantages:

- La non répudiation est assurée. En effet une personne est seule détentrice de sa clé privée nécessaire à l'authentification. Elle ne peut donc contester une transaction.
- Il n'y a pas besoin de se transmettre les clés au départ par un autre vecteur de transmission.

4.7 Les différents algorithmes et protocoles

4.7.1 Algorithmes de chiffrement asymétrique (clé publique)

Les algorithmes de chiffrement asymétrique les plus rependus sont :RSA, EL GAMAL, sont des algorithmes de cryptographie asymétrique base sur les logarithmes discrets..

4.7.2 Algorithmes de chiffrement symétrique (clé secrète)

On citera brièvement ici quelques algorithmes connus, sans entrer dans les détails de Leur implémentation [23].

4.7.2.1 Rot13

C'est un algorithme très simple de chiffrement de texte. Comme son nom l'indique, il s'agit d'un décalage de 13 caractères de chaque lettre du texte à chiffrer. Le défaut de ce chiffrement est que s'il s'occupe des lettres, il ne s'occupe pas des chiffres, des symboles et de la ponctuation. C'est pourquoi on supprime du texte à chiffrer toute accentuation, et si on veut conserver un texte correctement chiffre, il est nécessaire d'écrire les nombres en toutes lettres [23].

4.7.2.2 Le DES

L'algorithme DES, Data Encryption Standard, a été crée dans les laboratoires de la firme IBM corps. Il est devenu le standard du NIST en 1976 et a été adopte par le gouvernement Américain en 1977. C'est un chiffrement qui transforme des blocs de 64 bits avec une clé secrète de 56 bits au moyen de permutations et de substitutions. [23].Le DES est considère comme étant raisonnablement sécuritaire.

4.7.2.3 BLOWFISH

Blowfish a été conçu par Bruce Schneier en 1993 comme étant une alternative aux algorithmes existants, en étant rapide et gratuit. Blowfish est sensiblement plus que le DES. Il est un chiffrement Feistel, utilisant itérativement une fonction de chiffrement 16 fois des blocs la grandeur est de 64 bits.

Il n'est pas breveté et ainsi son utilisation est libre et gratuite.

4.7.2.4 RC2

Le RC2 a été conçu en 1989. Il avait été programme pour être efficace avec les processeurs de 16 bits comme remplacement au DES. Il s'opère sur des blocs de 64 bits.

La grandeur de la clé est variable, de 1 octet (8 bits) à 128 octets (1024 bits).

Habituellement, l'algorithme s'applique avec une clé de 64 bits.

Le procédé nouveau qu'a apporte cet algorithme a été d'offrir aux utilisateurs la possibilité

de choisir la grandeur de la clé. Cette propriété est maintenant offerte dans plusieurs chiffrements par blocs, étant primordiale dans les applications commerciales.

4.7.2.5 RC5

Le RC5 a été conçu en 1995. Il a l'avantage d'avoir une longueur de bloc de données variable, un nombre de rounds variable et une clé de longueur variable. Ainsi, l'utilisateur a le contrôle sur le rapport entre la vitesse d'exécution et la sécurité de son chiffrement. En général, une longue clé et un nombre élevé de rounds assurent une plus grande sécurité. La taille des blocs de données pour sa part accommode différentes architectures de systèmes.

4.7.2.6 RC6

Le RC6 a été crée en 1998. Il propose des améliorations au RC5 et, comme celui-ci, est fortement dépendant de la transformation de décalage de bits (rotation). Comme le RC5, il a l'avantage d'avoir une longueur de bloc de données variable, un nombre de rounds variable et une clé de longueur variable.[21][22].

4.7.2.7 Advanced encryption standard

AES est le sigle D'Advanced Encryption Standard, en français standard de chiffrement avance. Sous ce nom se cache un algorithme de chiffrement symétrique choisi en octobre 2000, pour être le nouveau standard de chiffrement pour les organisations du gouvernement des états-unis. Il est issu d'un appel d'offre international lance en janvier 1997 et ayant reçu 15 propositions. [22], [23]

L'AES remplace-le DES (choisi comme standard dans les années 1970) qui de nos jours devenait obsolète, puisque n'utilisant que des clefs de 56 bits.

Le chiffrement à une longueur de bloc variable, une longueur de clé variable et un nombre de rounds variables. Par contre, Rijndael version "AES" est restreinte à des longueurs de clé de 128, 192 et 256 bits avec une longueur de bloc fixée à 128 bits.

4.7.2.8 IDEA

IDEA (International Data Encryption Algorithm) [35] [47] est un des algorithmes de chiffrement de données par blocs proposés ces dernières années afin de remplacer DES. Xuejia lai et James Massey [37], deux chercheurs de l'école polytechnique fédérale de Zurich, ont conçu une première version de cet algorithme, appelée PES (proposed encryption standard), en 1990. Suite aux travaux de Biham et Shamir concernant la cryptanalyse différentielle, ils ont renforcé leur système contre les attaques et l'ont baptisé

IPES (improved proposed encryption standard), puis IDEA en 1992. Huit rondes de calcul et une ronde finale.

IDEA est un système de chiffrement par blocs de 64 bits, avec une clé de 128 bits, qui tourne sur 8 rondes. Cet algorithme, n'utilise que trois opérations simples: le XOR, l'addition modulo 2^{16} et la multiplication modulo 2^{16} +1.

Trois opérations binaires sont au cœur de « IDEA », portant sur 2 blocs de 16 bits

En entrée pour produire un bloc de 16 bits en sortie:

• L'addition modulo 2, le « XOR »,

• L'addition modulo 2^{16} (= 65536), addition bit à bit

• La multiplication modulo 2^{16} + 1 (=65537).

Chaque bloc est considère comme un entier de 16 bits non signé, pour « IDEA »,

« 0000000000000000 » vaut 2^{16}.

Le texte est découpé en blocs de 64 bits, redivisés en quatre blocs de 16 bits: X1, X2, X3, X4. La clé k est divisée en 8 blocs de 16 bits, puis décalée circulairement sur la gauche de 25 bits, et redivisée, et ainsi de suite jusqu'à obtenir 52 clés. Ces clés formeront 8 groupes de 6 clés (un groupe par ronde): k1, k2, k3, k4, k5, k6, et un groupe de 4 clés pour la ronde finale: k1, k2, k3, k4.

4.7.2.8.1 Détermination des sous –clés

Les 52 sous-clés générées à partir de la clé de 128 bits sont produites comme suit:

- La clé de 128 bits est divisée en huit blocs. Ces huit blocs sont en fait les huit premières sous-clés utilisées dans le chiffrement (les 6 de la première ronde et les 2 premières de la deuxième ronde).
- La clé de 128 bits est ensuite cycliquement décalée de 25 positions vers la gauche et à nouveau divisée en 8 sous clefs 16 bits. Ces huit blocs sont les huit sous-clés suivantes utilisées dans le chiffrement). Les 4 premières sont utilisées lors de la deuxième ronde et les 4 autres lors de la troisième ronde.
- Le cycle est répété jusqu'à ce que les 52 sous-clés soient toutes générées.. La clef est à nouveau décalée circulairement de 25 bits vers la gauche pour les 8 sous clefs suivantes, et ainsi de suite jusqu'à la fin de l'algorithme le déchiffrement est exactement le même, excepté que les sous clefs sont inversées et légèrement différentes. Les sous clefs de déchiffrements sont inversées par rapport à l'addition ou par rapport à la multiplication des sous clefs de chiffrement.

4.7.2.8.2 Utilisation des sous-clés de chiffrement

Round 1	K[1], k[2], k[3], k[4], k[5], k[6]
Round 2	K[7], k[8], k[9], k[10], k[11], k[12]
Round 3	K[13], k[14], k[15], k[16], k[17], k[18]
Round 4	K[19], k[20], k[21], k[22], k[23], k[24]
Round 5	K[25], k[26], k[27], k[28], k[29], k[30]
Round 6	K[31], k[32], k[33], k[34], k[35], k[36]
Round 7	K[37], k[38], k[39], k[40], k[41], k[42]
Round 8	K[43], k[44], k[45], k[46], k[47], k[48]
Transformation finale	K [49], k [50], k [51], k [52]

4.7.2.8.3 Génération de la clé

Les 8 sous-clés k1, k2, k3, k4, k5, k6, k7, k8 sont déduites directement de la clé, k1 étant égale aux 16 premiers bits (à gauche), k2 aux 16 suivants.

Clé : k1 k2 k3 k4 k5 k6 k7 k8

On effectue ensuite un décalage circulaire vers la gauche de 25 bits puis on découpe le résultat en 8 parties pour obtenir le jeu de sous-clés [k9, k16]. On réalise ce type d'opération 6 fois de suite en extrayant ainsi 8 sous-clés à chaque fois. Il faut noter que dans l'algorithme, on utilisera 6 sous-clés à chaque itération.

4.7.2.8.4 Déchiffrement

On utilise le même algorithme mais avec des clés différentes nommées U1 à U52 dérivées des clés de chiffrement de la façon suivante:

- Les 4 premières sous-clés de l'itération "i" dérivent des 4 premières sous-clés de l'itération "10 - i", la transformation finale étant appréhendée comme l'itération n° : 9,
- La première et la quatrième sous-clés sont égalent aux inverses multiplicatifs modulo 216 + 1 de la première et de la quatrième du chiffrement,
- Pour les itérations n°: 2 à n°: 8, la deuxième et la troisième sous-clés sont égales aux inverses additifs modulo 216 de la troisième et de la deuxième du chiffrement,
- Pour les itérations n°: 1 et n°: 9, la deuxième et la troisième sous-clés sont égales aux inverses additifs modulo 216 de la deuxième et de la troisième du chiffrement,

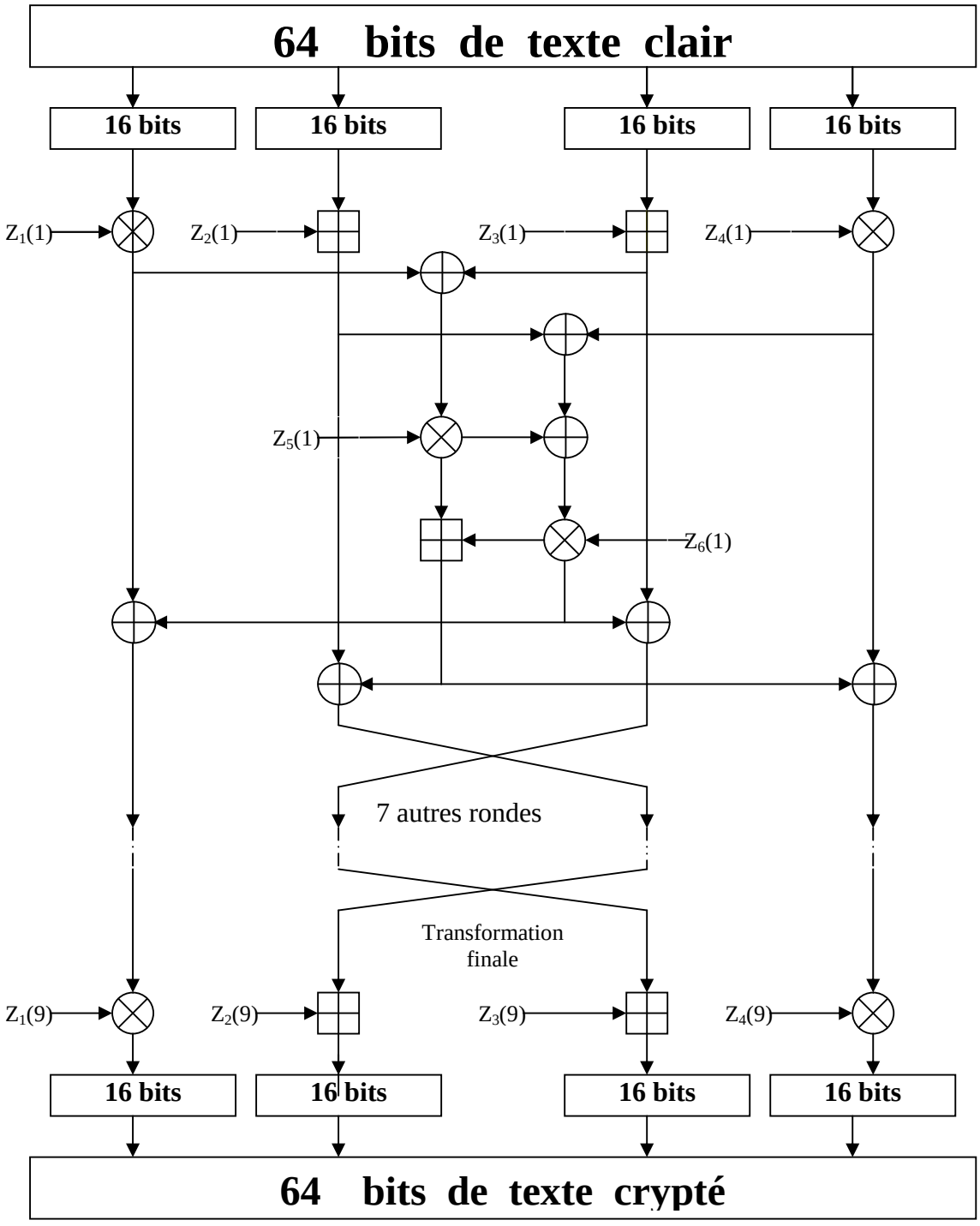
- Pour les huit premières itérations, les deux dernières clés de déchiffrement de l'itération "i" sont égalent aux deux dernières sous-clés de l'itération "9-i" du chiffrement,

Le tableau ci dessous indique les sous-clefs de chiffrement et les sous clefs de déchiffrement correspondantes.

Tableau 4.2 : Indiquant les sous-clefs de chiffrement
et les sous clefs de déchiffrement

Ronde	Sous clefs de chiffrement	Sous clefs de déchiffrement
1	$Z_1^{(1)}$ $Z_2^{(1)}$ $Z_3^{(1)}$ $Z_4^{(1)}$ $Z_5^{(1)}$ $Z_6^{(1)}$	$Z_1^{(9)-1}$ $-Z_2^{(9)}$ $-Z_3^{(9)}$ $Z_4^{(9)-1}$ $Z_5^{(8)}$ $Z_6^{(8)}$
2	$Z_1^{(3)}$ $Z_2^{(2)}$ $Z_3^{(3)}$ $Z_4^{(2)}$ $Z_5^{(2)}$ $Z_6^{(3)}$	$Z_1^{(8)-1}$ $-Z_2^{(8)}$ $-Z_3^{(8)}$ $Z_4^{(8)-1}$ $Z_5^{(7)}$ $Z_6^{(7)}$
3	$Z_1^{(3)}$ $Z_2^{(3)}$ $Z_3^{(3)}$ $Z_4^{(3)}$ $Z_5^{(3)}$ $Z_6^{(3)}$	$Z_1^{(7)-1}$ $-Z_2^{(7)}$ $-Z_3^{(7)}$ $Z_4^{(7)-1}$ $Z_5^{(6)}$ $Z_6^{(6)}$
4	$Z_1^{(4)}$ $Z_2^{(4)}$ $Z_3^{(4)}$ $Z_4^{(1)}$ $Z_5^{(4)}$ $Z_6^{(4)}$	$Z_1^{(6)-1}$ $-Z_2^{(6)}$ $-Z_3^{(6)}$ $Z_4^{(6)-1}$ $Z_5^{(5)}$ $Z_6^{(5)}$
5	$Z_1^{(5)}$ $Z_2^{(5)}$ $Z_3^{(5)}$ $Z_4^{(5)}$ $Z_5^{(5)}$ $Z_6^{(5)}$	$Z_1^{(5)-1}$ $-Z_2^{(5)}$ $-Z_3^{(5)}$ $Z_4^{(5)-1}$ $Z_5^{(4)}$ $Z_6^{(4)}$
6	$Z_1^{(6)}$ $Z_2^{(6)}$ $Z_3^{(6)}$ $Z_4^{6(1)}$ $Z_5^{(6)}$ $Z_6^{(6)}$	$Z_1^{(4)-1}$ $-Z_2^{(4)}$ $-Z_3^{(4)}$ $Z_4^{(4)-1}$ $Z_5^{(3)}$ $Z_6^{(3)}$
7	$Z_1^{7(1)}$ $Z_2^{(7)}$ $Z_3^{(7)}$ $Z_4^{(7)}$ $Z_5^{(7)}$ $Z_6^{(7)}$	$Z_1^{(3)-1}$ $-Z_2^{(3)}$ $-Z_3^{(3)}$ $Z_4^{(3)-1}$ $Z_5^{(2)}$ $Z_6^{(2)}$
8	$Z_1^{(8)}$ $Z_2^{(8)}$ $Z_3^{(8)}$ $Z_4^{(8)}$ $Z_5^{(8)}$ $Z_6^{(8)}$	$Z_1^{(2)-1}$ $-Z_2^{(2)}$ $-Z_3^{(2)}$ $Z_4^{(2)-1}$ $Z_5^{(1)}$ $Z_6^{(1)}$
Finale	$Z_1^{(9)}$ $Z_2^{(9)}$ $Z_3^{(9)}$ $Z_4^{(9)}$	$Z_1^{(1)-1}$ $-Z_2^{(1)}$ $-Z_3^{(1)}$ $Z_4^{(1)-1}$

4.7.2.8.5 Algorithme d'IDEA



4. 1: Organigramme de chiffrage D'IDEA

- Ou exclusif sur 2 blocs de 16 bits
- Addition modulo 2^{16} sur 2 blocs de 16 bits, multiplication modulo $2^{16} + 1$ sur 2 blocs de 16 bits

CHAPITRE 5
SIMULATION

5.1 Introduction

Avant toute conception d'une chaîne de transmission, et notamment la sélection de la forme d'onde, la nature ainsi que les propriétés du canal utilisées doivent être étudier. Puissance du bruit, type et stationnarité du canal, sont des paramètres dont la connaissance à 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.

Le taux d'erreur binaire (TEB) est une donnée d'une très grande importance dans une chaîne de transmission numérique. Afin d'assurer une transmission fiable, le TEB doit rester en dessous d'un seuil donné qui est en fonction de l'application. Les applications multimédias, en particulier, nécessitent une transmission quasiment sans erreurs. D'une manière générale, le taux d'erreur binaire, dépend directement du rapport signal sur bruit, et plus précisément du rapport signal sur bruit par bit utile [34].

5.2 Simulation de la chaîne de transmission

Pour cela nous avons divisé ce chapitre en deux parties, la première partie consiste à faire une évaluation des performances des différentes modulations, décodage et le cryptage (MATLAB) [7]. La deuxième partie est celle de réalisation (la programmation a été faite à base du langage BUILDER).

Les critères de choix d'une modulation

Les critères de choix d'une modulation sont :

- La constellation qui suivant les applications mettra en évidence une faible énergie nécessaire à la transmission des symboles ou une faible probabilité d'erreur.
- L'occupation spectrale du signal modulé.

Pour cela nous avons fait une étude comparative des différentes modulations étudier dans la partie théorique.

Pour pouvoir comparer les différentes modulations entre elles, il est d'usage d'exprimer la probabilité d'erreur en fonction du rapport Eb/N0 dans lequel:

E_b représente l'énergie émise par bit et n_0 représente la densité spectrale de puissance de bruit. Pour guider notre choix dans la détermination des éléments de chaîne de

transmission nous avons fait notre simulation à l'aide du logiciel MATLAB 7. 0 pour les différents états de M.

5.2.1 Partie 1: évaluation des performances de la modulation

Pour M= 2^n, le débit binaire et le débit baud sont reliés par la relation [43] suivante:

$D_b = D_S \log_2 M$, Et nous avons : $D_b = D_S \cdot n$ (5.1)

- L'énergie associée à un symbole a_0 fixé est définie par :

$$E_{a0} = \int_{-\infty}^{+\infty} \left| a_0 g(t) \right|^2 dt = |a_0|^2 \int_0^T |g(t)| dt = |a_0|^2 \quad (5.2)$$

- L'énergie moyenne par symbole est définie par :

$$E_s = E\{E_{a0}\} = E\{|a_0|^2\} = \frac{2A^2}{M} \sum_{p=1}^{M/2} (2p-1)^2 = \frac{2A^2}{M} \cdot \frac{(M-1)(M+1)M}{6} \quad (5.3)$$

$$\text{Soit : } E_S = A^2 \cdot \frac{M^2 - 1}{3} \quad (5.4)$$

- L'énergie moyenne par bit est donnée par :

$$E_b = \frac{E_s}{\log_2 M} = A^2 \frac{M^2 - 1}{3 \log_2 M} \quad (5.5)$$

- La puissance moyenne émise est :

$$P_b = E_b \; D_b = E_s \; D_s = D_b \cdot A^2 \frac{M^2 - 1}{3 \log_2 M} \quad (5.6)$$

Puisque la fonction h(t) est normée, la distance minimale entre deux signaux est définie par :

$$d_{min}^2 = \min_{i \neq j} (\alpha_j - \alpha_i)^2 = 4 \; A^2 \qquad \text{Où} \qquad d_{min} = 2A$$

d_{min} :La distance minimale ne dépend pas de la taille de l'alphabet mais la puissance transmise est proportionnelle à M.

- puissance transmise est :

$$P_t = \frac{M^2 - 1}{\log_2 M} \quad (5.7)$$

- L'énergie moyenne par symbole est définie par :

$$E_b = E_b \log_2 M \qquad \text{avec} \qquad E_b = \frac{p_e}{D_b} \tag{5.8}$$

- La valeur de A est définie à partir de E_b par :

$$A = \sqrt{E_b \frac{3\log_2 M}{M^2 - 1}} \tag{5.9}$$

La distance minimale est définie par :

$$d_{min} = 2A = 2\sqrt{E_b \frac{3\log_2 M}{M^2 - 1}} \tag{5.10}$$

5.2.1.1 Modulation par déplacement d'amplitude (MDA)

La probabilité d'erreur par symbole en fonction du rapport Eb/N0 est donnée par la formule (5.1) d'après [6]

- Il est possible de comparer les MDA entre elles, en utilisant la probabilité d'erreur par symbole en fonction du rapport Eb/N0.

$$P_S(e) = \frac{M-1}{M} \operatorname{erfc}\left(\sqrt{\frac{3\log_2 M}{M^2 - 1} \cdot \frac{E_b}{N_0}}\right) \tag{5.11}$$

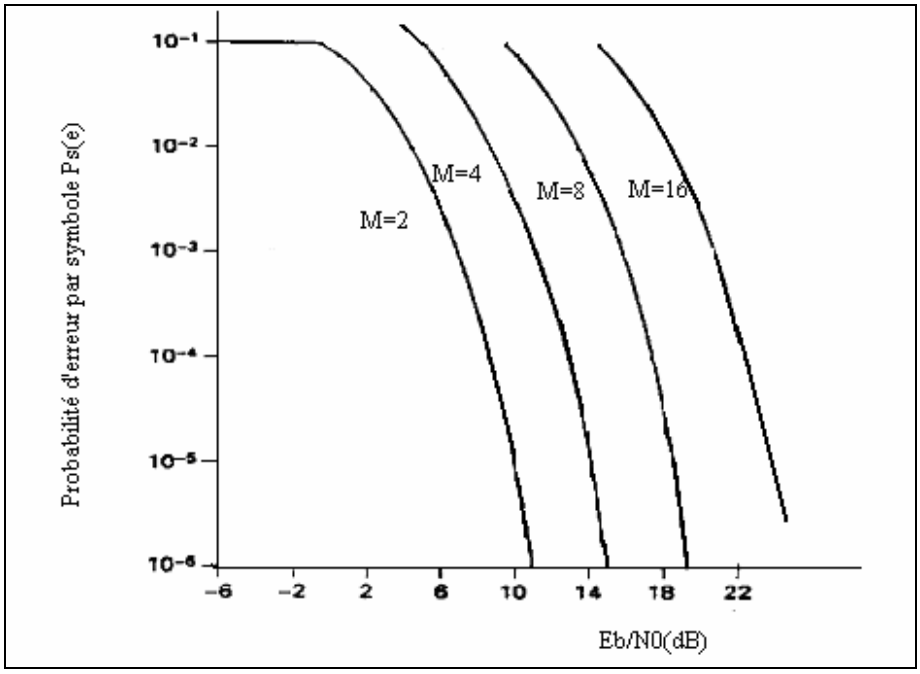


Figure .5.1 : La probabilite d'erreurs par symbole p_S (e) en fonction de Eb/ N_0

Nous avons tracé la courbe du taux d'erreurs binaire en fonction du signal sur bruit pour les différents M = 2, 4, 8, 16, 32,64

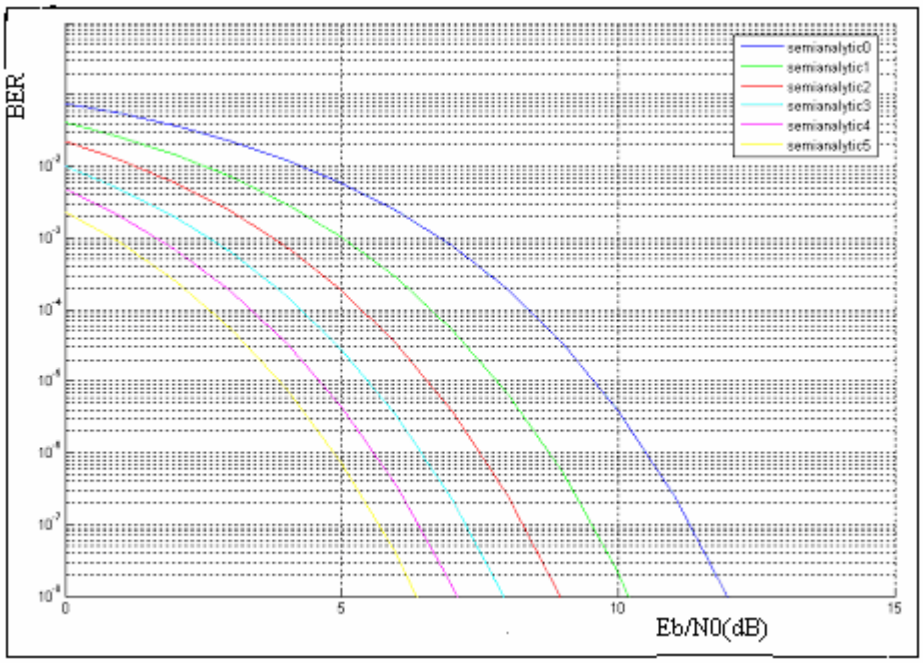


Figure .5.2 : Le taux d'erreurs binaires pour la modulation M-aires(MDA) en fonction de Eb/No

- Interprétation de la simulation sur la MDA

La tentation d'augmenter M (c'est à dire le nombre de bits transmis par symbole) est grande mais présente les avantages et les inconvénients suivants:

- L'efficacité spectrale augmente, (pour une largeur de la bande w donnée):

$$\eta=(\frac{1}{t.B}\log_2 M) \qquad (5.12)$$

- Malheureusement, la probabilité d'erreur par symbole ps(e) augmente aussi, et, pour ne pas la dégrader, il sera nécessaire d'augmenter l'énergie émise par bit E_b.
- Finalement, ce type de modulation est simple à réaliser mais est assez peu employé pour M>2 car ses performances sont moins bonnes que celles d'autres modulations, notamment pour sa résistance au bruit.
- Cette probabilité d'erreur par symbole $p_s(e)$ est tracée en fonction de Eb/N0 et du paramètre M à la figure (5.1). On peut alors constater que pour conserver une probabilité d'erreur par symbole, il faut aussi augmenter le rapport Eb/N0; Autrement dit, il faut augmenter l'énergie émise par bit E_b.

- Pour M = 4, le rapport $E_b/N0$ nécessaire à une probabilité d'erreur donnée est 4 dB plus grand que pour M =2. Pour M grand, le rapport $E_b/N0$ doit être augmenté de 6 dB chaque fois que l'on double M c'est-à-dire chaque fois que l'on ajoute un bit par symbole émis.
- Du point de vue pratique, c'est la probabilité d'erreur par bit $P_b(e)$ qui est la plus importante déterminer. Si on néglige la probabilité d'erreur entre symboles non voisins et si deux symboles voisins ne diffèrent que d'un bit (code de gray), alors la probabilité d'erreur par bit $P_b(e)$ peut s'écrire:

$$P_b(e)=\frac{P_s(e)}{\log_2 M} \qquad (5.13)$$

Car avec un symbole erroné, seulement un bit sur $n=\log_2 M$ est erroné.

- On constate quand chaque fois que M augmente le rapport signal sur bruit diminue.
- L'augmentation de M n'influe pas sur le taux d'erreurs binaire mais par contre une augmentation M entraîne une augmentation du rapport signal sur bruit. M augmente Eb/No augmente.
- On pourrait aller loin comme ça, mais l'on voit que plus on code de bit par symbole, plus les symboles sont rapprochés et donc plus on est sensible au bruit. Un symbole très bruité et donc éloigné de son emplacement d'origine, peut être confondu avec le symbole adjacent (d'où l'utilité des opérations d'entrelacement et de correction d'erreurs).

5.2.1.2 . Modulation par déplacement de phase (MDP)

Comme nous l'avions fait pour les MDA, il est possible de comparer les MDP entre elles, en utilisant la probabilité d'erreur par symbole peut en fonction du rapport Eb/N0.
L'augmentation de M réduit la distance entre symboles adjacents sur la constellation et cela dégrade naturellement les performances..
En fonction de ce rapport, on trouve en bibliographie [6] que la probabilité d'erreur par symbole est donnée par la relation:

$$p_s(e)=\operatorname{erfc}\left(\sqrt{\log_2 M\cdot\frac{E_b}{N_0}}.\operatorname{SIN}\frac{\pi}{M}\right) \qquad (5.14)$$

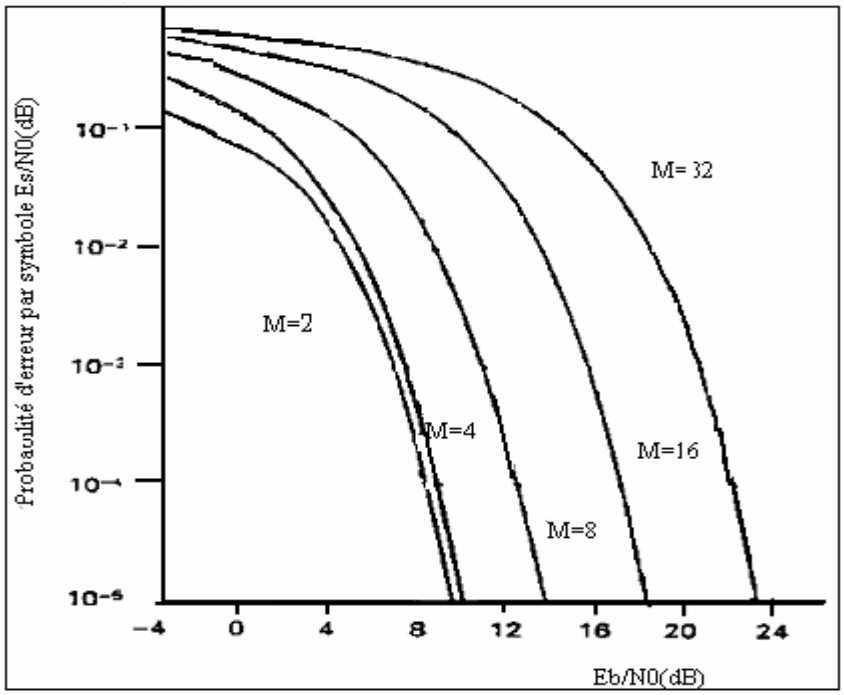


Figure. 5.3 : Probabilités d'erreurs par symbole de la MDP

Cette probabilité d'erreur par symbole $P_s(e)$ est tracée à la figure (5.6) pour M allant de 2 à 32 en fonction de E_b /N0.

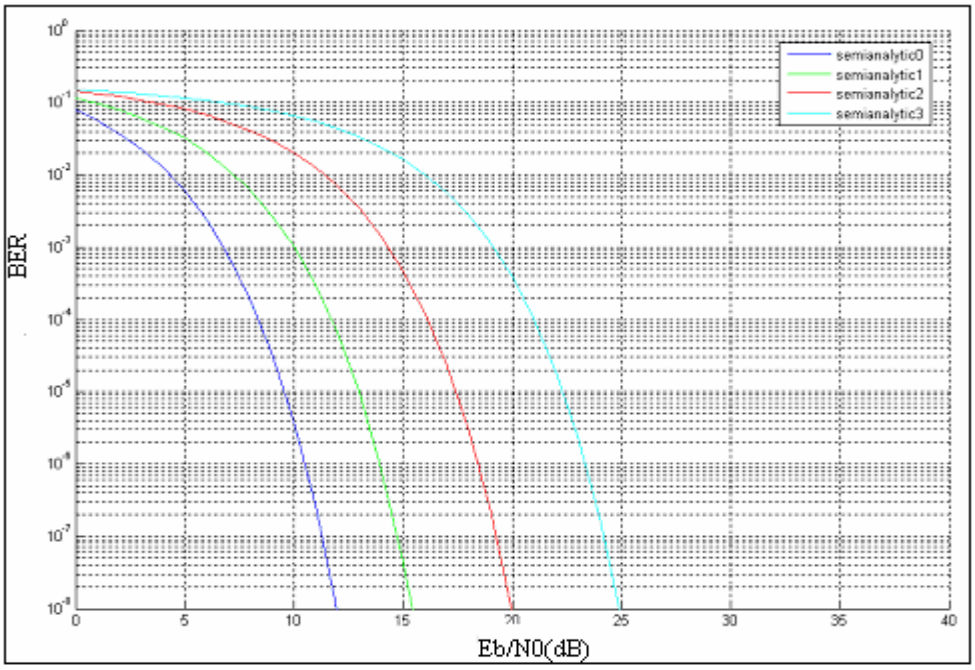


Figure.5.4 : La courbe du taux d'erreurs TEB(BER) en fonction du signal sur bruit pour différents états de M

L'interprétation de la simulation sur la MDP

- Pour conserver une probabilité d'erreur par symbole constante lorsque M augmente, il faut aussi augmenter le rapport E_b /N0. Autrement dit, il faut augmenter l'énergie émise par bit E_b .
- Pour M = 8, le rapport E_b /N0 nécessaire à une probabilité d'erreur donnée est 4 dB plus grand que pour M =4. Pour M grand, le rapport E_b /N0 doit être augmente de 6 dB chaque fois que l'on double M c'est-à-dire chaque fois que l'on ajoute un bit par symbole émis.
- Dans le cas de l'utilisation d'un code de gray et en négligeant la probabilité d'erreur entre symboles non voisins, alors la probabilité d'erreur par bit $P_b(e)$ peut s'écrire:

$$p_b(e)=\frac{p_s(e)}{\log_2 M} \qquad (5.15)$$

- Chaque fois que le nombre d'état augmente chaque fois que le rapport E_b /N0 augmente.
- La tentation d'augmenter M (c'est à dire le nombre de bits transmis par symbole) est grande et présente les avantages et les inconvénients suivants:

- L'efficacité spectrale augmente, (pour une largeur de la bande w donnée)et elle est égale à :

$$\eta=\frac{1}{t.B}\log_2 M \qquad (5.17)$$

- La probabilité d'erreur par symbole $p_s(e)$ augmente aussi, et, pour ne pas la dégrader, il est nécessaire d'augmenter le rapport signal sur bruit, cette augmentation restant raisonnable jusque M = *16*.
- Nous avons vu que la complexité de l'ensemble émission/réception de la MDP augmente avec M. Cependant cette complexité n'est pas très élevée et fait de la MDP une modulation fréquemment utilisée pour M allant de 2 à 16 avec de bonnes performances.
- Dans les inconvénients de la MDP, citons l'existence de sauts de phase importants de $\pm\pi$ radiants qui font apparaître des discontinuités d'amplitude. Les modulations décalées sont une solution à ce problème.

Remarque:

La forme rectangulaire de l'impulsion, qui est une condition nécessaire pour le maintien de la propriété d'enveloppe constante, implique que la largeur de bande du signal MDP est infinie. Pour économiser le spectre un filtrage réduisant la bande occupée par le signal et entraînant une détérioration acceptable de l'enveloppe s'impose donc. Ainsi dans la pratique le signal MDP est un MDP filtre, il perd la forme d'impulsion rectangulaire, mais il conserve la constellation circulaire.

5.2.1.3 Comparaison de la MDA et la MDP

La courbe du taux d'erreurs TEB(BER) en fonction du signal sur bruit pour les différents états de M (théorique) pour la modulation QAM, PSK, FSK (M=8).

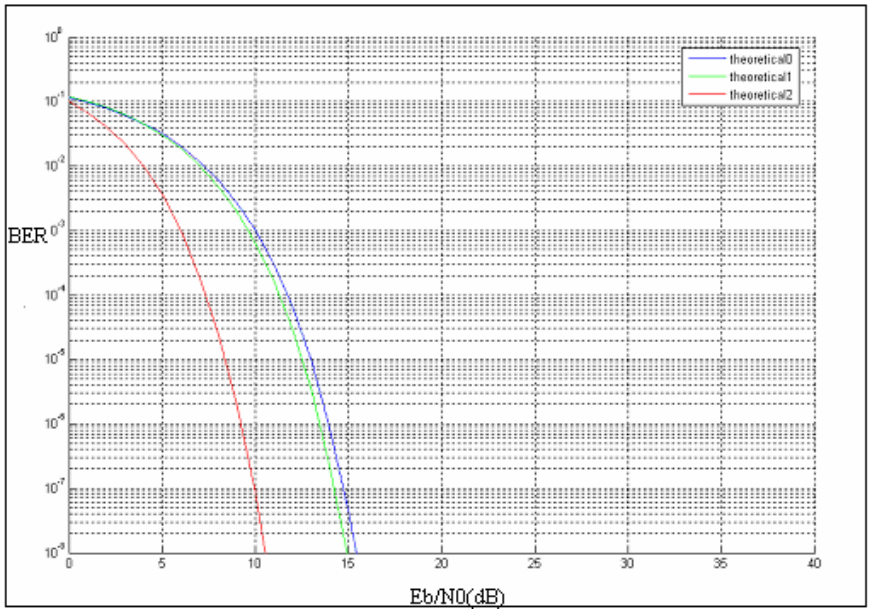


Figure. 5.5 : Courbe de la modulation ASK, QAM et FSK pour M=8

On constate que pour M=8 la courbe de PSK et celle de QAM sont presque confondue (deuxième et la troisième sur le graphe) par contre FSK décalée.

La comparaison de la MDA avec la MDP en fonction de M peut se faire a partir des courbes de probabilité d'erreur par symbole $p_s(e)$. Par exemple, pour une probabilité d'erreur par symbole $p_s(e)$ de 10^{-5} et pour un rapport signal à bruit $E_b/N0$ de 14 dB, la MDA ne peut émettre que 2 bits par symbole (M = 4), là où la MDP peut en émettre 3 bits (M = 8).

- Ceci donne un net avantage à la MDP pour M allant de 2 à 16. Pour des valeurs de M supérieures à 16 la dégradation des performances de la MDP conduit à

rechercher d'autres modulations aux prix d'une complexité accrue des modulateurs et des démodulateurs.

- Du point de vu de la simplicité de réalisation c'est la MDA qui est avantagée, ceci venant du fait qu'elle est toujours mono dimensionnelle.
- La MDA et la MDP ne constituent pas une solution satisfaisante pour utiliser efficacement l'énergie émise lorsque le nombre de points M est grand. En effet, dans la MDA les points de la constellation sont sur une droite, et dans la MDP les points sont sur un cercle. Or, la probabilité d'erreur est fonction de la distance minimale entre les points de la constellation, et la meilleure modulation est celle qui maximise cette distance pour une puissance moyenne donnée.

5.2.1.4 Modulation par déplacement de fréquence (MDF)

Il est possible de comparer les MDF-M entre elles, en utilisant la probabilité d'erreur par bit en fonction du rapport E_b /N0. Les courbes données ici, figure (5.6), correspondent à une MDF-M avec détection cohérente et sont voisines d'une MDF-M avec détection non cohérente.

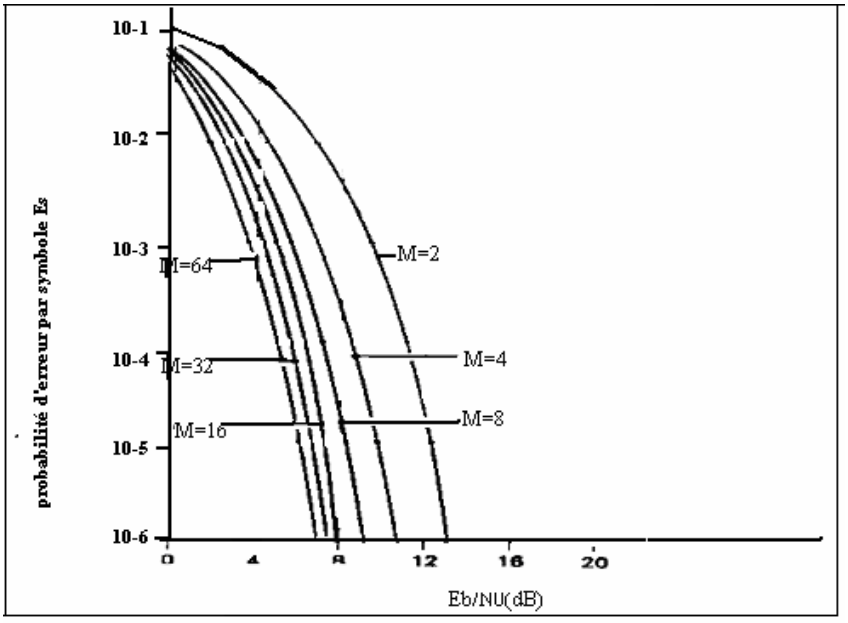


Figure.5.6 : Probabilité d'erreurs par bit de la modulation m-aires (MDF)

- Ces courbes montrent que contrairement aux modulations MDA et MDP, les performances sont améliorées lorsqu'on augmente M. Cependant l'augmentation de M entraîne aussi l'augmentation de l'occupation spectrale.

5.2.1.5 Efficacité spectrale des modulations

Tableau 5.1 : Efficacité spectrale

Type de modulation	Efficacité spectrale maxi (α=0) d_B /b_t(bit/s.Hz
MDP-2(BPSK)	1
MDP-4(QPSK)	2
MDP-8 (8-PSK)	3
MAQ-16(16-QAM)	4
MAQ-64(64-QAM)	6
MAQ-256(256-QAM)	8

Observations:

- On constate que la modulation MDP-4 possède les mêmes performances en probabilité d 'erreurs que la modulation MDP-2 voir figure (5.7) soit:

$$P(e)=q\sqrt{2.\frac{E_b}{N_0}} \qquad (5.18)$$

- Cependant, l'efficacité spectrale en MDP-4 est le double de celle obtenue en MDP-2, ce qui permet de doubler le débit binaire sans accroissement de la bande passante.
- La modulation MDP-4 constitue une sorte d'optimum et se trouve donc très utilisée pour cette raison.
- De façon plus générale, l'intérêt par rapport à la MDA des modulations de type « bidimensionnel » MDP-M et essentiellement MAQ-M, est ici clairement mise en évidence: En MAQ-M, l'efficacité spectrale est doublée par rapport E_b / N_0 (cependant, ce type de modulation résiste mal aux non linéarités du canal).
- On constate un phénomène « d'échange puissance contre bande passante) » en effet pour un débit binaire et une probabilité d'erreurs donnés, l'augmentation de M permet une réduction de la bande passante (efficacité spectrale croit) mais exige, en contre partie, une augmentation de la puissance (rapport de E_b /N_0 plus élevé).

5.2.1.6 Les courbes du taux d'erreurs TEB en fonction du signal sur bruit pour les différents états

- La courbe du taux d'erreurs TEB en fonction du signal sur bruit pour les différents états de M (théorique) pour la modulation QAM, PSK, FSK (M=8)

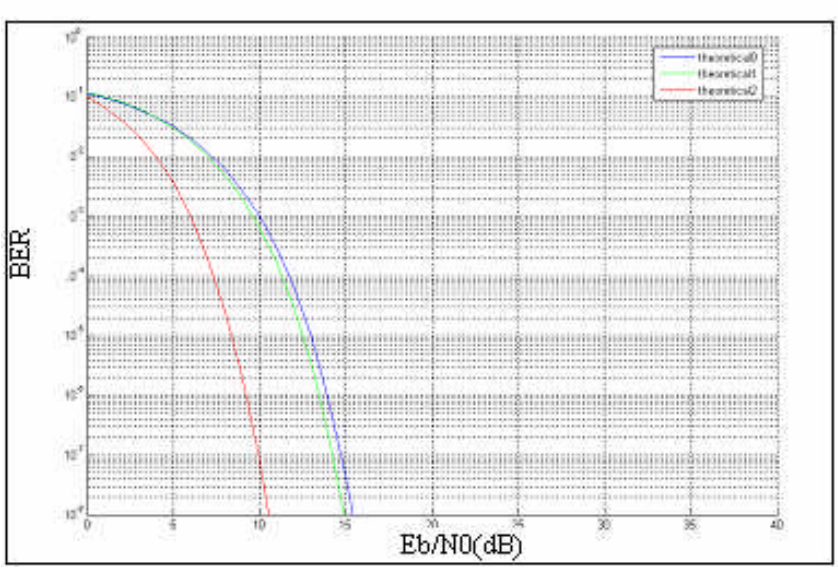


Figure.5.7 : Courbes du taux d'erreurs binaires en fonction de la modulation QAM (bleu),PSK(vert) et FSK(rouge) pour M=8

On constate que pour M=8 la courbe de PSK et de QAM sont légèrement confondues (deuxième et la troisième sur le graphe) par contre FSK est décalée.

- La courbe du taux d'erreurs TEBen fonction du signal sur bruit pour les différents états de M (théorique) pour la modulation QAM, PSK, FSK(M=16).

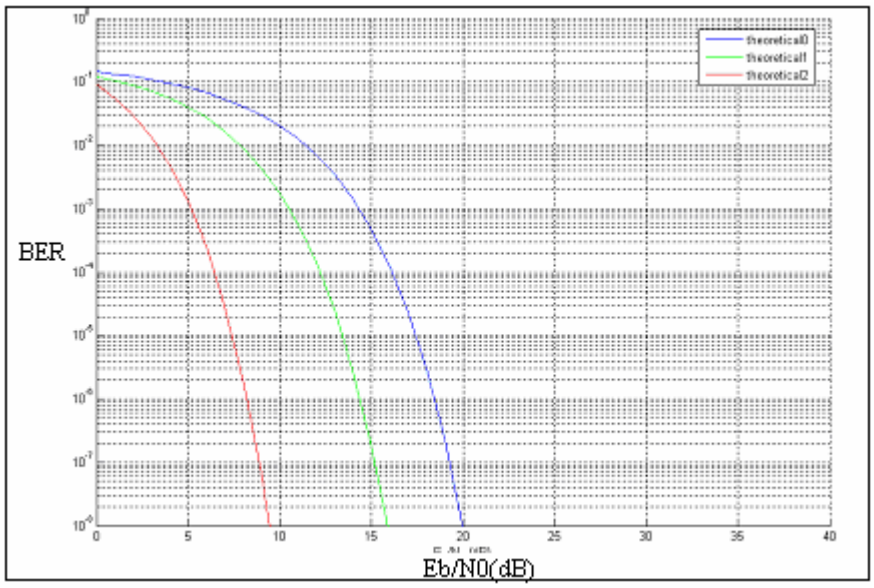


Figure 5.8 : Courbes du taux d'erreurs binaires en fonction de la modulation QAM (bleu), PSK (vert) et FSK (rouge) pour M=16

On constate plus M augmente plus l'écart entre la modulation PSK et QAM est important par contre la modulation FSK reste presque stable pour M supérieur à 16

La courbe du taux d'erreurs TEB(BER) en fonction du signal sur bruit pour les différents états de M pour la modulation QAM, PSK, FSK (M=32).

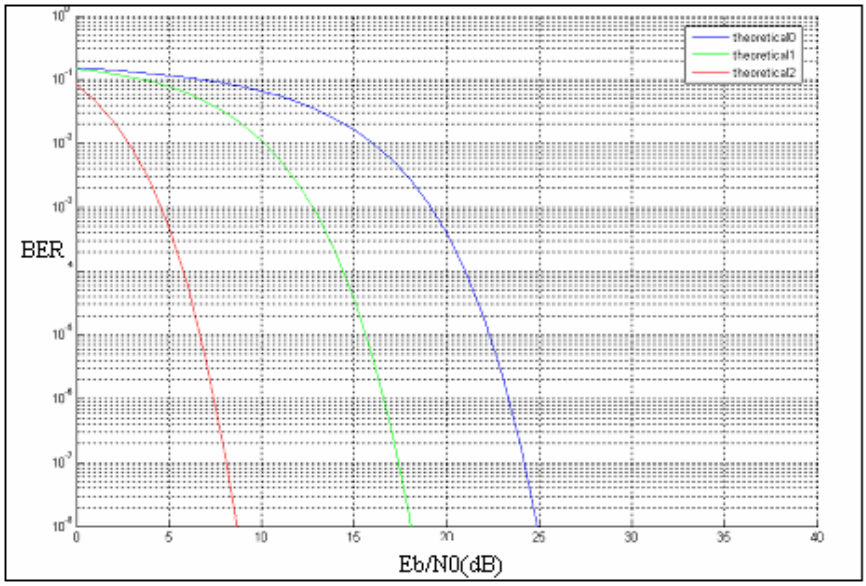


Figure 5.9 : Courbes du taux d'erreurs binaires en fonction de la modulation QAM (bleu), PSK (vert) Et FSK (rouge) pour M=32

Pour M=32 même remarque que pour M=16 sauf que la courbe de la modulation FSK devient plus raide.

- La courbe du taux d'erreurs TEB(BER) en fonction du signal sur bruit pour les différents états de M pour la modulation QAM, PSK, FSK (M=64).

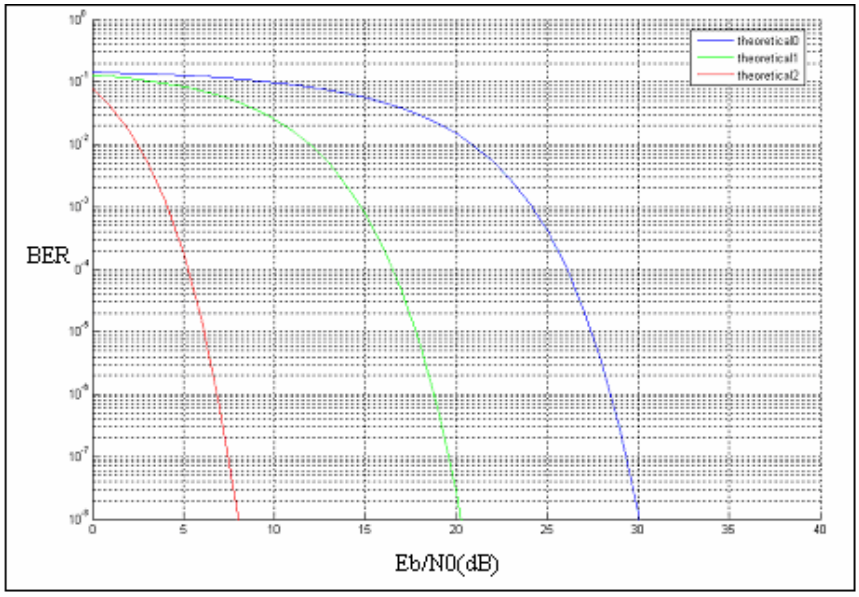


Figure 5.10 : Courbes du taux d'erreurs binaires en fonction de la modulation QAM (bleu), PSK (vert) Et FSK (rouge) pour M=64

Pour M=64 la courbe de PSK et de QAM sont décalées (deuxième et la troisième sur le graphe) et le rapport signal sur bruit augmente avec l'augmentation de M, par contre ce rapport diminue pour la FSK en fonction de l'augmentation de M

5.3 Comparaison des performances du canal en vue du taux d'erreurs binaires(TEB)

La figure (5 11) nous montre l'efficacité spectrale de quelques modulations m-aires linéaire:

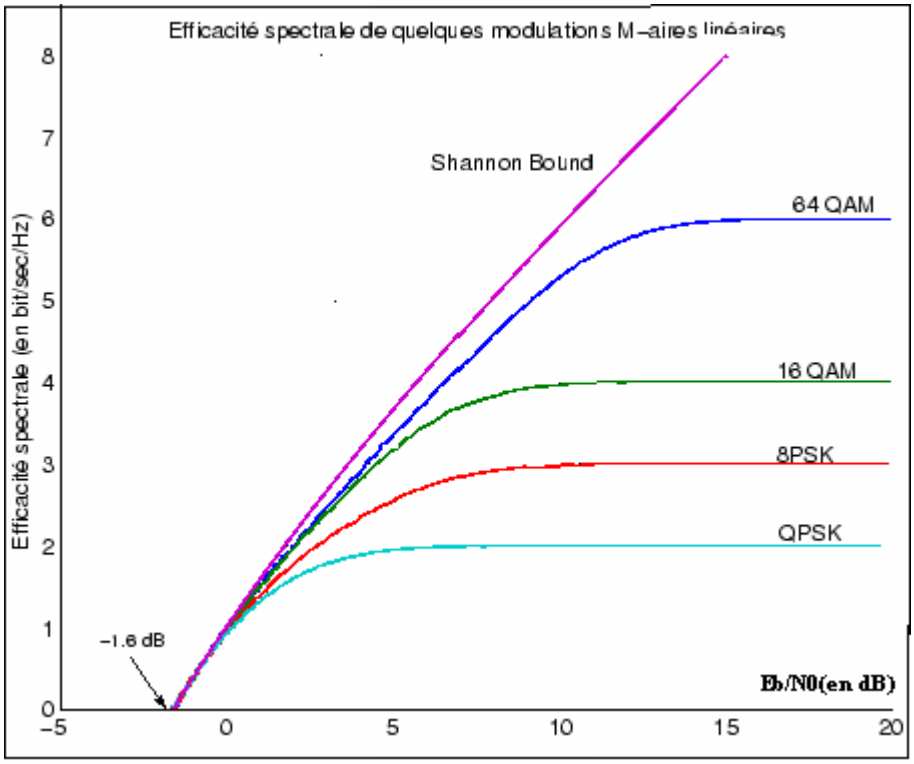


Figure 5.11 : Efficacité spectrale de modulation m-aires en fonction du Eb/N0

Constatation:

- A faible rapport E_b /No, la capacité maximale du canal est quasiment identique pour toutes les formes d'onde. Il est ainsi inutile d'adopter des modulations d'ordre élevé dans cette région même si le processus de codage canal permet d'approcher sa capacité maximale.
- Par contre, dans le cas d'un fort rapport E_b /No, les formes d'ondes d'ordre élevé sont plus attractives d'un point de vue efficacité spectrale.
- On peut aussi remarquer que la capacité maximale d'une modulation M-aire, qui est égale à $\log_2$ (M), est théoriquement irréalisable notamment à faible rapport signal sur bruit. Ce fait traduit la nécessite de l'utilisation d'un processus de codage canal pour assurer une communication sans erreurs.
- Bien évidemment, le rendement du code optimal est fonction du rapport E_b /No. Plus précisément, en notant ρ_m le taux de codage optimal qui permet d'atteindre la

capacité maximale du canal η_m d'une modulation m-aire donnée, on peut exprimer ce taux de codage optimal par l'équation:

$$\rho_M = \frac{\eta_M}{\log_2 M} \qquad (5.19)$$

La figure (5.12) illustre l'évolution du rendement du code optimal en fonction du rapport Eb/No.

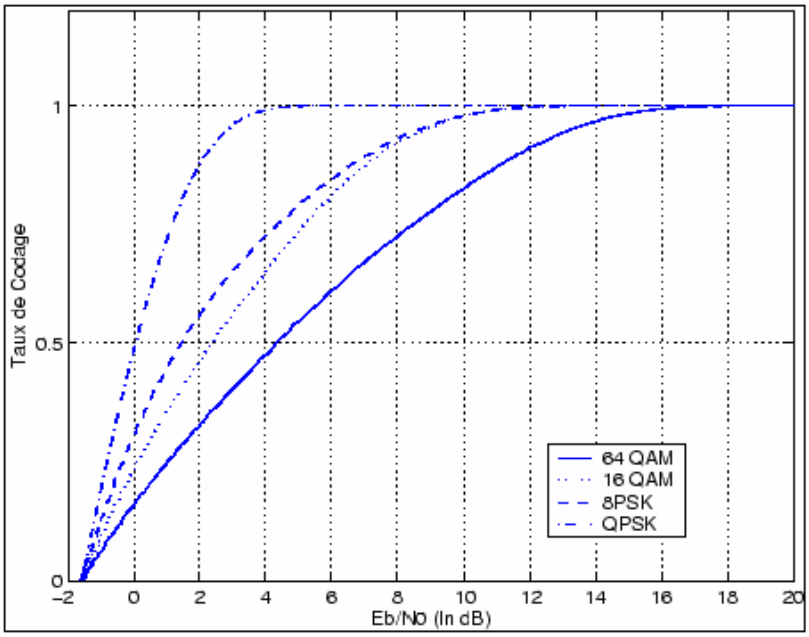


Figure 5.12 : Taux de codage optimal en fonction du E_b /No pour les modulations M-aires

- A un même rapport E_b /No, les modulations d'ordre moins élevé nécessitent un taux de codage plus élevé, ceci est du au fait que ces formes d'ondes sont plus efficaces en puissance que les modulations à ordre plus élevé.
- Autre que le rendement, ce résultat ne fournit aucune information concernant le code qui permet d'atteindre la capacité maximale.

Conclusion :

- Le choix de la modulation et du taux de codage doit s'effectuer d'une façon conjointe. Ce choix doit tenir compte des conditions de propagation.
- Il se trouve que la capacité d'une forme d'onde est affecté par d'autres éléments extérieurs telles que la gradation due à une synchronisation imparfaite.

- Les non-linearités du canal ainsi que celles des amplificateurs peuvent aussi dégrader les performances de la forme d'onde par rapport aux performances théoriques. L'ampleur de la dégradation varie d'une forme d'onde à une autre.

Pour pouvoir comparer le rendement des différents types de bandes du signal transmis, et des différents nombres d'état de la modulation, nous avons tracé le rapport Eb/N0 permettant d'obtenir un TEB donné en prenant en considération les paramètres cites ci-dessus.

Cette série de simulation, visait à prédire les conséquences d'un choix de ces paramètres sur la performance du système.

- La dégradation du TEB augmente avec l'augmentation du nombre d'état.
- Les éléments qu'ont été données dans les paragraphes ci-dessus permettent de comprendre l'intérêt des systèmes à M niveaux qui suivant les systèmes ont trois catégories d'avantages:
  - Soit (saut de fréquence à M niveaux) un taux d'erreurs plus faible que le système binaire équivalent à même puissance d'émission mais au prix d'une largeur de bande plus importante.
  - Soit (saut de phase ou d'amplitude à M niveaux) une largeur de bande beaucoup plus faible que le système binaire équivalant mais au prix d'un taux d'erreurs plus élevé ou plus exactement a taux d'erreurs constant, il faut une puissance d'émission plus importante.
  - Pour une plage de signal donnée plus le nombre d'états augmente, plus la probabilité d'erreurs augmente. Il n'est donc pas possible, pour un rapport signal/bruit donné, d'augmenter indéfiniment le débit binaire en augmentant le nombre d'états.
- La probabilité d'erreurs diminue très rapidement quand le rapport signal/bruit augmente. C'est en fait un des nombreux avantages de la transmission numérique.
- On remarque que pour B et T donnés, l'efficacité spectrale augmente, comme on pouvait s'y attendre, avec le nombre de bit/symbole $n = \log_2 M$. C'est en effet la raison d'être de la modulation M-aire.

5.4 Simulation de la chaîne complète

Apres avoir évaluer les performances des différentes modulations sur le plan efficacité spectrale et le taux d'erreurs binaires on passera maintenant à la simulation de la chaîne de transmission sur un canal bruite.

- On a assimile le canal bruite à un bruit blanc additionnel gaussien (BBAG) le programme est écrit en MATLAB.

Pour la simulation nous avons fait une série de test en fonction du facteur de roll-off (filtre de Nyquist), car le filtre en cosinus surélevé élimine l'IES (interférence entre les symboles) et limite la bande passante.

5.4.1 Les résultats de la réponse impultionnelle pour les différentes valeurs de roll- off.

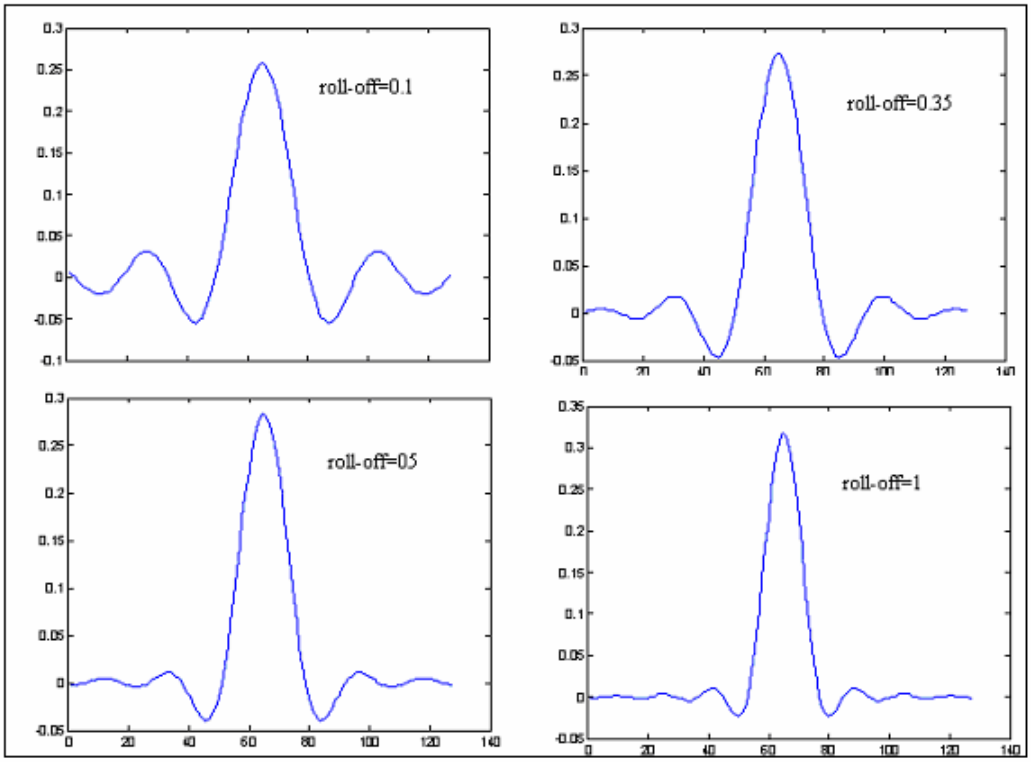


Figure 5.13 : Réponse impulsionnelle pour les différentes valeurs de roll-off

La réponse impulsionnelle en racine de Nyquist pour les différentes valeurs du roll-off.

- On voit que plus est grand est grand, plus les lobes secondaires sont de faibles amplitudes.
- Plus, α est grande, plus le maximum de la courbe augmente, il atteint la valeur de 0.33 pour α=1. Il s'ensuit, que lors d'un décalage de l'horloge d'échantillonnage, l'amplitude de l'IES est d'autant plus faible que α est grand.

5.4.2 Les résultats obtenus des fonctions de transfert en racine de Nyquist pour les différentes valeurs du roll-off

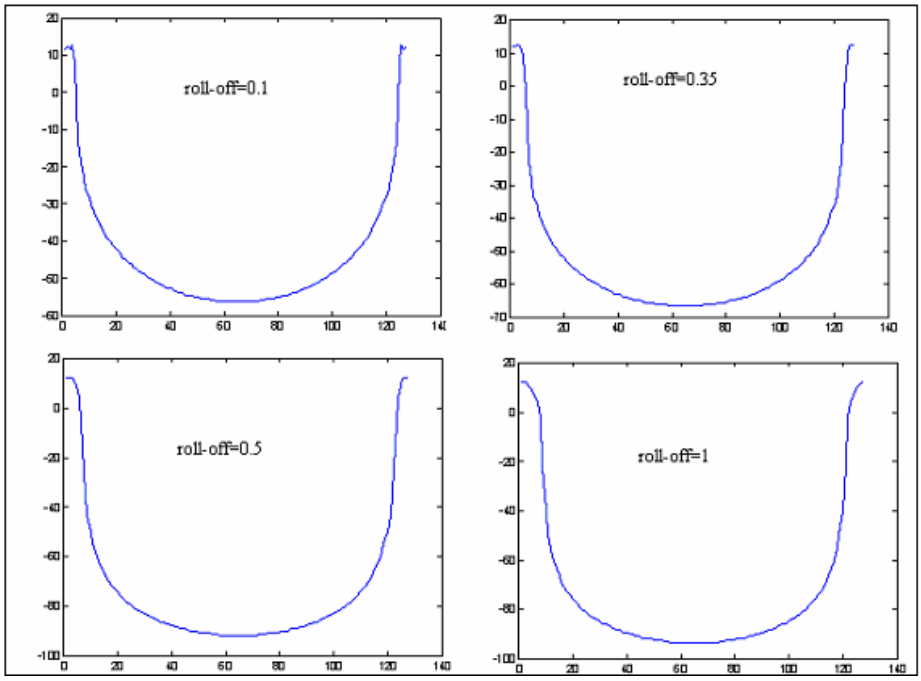


Figure 5.14 : Fonction de transfert pour les différentes valeurs de α

5.4.3Les résultats de la simulation de la condition de Nyquist

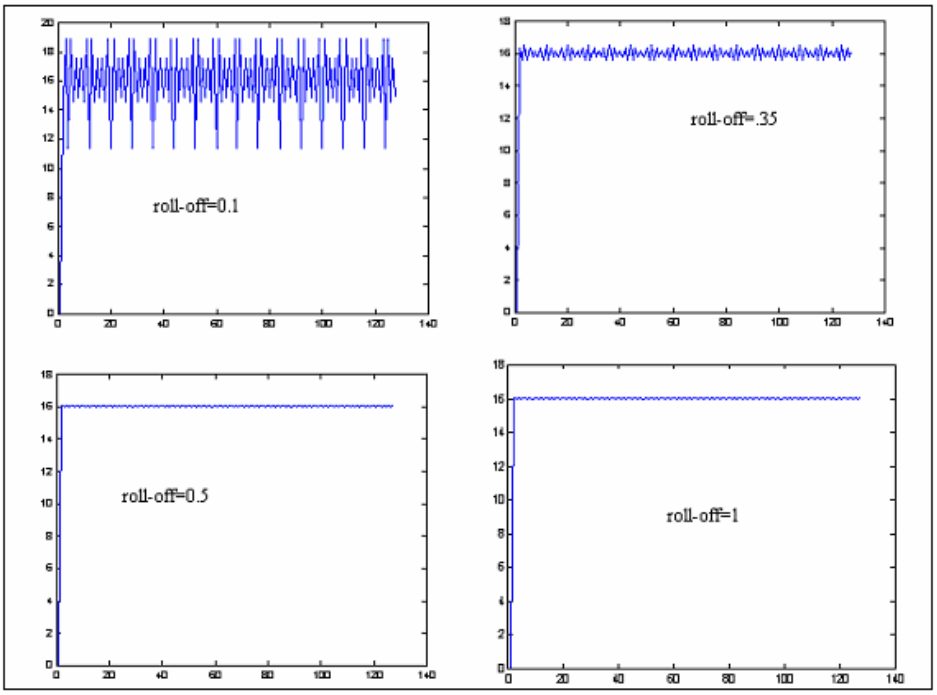


Figure 5.15 : Condition de Nyquist pour les différentes valeurs de α

5.4.4 Les résultats de la simulation du signal modulé

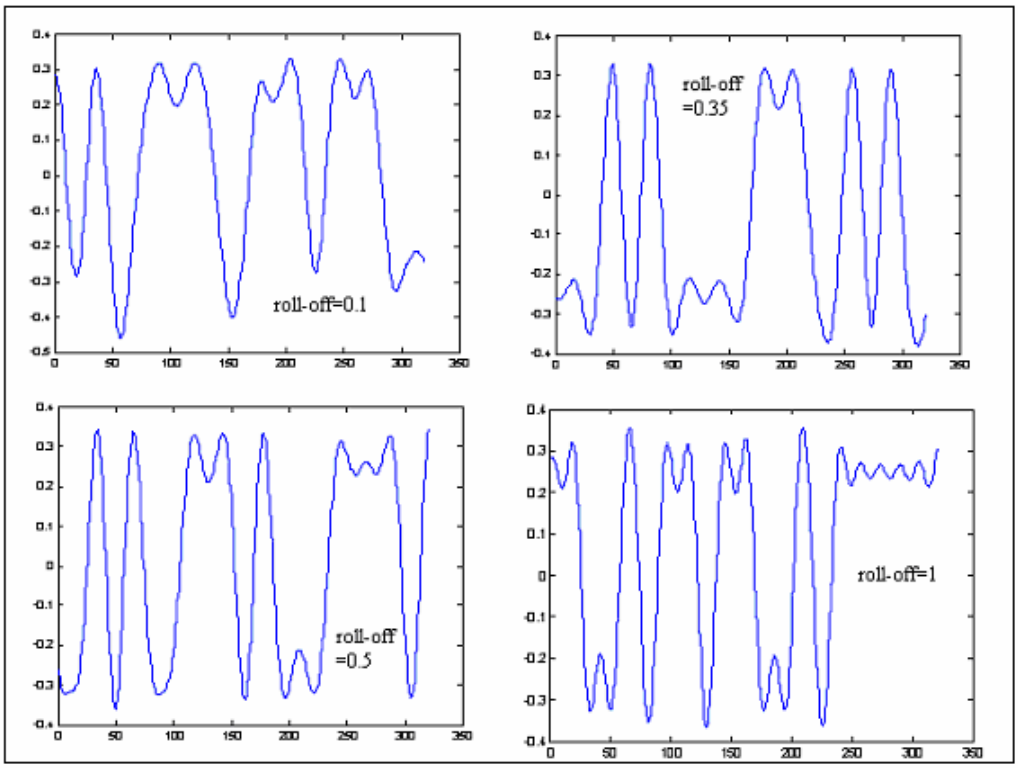


Figure 5.16 : Signal module pour les différentes valeurs de α

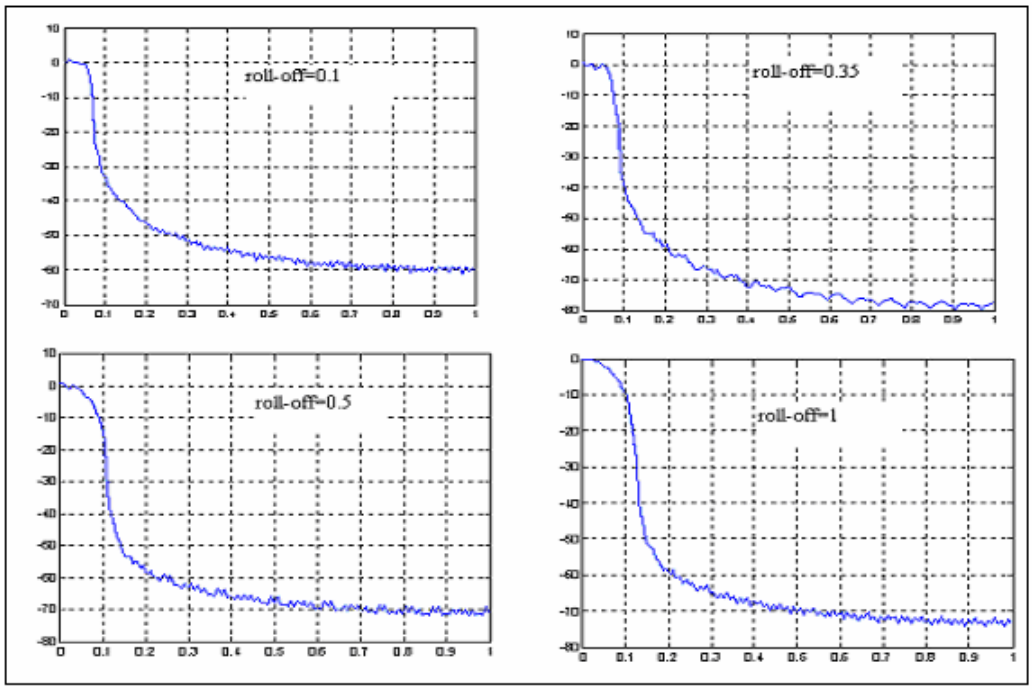


Figure 5.17 : Densité spectrale du signal modulé pour les différentes valeurs de α

5.4.5 Densité spectrale du signal module par un rectangle pour les différentes valeurs du roll-off

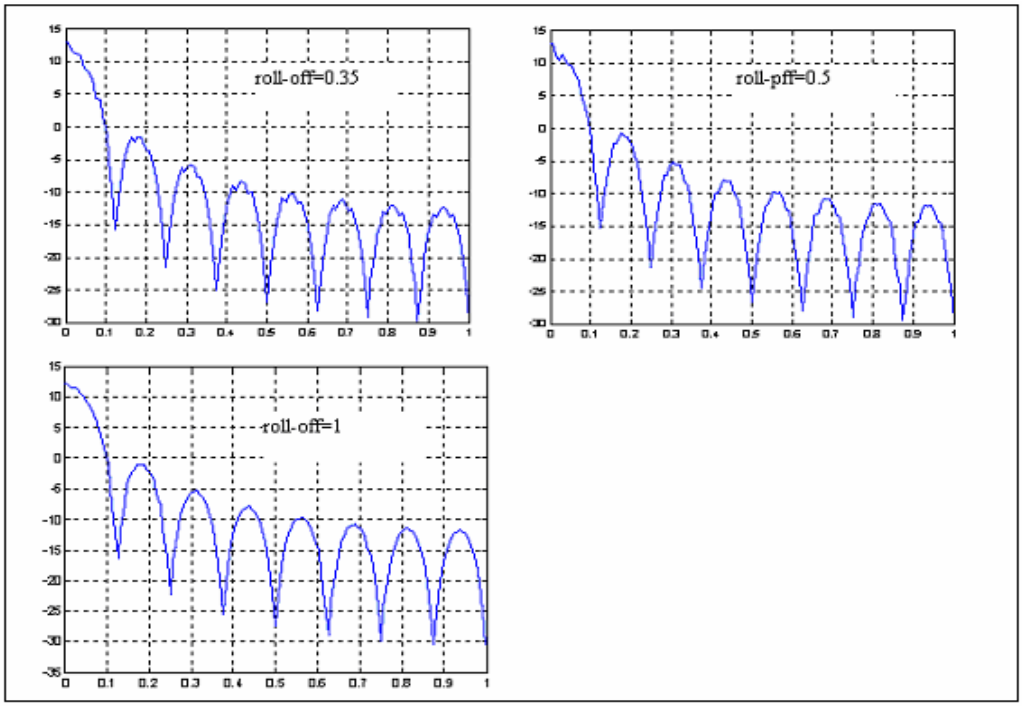


Figure 5.18 : Densité spectrale du signal modulé par un rectangle
Pour les différentes valeurs de α

5.4.6 Signal émis et reçu pour les différentes valeurs du roll-off

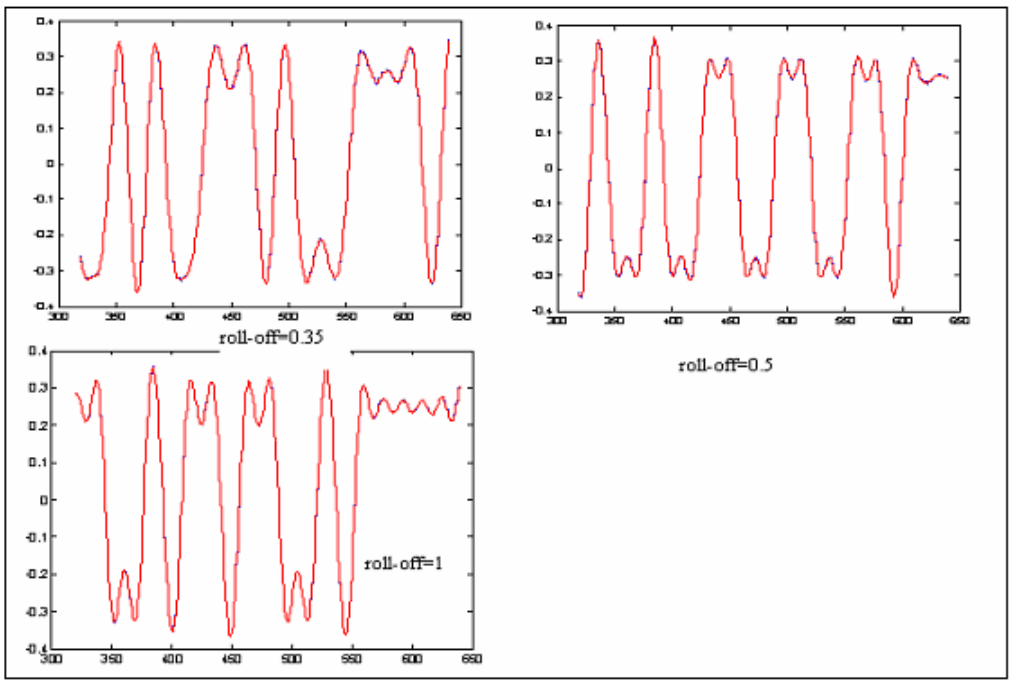


Figure 5.19 : Signal émis et reçus pour les différentes valeurs de α

5.4.7 Densité spectrale du signal reçue pour les différentes valeurs du roll-off

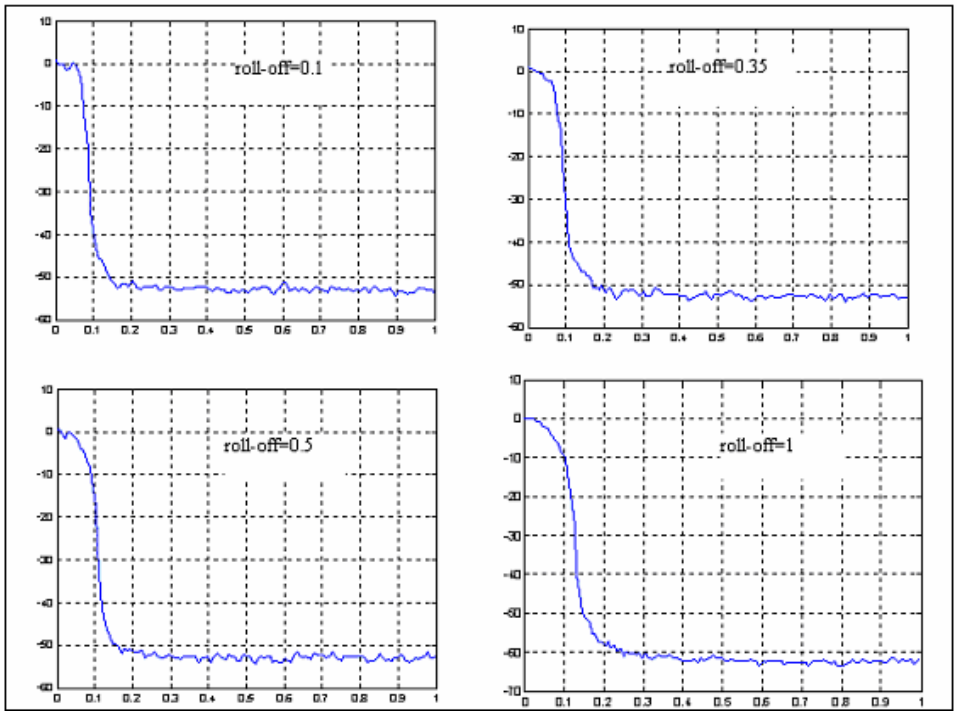


Figure 5.20 : Densité spectrale du signal reçu (bruite) pour les différentes valeurs du α

5.4.8 Représentation du diagramme de l'œil, sur le canal de nyquist, pour M = 2, avec un rapport signal sur bruit de 7dB pour les différentes valeurs du roll-off.

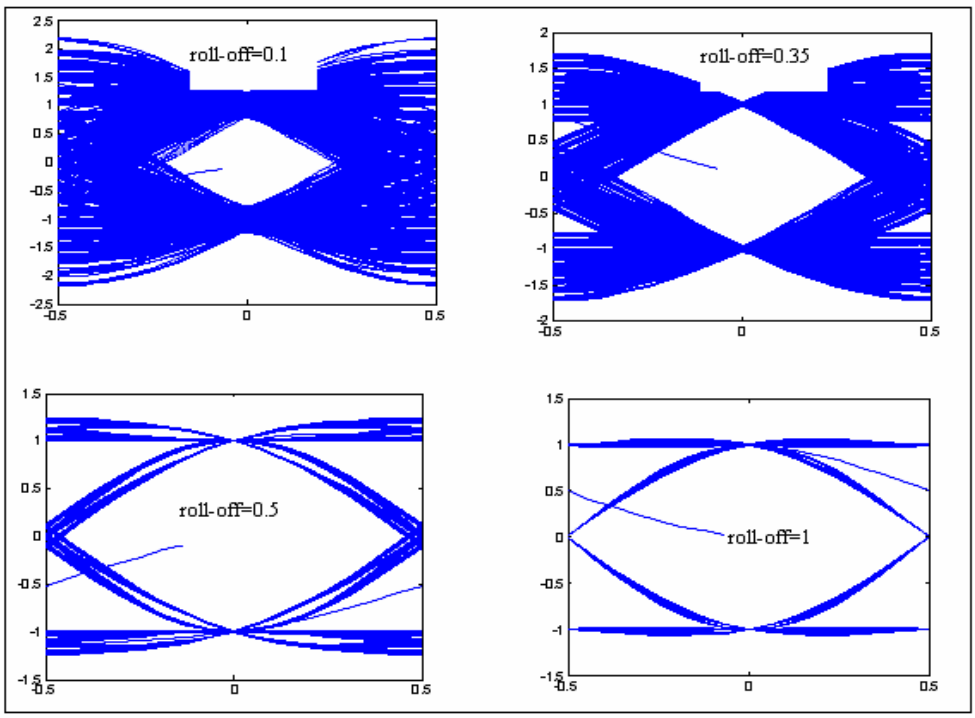


Figure 5.21 : Diagramme de l'œil pour les différentes valeurs du roll-off

Constatation:

- En absence d'IES, l'œil est complètement « ouverte » à l'instant de décision: Tous les points passent par deux points seulement en binaire et par M points en M-aire..
- On remarquera que la décision symbole par symbole sera la meilleure la où l'œil est le plus ouvert verticalement. Malgré le bruit, les niveaux significatifs des deux symboles restent relativement bien discriminables.
- La bande passante peut aussi s'exprimer en fonction du débit binaire:

  $B_t = (1+\text{roll-off})\, D_b/2\log_2 (m)$.
- La bande passante minimale théorique est égale à $D_s/2$: aucune transmission ne peut s'effectuer sans IES si la bande passante du canal est inférieur à cette limite.
- Le diagramme de l'œil se ferme horizontalement quand le facteur de roll off diminue ; Le récepteur devient sensible à la position de l'impulsion d'acquisition.
- L'ouverture de l'œil est faible, ce qui n'est guère favorable. La situation serait encore pire si on avait choisi des symboles pouvant prendre plus de deux états.
- Le diagramme en œil correspondant au même ensemble de symboles binaires.
- Le diagramme en œil est excellent; c'est normal, c'est ce qu'on recherchait test

α=0. 35.

L'observation du diagramme de l'œil fournit les indications suivantes:

- L'ouverture verticale mesure les performances contre le bruit. Plus l'œil est ouvert en hauteur, plus il est facile de discriminer les symboles en présence de bruit, donc plus la probabilité d'erreur est faible. Si le diagramme manifeste la présence d'une IES (faible), et que l'on souhaite continuer à utiliser une détection à seuil (solution sous optimale), il faudra venir échantillonner le signale aux instants où l'œil à une ouverture maximale.
- L'ouverture horizontale indique une résistance à un décalage des instants d'échantillonnage. Ainsi, plus l'œil est ouvert en largeur, plus les lobes secondaires de la réponse en temps seront faibles et plus l'accumulation des interférences dues au décalage des instants d'échantillonnage aura une influence moindre en terme de probabilité d'erreur. C'est le cas pour les fonctions en cosinus surélevé lorsque M augmente.

5.4.9 Test décodage par algorithme de viterbi

Il est souvent difficile d'établir un outil théorique qui permet de calculer le taux d'erreur binaire d'un schéma de codage/décodage. Le code utilise pour la partie émettrice c'est le code convolutif et pour la partie réception le code de viterbi.

Pour le code de correction nous avons utilise le code de viterbi (simulation par MATLAB)

Test de décodage par l'algorithme de viterbi

Probabilité d'erreur sur le canal:

Error rate = 0. 1000

Taux d'erreur en sortie

E =0

Itération =320

Résultats de l'algorithme de viterbi

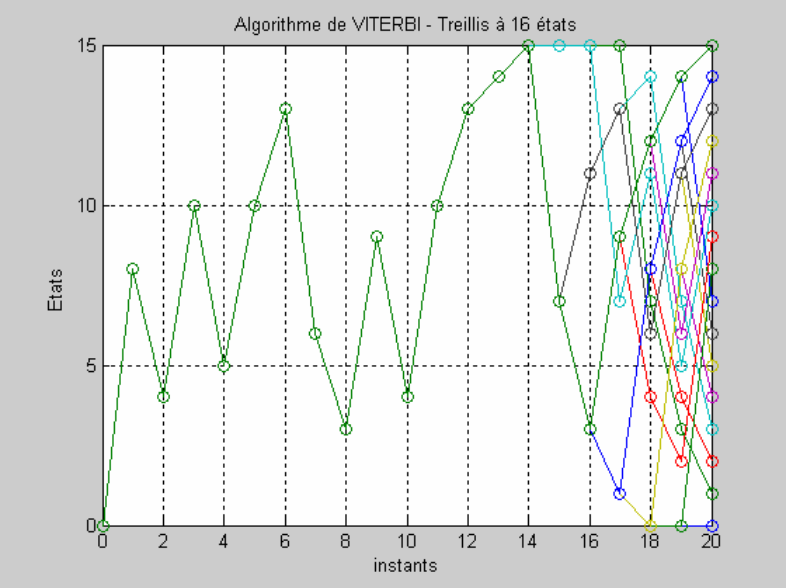


Figure 5.22 : Algorithme de Viterbi pour 16 états

5.4.10 Le cryptage

Pour la partie cryptage nous avons optés pour le cryptage IDEA.

IDEA, un algorithme de chiffrement de données par blocs, offre d'excellentes garanties de sécurité. A ce jour, personne n'a encore publie de résultats démontrant des faiblesses de l'algorithme. IDEA constitue ainsi un choix judicieux pour le cryptage de transmissions de données.

Le texte est découpe en blocs de 64 bits, re divisés en quatre blocs de 16 bits: x1, x2, x3, x4. La clé k est divisée en 8 blocs de 16 bits, puis décalé circulairement sur la gauche de 25 bits, et re divisé, et ainsi de suite jusqu'à obtenir 52 clés. Ces clés formeront 8 groupes de 6 clés (un groupe par ronde): k1, k2, k3, k4, k5, k6, et un groupe de 4 clés pour la ronde finale: k1, k2, k3, k4.

Algorithme du IDEA a été donné dans le quatrième chapitre.

Soient a, b, c et d quatre blocs de 16 bits et 52 sous-clé k[1] à k[52].

(« · » est une multiplication et « + » est une addition).

IDEA est un système de chiffrement par blocs de 64 bits, acceptant le mode de chaînage ECB (Electronic Code book), CBC (Cipher Block Chaining), OFB (output Feedback) et CFB **(**Cipher Feedback) avec une clé de 128 bits, qui tourne sur 8 rondes.

5.4.10.1 L'Algorithme de cryptage et de décryptage (avec le mode ECB) :

Entrée : **1**. m blocs de n bits X1…..Xm de texte en clair, une clé K de k bits et un . Algorithme de cryptage Ek.

2. m blocs de n bits y1…..ym de texte chiffré, une clé K de k bits et un Algorithme de cryptage Ek-1.

Résultat : **1**. m blocs de n bits y1……..ym cryptés avec Ek.

2. m blocs de n bits x1……..xm cryptés avec E_{k-1}.

Cryptage : **1. POUR** j= 1 **à** m **faire**

2. yj → E_k (xj)

3. **FIN faire**

Décryptage : **1. POUR** j= 1 **à** m **faire**

2. xj → E_{k-1} (yj)

3. **FIN faire**

5.4.10.2 Le découpage du texte en blocs de 64 bits

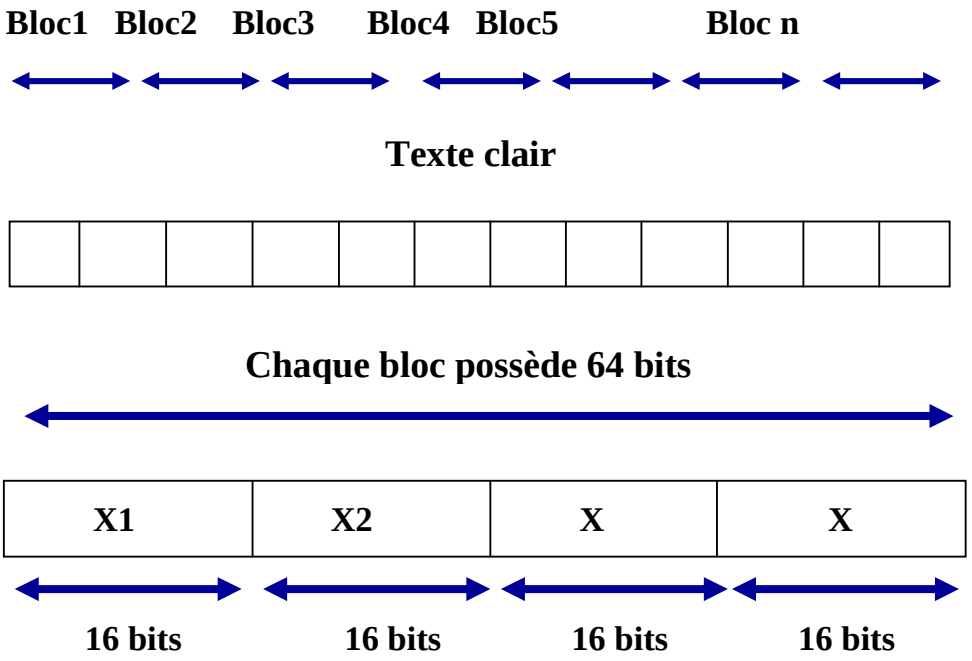


Figure 5.23 : Découpage du texte

- Les 4 sous blocs (X1 ,X2 ,X3 ,X4) deviennent des Entrées du 1er ronde
- Il y a 8 rondes au total.
- Les 4 sous blocs sont combinés par OU Exclusif, additionnés et multipliés entre eux.

5.4.10.3 Détermination des sous –clés

Les 52 sous-clés générées à partir de la clé de 128 bits sont produites comme suit:

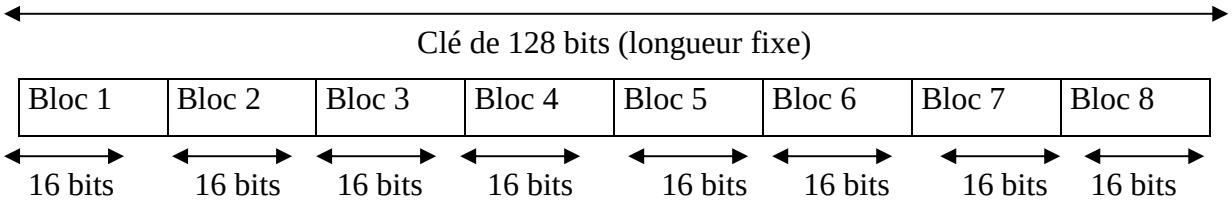
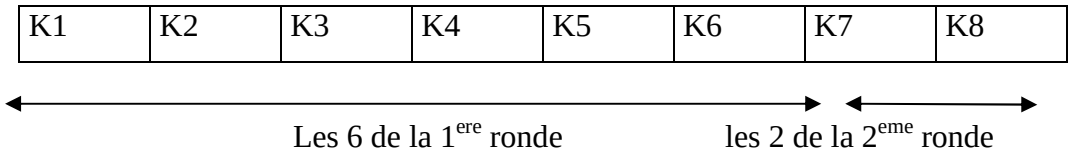


Figure 5.24 : Découpage de la clé

Donc 16 bits multiplié par 8 blocs =128 bits.

- La clé de 128 bits est divisée en huit blocs comme le montre la figure 2. Ces huit blocs sont en fait les huit premières sous-clés utilisées dans le chiffrement (les 6 de la première ronde et les 2 premières de la deuxième ronde).



- La clé de 128 bits est ensuite cycliquement décalée de 25 positions vers la gauche et à nouveau divisée en 8 sous clefs 16 bits. Ces huit blocs sont les huit sous-clés suivantes utilisées dans le chiffrement). Les 4 premières sont utilisées lors de la deuxième ronde et les 4 autres lors de la troisième ronde.

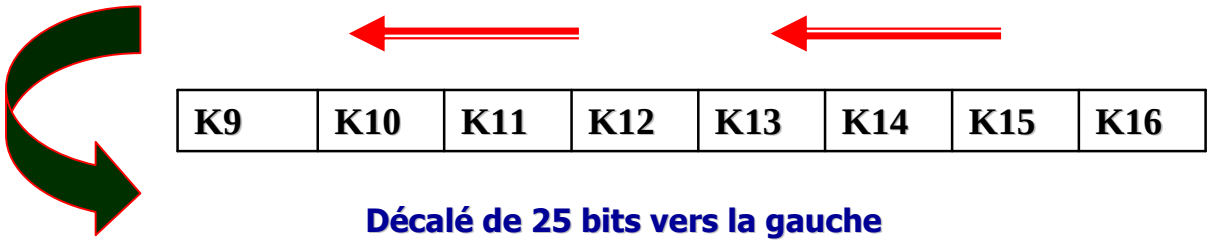


Figure 5.25 : Rotation de la clé

Le cycle est répété jusqu'à ce que les 52 sous-clés soient toutes générées. La clef est à nouveau décalée circulairement de 25 bits vers la gauche pour les 8 sous clefs suivantes, et ainsi de suite jusqu'à la fin de l'algorithme, le déchiffrement est exactement le même, excepté que les sous clefs sont inversées et légèrement différentes. Les sous clefs de déchiffrements sont inversées par rapport à l'addition ou par rapport à la multiplication des sous clefs de chiffrement.

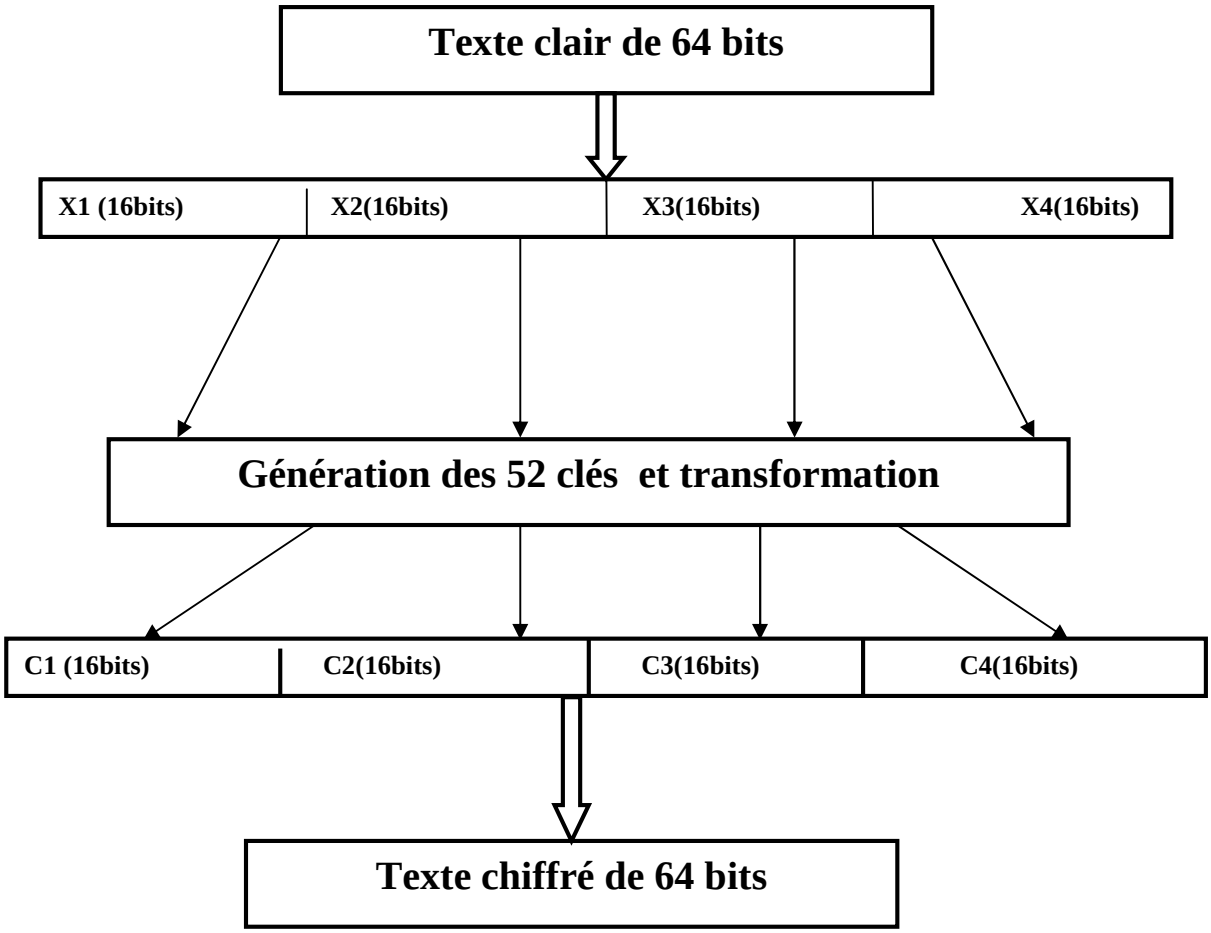


Figure 5.26 : Synoptique IDEA

Déroulement de l'algorithme

- **<u>Les Etapes d'une ronde de chiffrement:</u>**

- Etape1 = X1 * K1
- Etape2 = X2 + K2
- Etape3 = X3 + K3
- Etape4 = X4 * K4
- Etape5 = Etape1 XOR Etape3
- Etape6 = Etape2 XOR Etape4
- Etape7 = Etape5 * K5
- Etape8 = Etape6 + Etape7
- Etape9 = Etape8 * K6
- Etape10 = Etape7 + Etape9
- Etape11 = Etape1 XOR Etape9 => X1 de la ronde suivante
- Etape12 = Etape3 XOR Etape9 => X3 de la ronde suivante

- Etape13 = Etape2 XOR Etape10 => X2 de la ronde suivante
- Etape14 = Etape4 XOR Etape10 => X4 de la ronde suivante

Pour finir, on applique une étape supplémentaire après la huitième ronde :

- C1 = X1 * K49
- C2 = X2 + K50
- C3 = X3 + K51
- C4 = X4 * K52

Les 4 blocs C1, C2, C3, C4, forment alors le message chiffré.

- **Les Etapes d'une ronde de déchiffrement:**

Pour déchiffrer le texte, il faut d'abord inverser la dernière opération :

- $C1 = C1 * K1^{-1}$
- C2 = C2 - K2
- C3 = C3 - K3
- $C4 = C4 * K4^{-1}$

On applique alors les opérations suivantes selon 8 rondes, en utilisant les groupes de 6 clés en partant de la dernière à la première :

- Etape1 = C1 XOR C3 (Etape5 lors du cryptage)
- Etape2 = C2 XOR C4 (Etape6 lors du cryptage)
- Etape3 = Etape1 * K5 (Etape7 lors du cryptage)
- Etape4 = Etape2 + Etape3 (Etape8 lors du cryptage)
- Etape5 = Etape4 * K6 (Etape9 lors du cryptage)
- Etape6 = Etape3 + Etape5 (Etape10 lors du cryptage)
- Etape7 = C1 XOR Etape5 (Etape1 lors du cryptage)
- Etape8 = C3 XOR Etape5 (Etape3 lors du cryptage)
- Etape9 = C2 XOR Etape6 (Etape2 lors du cryptage)
- Etape10 = C4 XOR Etape6 (Etape4 lors du cryptage)
- Etape11 = Etape7 * $K1^{-1}$ => C1 de la ronde suivante
- Etape12 = Etape8 - K3 => C3 de la ronde suivante
- Etape13 = Etape9 - K2 => C2 de la ronde suivante
- Etape14 = Etape10 * $K4^{-1}$ => C4 de la ronde suivante

Les 4 blocs C1, C2, C3, C4 obtenus après la dernière ronde forment alors le message en clair.

Résultat du cryptage 1.

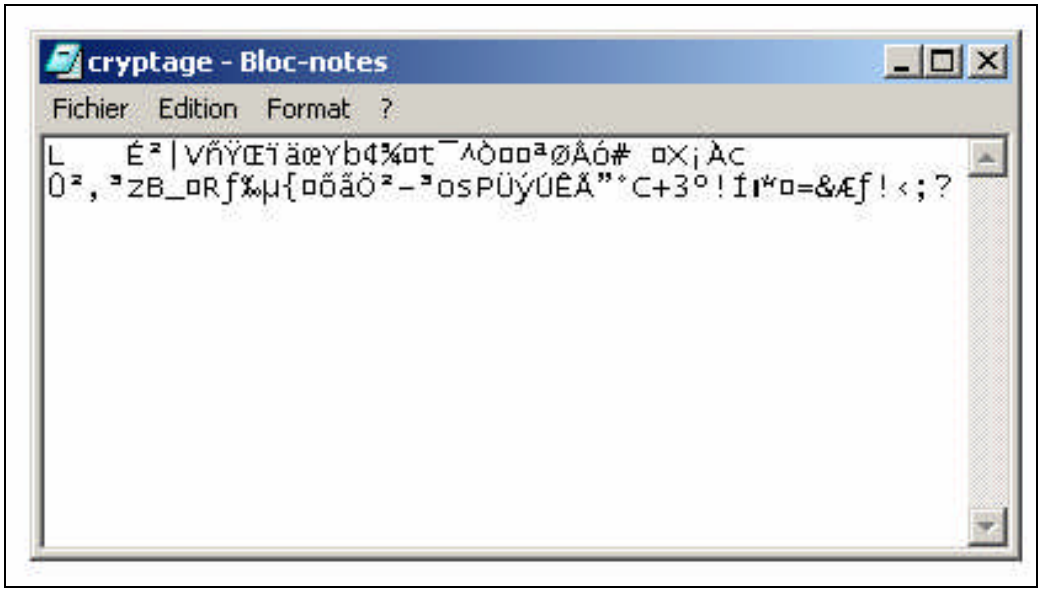


Figure 5.27.a : Cryptage

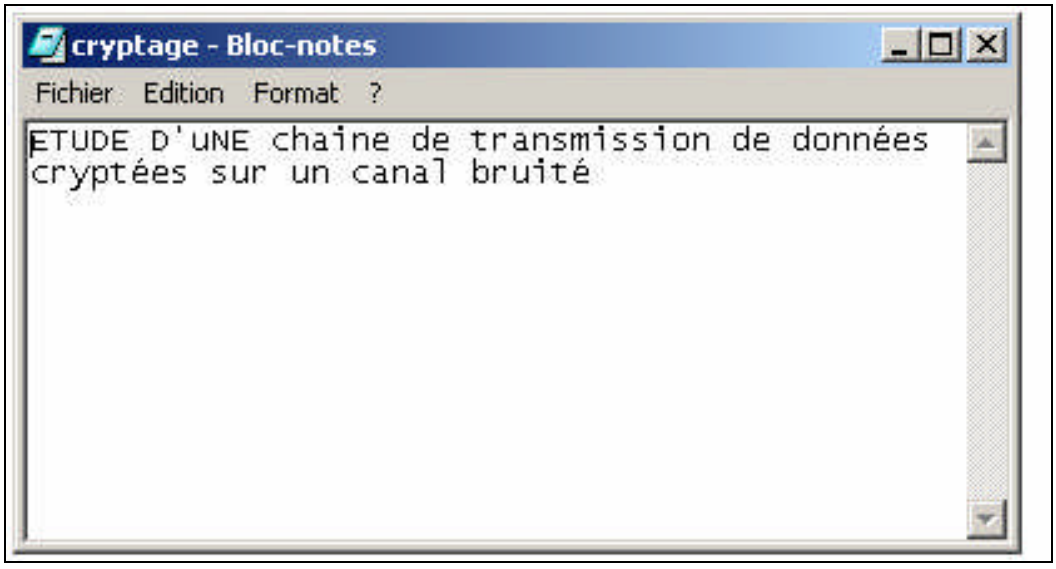


Figure 5.27.b : Décryptage

Exemple de cryptage du même texte avec trois clés différentes

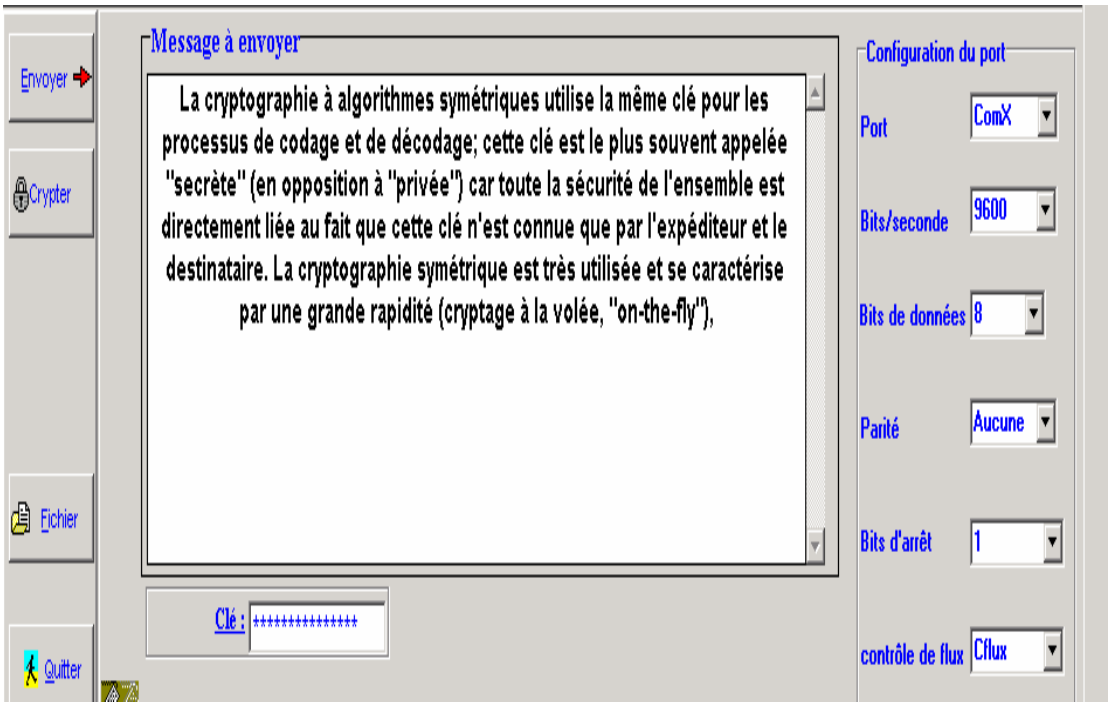


Figure 5.28.a : Texte clair

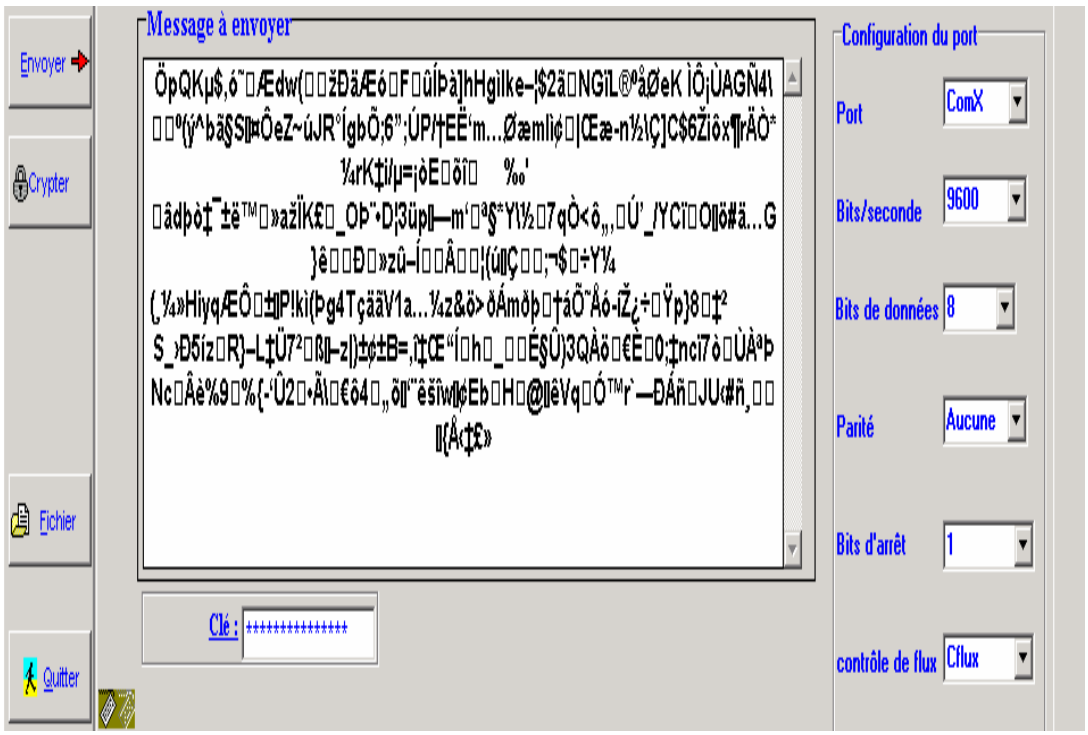


Figure 5.28.b : Texte crypté avec la clé 1

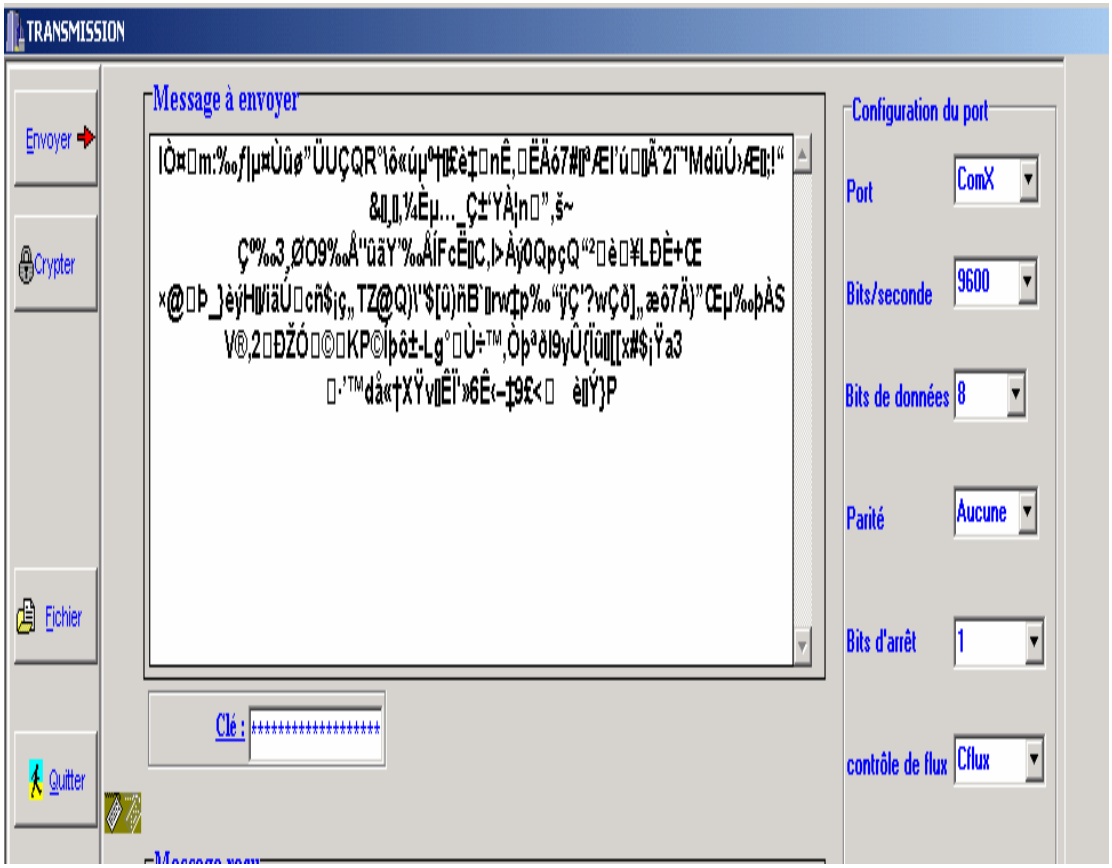


Figure 5.28.c : texte crypté avec la clé 2

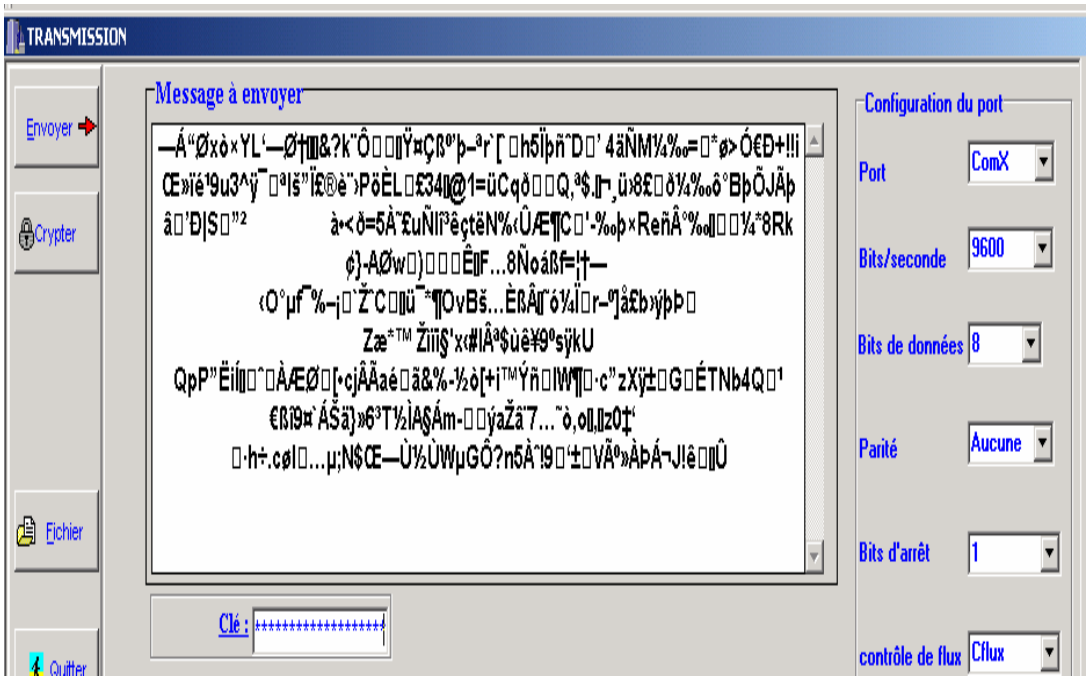


Figure 5.28.d : texte crypté avec la clé 3

5.5 La réalisation

Pour la réalisation : nous avons réalisé une liaison point à point à base du RS 232.Une liaison série est une ligne où les bits d'information (1 ou 0) arrivent successivement, soit à intervalles réguliers (transmission synchrone), soit à des intervalles aléatoires, en groupe (transmission asynchrone). La liaison RS232 est une liaison série asynchrone.

5.5.1 Principe

L'intérêt de la liaison RS232, c'est qu'il suffit de 3 fils pour assurer la communication entre deux appareils A et B. Il faut bien sûr un fil de référence électrique ("masse"), un fil pour envoyer les signaux dans un sens (A vers B), et un fil pour envoyer les signaux dans l'autre sens (B vers A).

La prise normalisée RS232 était une prise à 25 broches. Actuellement, elle est souvent réduite à une prise à 9 broches mâle, située à l'arrière de l'ordinateur.

L'octet à transmettre est envoyé bit par bit (poids faible en premier) par l'émetteur sur la ligne Tx, vers le récepteur (ligne Rx) qui le reconstitue.

La vitesse de transmission de l'émetteur doit être identique à la vitesse d'acquisition du récepteur. Il existe différentes vitesses normalisées: 9600, 4800, 2400, 1200... Bauds.

La communication peut se faire dans les deux sens (duplex), soit émission d'abord, puis réception ensuite (half-duplex), soit émission et réception simultanées (full-duplex).

La transmission étant du type asynchrone (pas d'horloge commune entre l'émetteur et le récepteur), des bits supplémentaires sont indispensables au fonctionnement: bit de début de mot (start), bit(s) de fin de mot (stop).

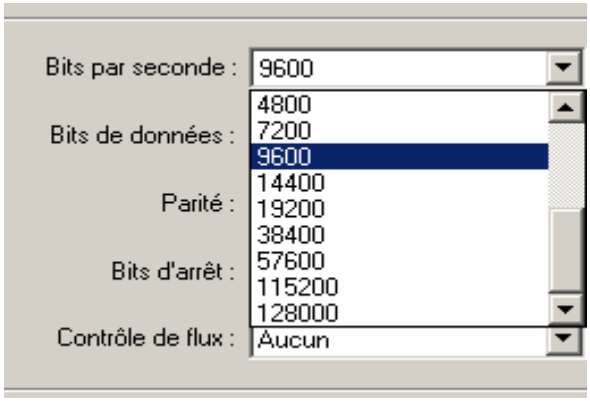
D'autre part, l'utilisation éventuelle d'un bit de parité, permet la détection d'erreurs dans la transmission.

Le message est transmis par créneaux de tension entre le fil d'émission et le fil de masse, donc bit par bit. La liaison série aux normes RS232 est utilisée dans tous les domaines de l'informatique et plus particulièrement pour les ports de communication COM1 et COM2 des ordinateurs, permettant ainsi la communication avec des périphériques tels que modem et souris.

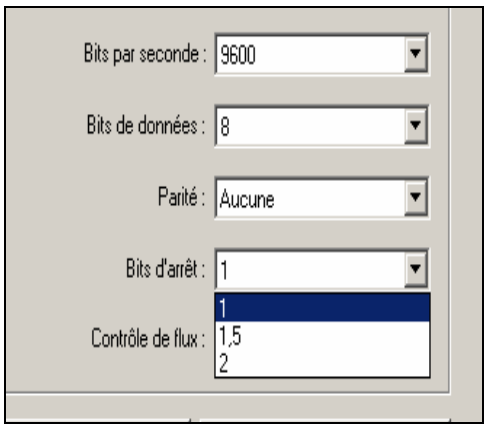
5.5.2 Protocole de transmission

Afin que les éléments communicants puissent se comprendre, il est nécessaire d'établir un protocole de transmission. Ce protocole devra être le même pour les deux éléments afin que la transmission fonctionne correctement. Le protocole de transmission est défini par :

- La vitesse de transmission. Les différentes vitesses de transmission sont réglables à partir de 110 bauds, la façon suivante : 110 bds, 150 bds, 300 bds, 600 bds, 1200 bds, 2400 bds, 4800 bds, 9600 bds .



- Bit de start. La ligne au repos est à l'état logique 1. Pour indiquer qu'un mot va être transmis, la ligne passe à l'état bas 0 avant de commencer le transfert. Ce bit permet de synchroniser l'horloge du récepteur.
- Bit de stop. après la transmission, la ligne est positionnée au repos pendant 1, 2 ou 1,5 périodes d'horloge selon le nombre de bits de stop.

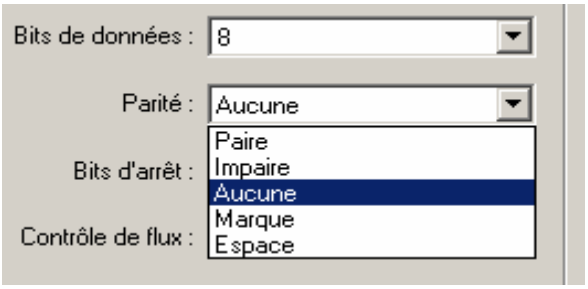


- Longueur des mots : Un protocole avec 7 bits de données peut coder 128 caractères (0 à 127). Un protocole avec 8 bits de données peut coder 256 caractères (0 à 255).

- Parité. Le mot transmis peut être suivi ou non d'un bit de parité qui sert à détecter les erreurs éventuelles de transmission. Il existe deux types de parité :

-parité paire : le bit ajouté à la donnée est positionné de telle façon que le nombre des états 1 soit paire sur l'ensemble donné + bit de parité.

-parité impaire : le bit ajouté à la donnée est positionné de telle façon que le nombre des états 1 soit impaire sur l'ensemble donné + bit de parité.



Un message est donc composé d'un certain nombre de caractères, avec parfois un caractère de fin de message et un caractère de contrôle.

Après avoir étudier les différents protocoles de transmission, nous avons réalisé une interface comme le montre la figure (5.28.a) elle comporte trois fenêtres :

- Une fenêtre pour le message à envoyer : Dans cette partie on écrit le message voulu, le problème de taille ne se pose pas .
- Une deuxième fenêtre pour la clé : la taille de la clé est de 128 bits (c'est à dire 16 caractères), même si la clé est inférieure à 128 bits le message pourra toujours être crypté car le manque de bits vont être considérer comme un blanc.
- Une troisième fenêtre pour le message reçu : C'est à dire le message chiffré.

5.5.3 Cryptage :

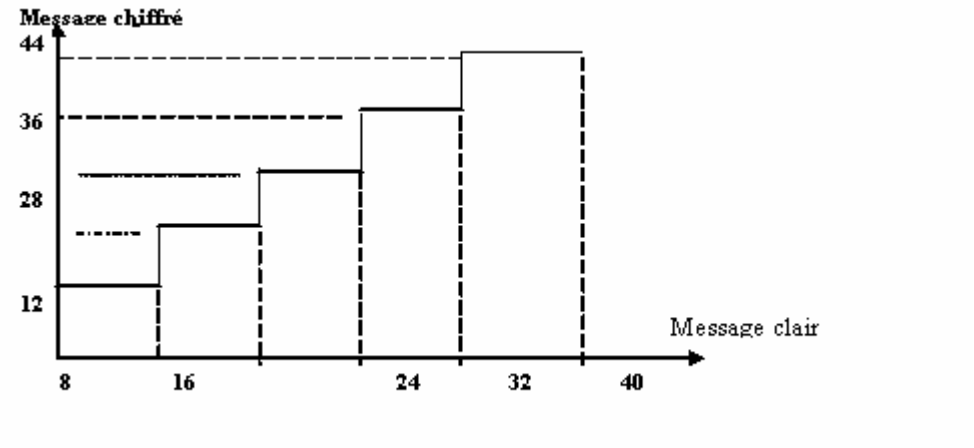
Cette partie a été développée auparavent sauf qu'au moment de transmission entre deux postes, nous avons rencontré un problème de capacité du message entre le cryptage et le décryptage. Car la taille du message crypté et décrypté n'est pas la même donc la taille du buffer de la station réceptrice est inconnue pour remédier à cela, nous avons fait une série de test.

Résultat du test :

Message clair	**Message chiffré**
Un caractère à 8 caractères	12 caractères
9 caractères à 16 caractères	20 caractères
17 caractères à 24 caractères	28 caractères

25 caractères	à	32 caractères		36 caractères
33 caractères	à	40 caractères		44 caractères

D'après ce tableau nous avons tracé la courbe suivante :



Constatation :

Nous avons une fonction escalier, le message reçu c'est à dire le message chiffré (crypté) est $M_C = M_{Cl} + 4$ caractères. Maintenant la taille du buffer est connue. Nous avons préféré que la clé de cryptage ne soit pas dans le programme et cela par mesure de sécurité. Donc il nous faut autant de clés que de couples d'utilisateur qui communiquent.

CONCLUSION

Ce travail est consacré à l'allocation et l'optimisation des ressources d'une chaîne de communication pour des transmissions de données. Pour ce faire, nous avons considéré six points d'étude, de nombreux résultats peuvent être déduits des performances présentées sur la chaîne globale de transmission :

- Pour l'obtention des performances optimales nécessaires pour une modulation numérique fiable, le TEB doit rester en dessous d'un seuil donné. Nous avons illustré les algorithmes évoqués par des résultats de simulation, et tenté d'expliquer leur comportement. Donc la simulation, visait à prédire les conséquences d'un choix de paramètres sur la performance du système. Nous avons constaté que :
  - La dégradation du TEB augmente avec l'augmentation du nombre d'état.
  - Ces courbes montrent que contrairement aux modulations MDA et MDP, les performances sont améliorées lorsqu'on augmente M entraînant aussi l'augmentation de l'occupation spectrale.
  - Pour une plage de signal donnée plus le nombre d'états augmente, plus la probabilité d'erreurs augmente. Il n'est donc pas possible, pour un rapport signal/bruit donné, d'augmenter indéfiniment le débit binaire en augmentant le nombre d'états.
  - La probabilité d'erreurs diminue très rapidement quand le rapport signal/bruit augmente. C'est en fait un des nombreux avantages de la transmission numérique.

  On remarque que pour B et T donnés, l'efficacité spectrale augmente, comme on pouvait s'y attendre, avec le nombre de bit/symbole $n = \log_2 M$. C'est en effet la raison d'être de la modulation M-aire.

- Pour la sécurité de la chaîne de transmission nous avons opté pour l'implémentation de l'algorithme IDEA opérant en mode ECB. Au cours de cette

implémentation nous sommes parvenu à cette constatation que l'algorithme symétrique bien qu'il présente des inconvénients offre une fiabilité avérée :

- Parmi ces inconvénients, nous citerons, en premier lieu, la méthode de génération des sous clés qui est toujours régulière(clé partagée) et donc pourrait être une faiblesse surtout que la robustesse de l'algorithme repose sur la sécurité de la clé.
- En deuxième lieu, le mode d'opération ECB utilisé, présente des faiblesses car 2 blocs identiques seront chiffrés de la même manière et auront le même bloc chiffré, il est donc possible de recenser ces lettres (d'où le nom dictionnaire électronique). Mais si la clé a une taille de 128 bits, cette attaque n'est pas exploitable en pratique de nos jours.

Les clés de 128 bits sous une configuration de chiffrage en parallèle (ECB) des blocs confèrent au système un niveau de sécurité assez élevé avec un accès très rapide aux zones de texte chiffrée et une capacité de déchiffrement partiel des données avec en prime une immunité inter blocs en cas d'infection de l'un d'eux. Aussi si une erreur est parvenue au niveau du premier bloc, il n'y aura pas d'effet sur les autres blocs car ils sont indépendants.

L'algorithme de chiffrement de donnée par bloc offre d'excellentes garanties de sécurité et constitue un choix judicieux pour le cryptage des données.

Perspectives :

Quant aux perspectives de ces recherches :

- Afin d'amélioré le taux d'erreurs de la liaison l'ajout d'autres codes de corrections tels que les turbo codes pourrait être envisagé.
- Un point qui n'a pas été traité dans cette thèse concerne l'aspect multi-utilisateurs. Il serait intéressant d'étudier les potentialités de cette transmission multipoint, ainsi que leurs protocoles de gestion et concernant le cryptage.

- il serait intéressant d'essayer de casser l'algorithme IDEA par les différentes forces d'attaques, et de l'essayer avec les autres modes tels que les modes CBC, CFB, OFB.

APPENDICE A

LISTE DES SYMBOLES ET DES ABREVIATIONS

D_{min}	Distance minimale entre symbole
M	Valence
m	Le nombre de bit par niveau
E_b	Energie moyenne par symbole
E_s	Energie moyenne par bit
P_b	Puissance moyenne émise
DSP	Densité spectrale de puissance
ASK (MDA)	Amplitude Shift Keying(modulation par déplacement d'amplitude
PSK (MDP)	Phase Shift Keying (modulation par déplacement de phase)
FSK (MDF)	Frequency Shift Keying (modulation par déplacement de fréquence)
QAM (MAQ)	Quadrature Amplitude modulation (modulation d'amplitude de deux porteuses en quadrature)
E_b/N_0	rapport signal sur bruit
NRZ	Non retour à zéro
IES	Interférence entre les symboles
BBAG	Bruit blanc additionnel gaussien
D_b	Débit binaire
D_S	Débit bauds ou la rapidité
TEB (BER)	Taux d'erreurs binaire = Eb/N0
$P_b(e)$	Probabilité d'erreurs par bit

$P_s(e)$	Probabilité d'erreurs par symbole
η	Efficacité spectrale
R	Rapidité ou débit par symbole
g(t)	est une fonction de mise en forme spectrale du signal x(t)
$\{a_k\}$	Représente la suite des symboles d'information à transmettre.
E_k	Clé secrète de chiffrement
E_{k-1}	Clé secrète de déchiffrement

APPENDICE B

- Les principaux algorithmes symétriques (chiffrement par bloc) en 2004

Nom	Période	Taille bloc	Taille clé	Caractéristique	Implémentation
RC2	70	64	128	Sous brevet - RSA (US)	Outlook http://www.rsasecurity.com/
RC5/RC6	90	128	128 et plus	Sous brevet - RSA (US)	http://www.rsasecurity.com/
IDEA	90	64	128	Sous brevet - MediaCrypt (Suisse	http://www.rsasecurity.com/
DES (DEA)	70	64	56	NIST (US gouv)	Outlook
AES (Rijndael)	90	128	128 et plus	NIST (US gouv)	PGP csrc.nist.gov/CryptoToolkit/aes/rijndael/
CAST-256	90	128	256	Entrust Technology (US)	PGP
TowFish	90	64	448		PGP
Camelia	90	64	128	NTT & Mitsubishi Electric	info.isl.ntt.co.jp/camellia/

- Les principaux algorithmes symétriques (chiffrement par flux) en 2004

Nom	Période	Taille clé	Caractéristique	Implémentation
RC4	70	128	Sous brevet - RSA (US)	Outlook Open's http://www.rsasecurity.com/
BMGL	00	128	Ericsson, KTH Stockholm (Suede)	
SNOW	00	128	Université (Italie)	www.it.lth.se/cryptology/snow/index.html
SOBER-t16 / t32	00	128	Qualcomm Int. (Australie)	www.qualcomm.com.au/

- Les principaux algorithmes symétriques en 2004 et en détail

Algorithme	Détails
IDEA - International Data Encryption Algorithm Brevet jusqu'en 2010 64-bits block ciphers et clé de 128 bits	Proposé dans PGP. Algorithme utilisé en mode logiciel et matériel. Grande vitesse de chiffrement. http://www.media-crypt.com/ (et RFC3058 Use of the IDEA Encryption Algorithm in CMS
DES / Triple-DES - Data Encryption Standard [DEA Data Encryption Algorithm Ancien standard du gouvernement américain (FIPS 46-3 ou ANSI standard X3.92). Développé essentiellement par IBM. Aujourd'hui remplacé par AES. Libre. 64-bits block ciphers et 56 bits de clé	Triple DES (3DES) revient à chiffrer trois fois. Utilisé dans PGP DES représente l'implémentation de DEA, Data Encryption Algorithm, dérivé de Lucifer, algorithme d'IBM (1970) Développé initialement pour fonctionner au sein d'équipements matériels. 3DES revient à chiffrer trois fois, chque blocs, avec DES
AES - Advanced Encryption Standard [Rijndael] (AES 128, AES 192, AES 256) Standard du gouvernement américain (FIPS-197) AES utilise l'algorithme Rijndael, développé par 2 chercheurs flamand/belge (Joan DAEMEN et Vincent RIJMEN) en 2001 suite à un appel à contribution mondial lancé par le NIST (National Institute of Standards and Technology). Libre Taille des blocs 128 bits, taille des clés 128 bits au moins. Cet algorithme semble ne pas avoir de défaut, décrit comme rapide, simple, sécurisé, souple et utilisable dans des cartes à puces.	Il peut travailler sur des blocs de 128, 192 ou 256 bits. Utilisé aussi dans PGP. AES imposait que la taille des blocs soit de 128 bits lors de l'appel à contribution. Au début de l'appel, 15 algorithmes furent retenus (dont RC5, CAST, SAFER-SK) puis plus que 5. Parmis ces cinq, on compte : - MARS (proposé par IBM, accepte des clés juqu'à 448 bits, parce que complexe et ne reposant pas sur un algorithme réputé, sa fiabilité sera jugée difficile à estimer) - RC6 (voir les RC* de RSA) - Rijndael (voir ci-contre, AES) - Serpent (Ross Anderson (United Kingdom), Eli Biham (Israel), Lars Knudsen (Norway) moins performant mais peu exigent en mémoire, similaire à CAST-256) - Twofish (voir Blowfish) Rijndael fut l'élu. Utilisé dans PGP. csrc.nist.gov/
Blowfish, Towfish Créé Bruce Schneier. Libre Bloc s de 64 bits, clés jusqu'à 448 bits.	Utilisé dans PGP. Puis avec John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson (US), ils le fire évoluer vers **Towfish** pour le soumettre à l'appel à contribution effectué par les US en 2000 (AES).

	Feistel
CAST-128 Créé par Carlisle Adams et Stafford Tavares (Canada). Libre. Blocs de 64 bits, clé de 128 bits. **CAST-256** Blocs de 128 bits, clé de 256 bits.	CAST est la propriété d'Entrust Technologies mais il est libre d'utilisation sans restriction. Utilisé par Microsoft, IBM, PGP. Feistel **The CAST-256 Encryption Algorithm (**RFC 2612
RC2, RC5, RC6 Créés par Ron Rivest, co-inventeur de RSA. "RC" signifie "Ron's Code" ou "Rivest's Cipher". RC2, blocs de 64 bits et clé de 56 bits. RC5, blocs de 128 bits et clés de 128 bits au moins. **RC4** RC4 est libre, c'est un "stream cipher" (chiffrement par flux	RC4 (stream cipher) ne chiffre pas par blocs mais bit à bit, par flux ("stream cipher"). Utilisé dans SSL. Algorithme très répandu. L'algorithme ArcFour était censé devenir une alternative à RC4 (ArcFour signifie "Alleged RC4") Des accords ont permit très tôt de pouvoir exporter ces algorithmes (RC2 et RC4) hors des Etats Unis. RC6 est le même algorithme que RC5 avec des objectifs supplémentaires d'atteindre les exigences de l'appel à contribution effectué par les US en 2000 (AES). RC6 est sous license RSA. http://www.rsasecurity.com/
Skipjack	Cet algorithme faisait parti du projet Capstone (initié par le NIST et la NSA américains) etest enregistré dans la standard [FIPS 185]. Cet algorithme était utilisé dans les composants électroniques Clipper.

Et dans le désordre....CS-cipher, Hierocrypt, Khazad, Misty1, Nimbus, NUSH, Safer, SHACAL, Anubis, Camellia, Grand Cru, Noekeon, NUSH, BMGL, LEVIATHAN, LILI-128, SNOW SOBER

.

APPENDICE C

Dictionnaire de codes : « Electronic code book » (ECB)

Il s'agit du mode le plus simple, le message à chiffrer est subdivisé en plusieurs blocs qui sont chiffrés séparément les uns après les autres. Le gros défaut de cette méthode est que deux blocs avec le même contenu seront chiffrés de la même manière, on peut donc tirer des informations à partir du texte chiffré en cherchant les séquences identiques. On obtient dès lors un « dictionnaire de codes » avec les correspondances entre le clair et le chiffré d'où le terme *code book*.

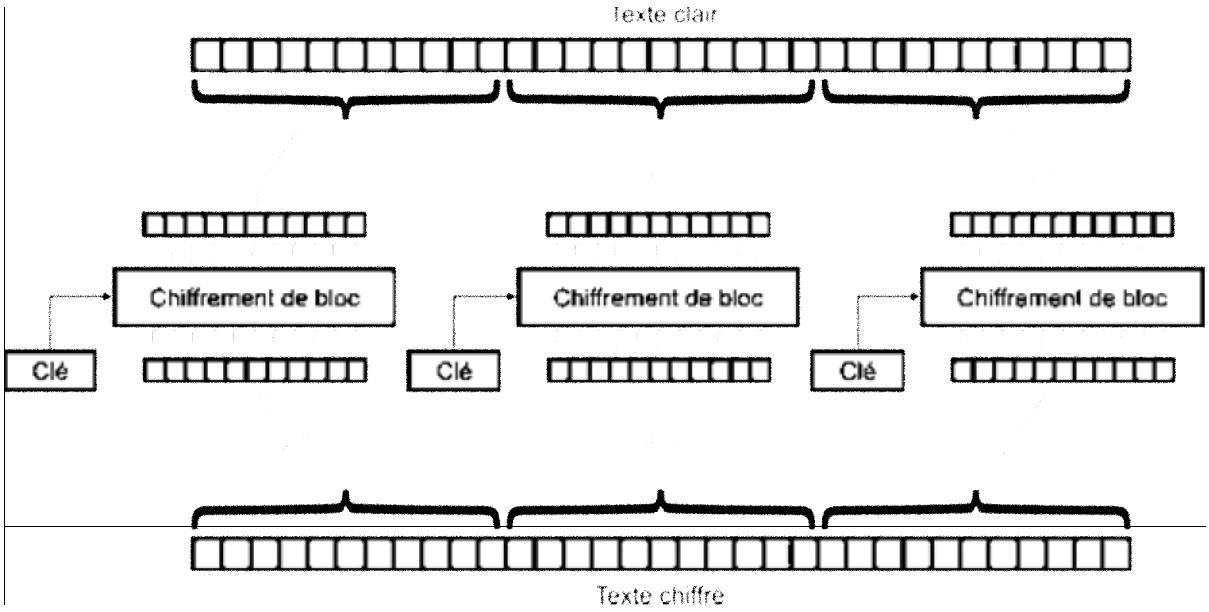


Schéma avec les étapes d'un mode de type ECB. Le texte en clair est découpé en bloc et chaque bloc est chiffré, indépendamment des autres, avec la clé de chiffrement. Le problème relatif à ce mode est :

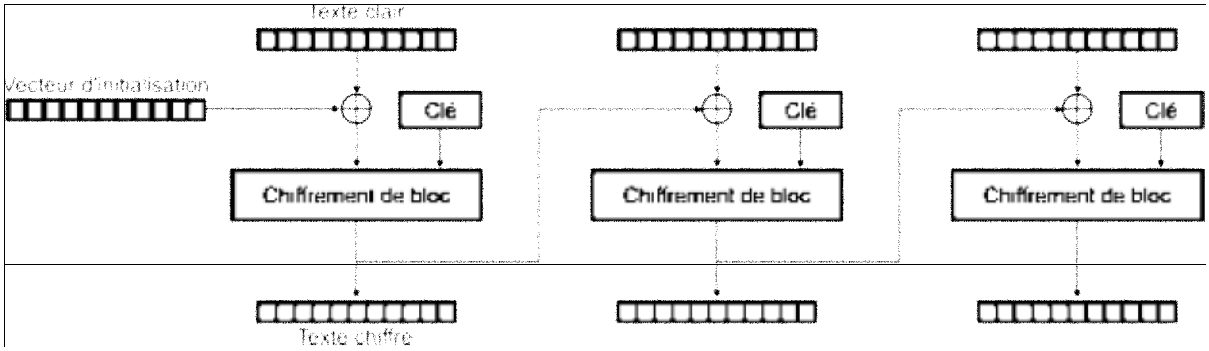
- Si on utilise deux fois le même texte clair et la même clé de chiffrement, le résultat du chiffrement sera identique d'où la nécessité de changer la clé si nous voulons garder le même message.

L'avantage qu'il peut procurer est :

- Un accès rapide à une zone quelconque du texte chiffré et la possibilité de déchiffrer une partie seulement des données, et il permet le chiffrement en parallèle des différents blocs composant un message.

Enchaînement des blocs : « Cipher Block Chaining » (CBC)

Dans ce mode, on applique sur chaque bloc un 'OU exclusif' avec le chiffrage du bloc précédent avant qu'il soit lui-même en crypté. De plus, afin de rendre chaque message unique, un vecteur d'initialisation est utilisé.

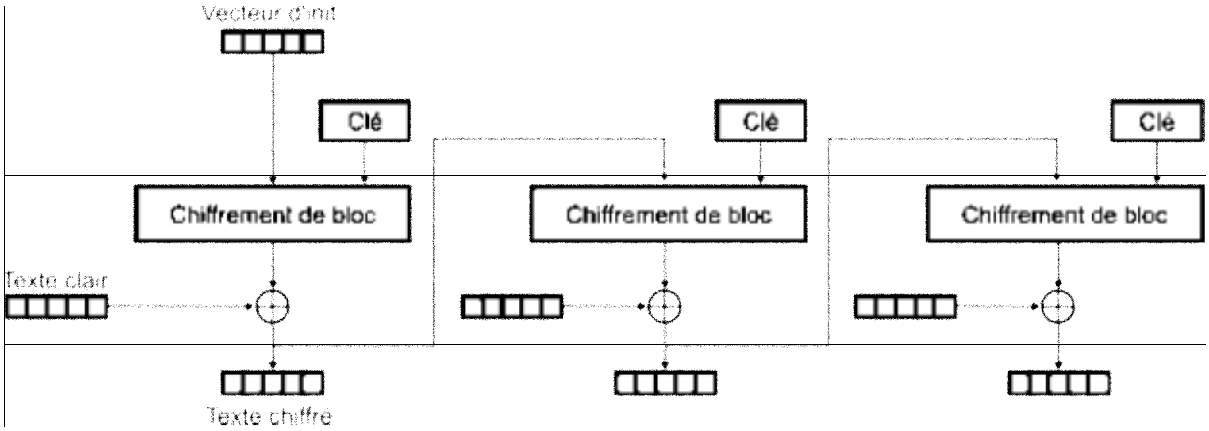


Chiffrement à rétroaction : « Cipher Feedback » (CFB)

Ce mode agisse comme un chiffrement par flux. Il génère un flux de clés qui est ensuite appliqué au document original.

Le mode qui semble éviter tous les problèmes vus précédemment est le CFB. L'opération XOR est appliquée entre le bloc de texte clair et le résultat précédent chiffré à nouveau par la fonction de chiffrement.

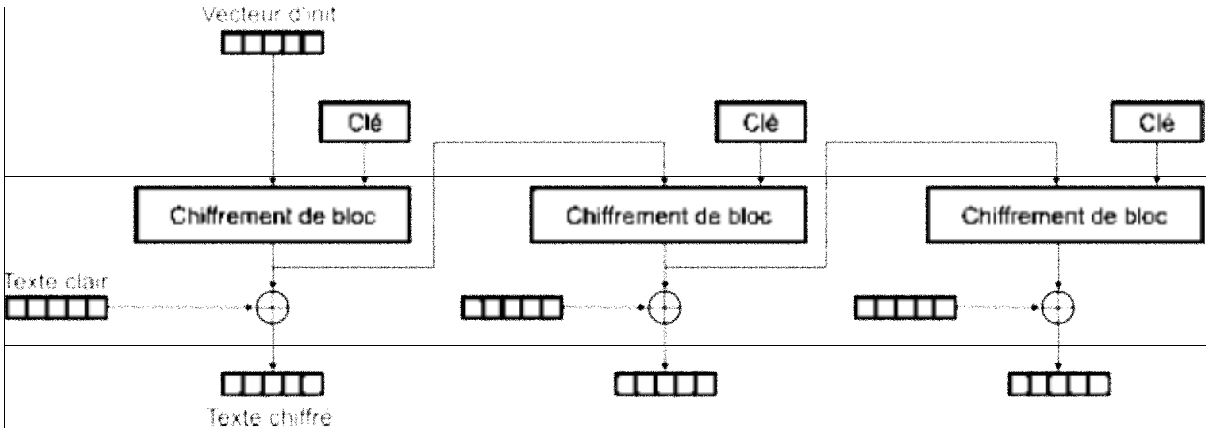
Pour le premier bloc de texte clair, on génère un vecteur d'initialisation.



Le mode CFB offre une grande sécurité, le flux de clé est obtenu en encryptant le précédent bloc chiffré.

Chiffrement à rétroaction de sortie : « Output Feedback » (OFB)

Dans ce mode, le flux de clé est obtenu en encryptant le précédent flux de clé.



Le mode OFB est une solution aux deux problèmes relatifs au mode ECB. Au départ un vecteur d'initialisation est généré. Ce bloc est chiffré à plusieurs reprises et chacun des résultats est utilisé successivement dans l'application de l'opération XOR avec un bloc de texte clair. Le vecteur d'initialisation est envoyé tel quel avec le message chiffré.

Ce mode a lui-même deux autres problèmes. Le texte clair est seulement soumis à un XOR. Si le texte clair est connu, un tout autre texte clair peut être substitué en inversant les bits du texte chiffré de la même manière qu'inverser les bits du texte clair (*bit-flipping attack*). De plus il y a une mince possibilité qu'une clé et un vecteur d'initialisation soient

choisis tels que les blocs successifs générés puissent se répéter sur une courte boucle. Le mode OFB est souvent utilisé comme générateur de nombre aléatoire.

Vecteur initial

En cryptographie , un vecteur d'initialisation (en anglais *initialization vector* ou *IV*) est un bloc de bits combiné avec le premier bloc de données lors d'une opération de chiffrement. Il est utilisé dans le cadre des modes d'opération d'un algorithme de chiffrement symétrique par blocs ou pour un chiffrement par flux comme RC4. Dans certains crypto systèmes, le vecteur est généré de manière aléatoire, puis transmis en clair avec le reste du message.

Tous les modes (à l'exception d' ECB) requièrent un « vecteur d'initialisation ». C'est un bloc de données aléatoires pour démarrer le chiffrement du premier bloc et fournir ainsi une forme de hasard indépendant du document à chiffrer. Il n'a pas besoin d'être lui-même chiffré lors de la transmission, mais il ne doit jamais être réemployé avec la même clé.

REFERENCES

1. groupe "article 29" sur la protection des données 11647/02/fr/final wp 66 « avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis » Adopté le 24 octobre 2002

2. C. E. Shannon « A mathematical theory of communication et communication in the presence of noise »,vol. 27, pp. 379-423 and 623-656, july 1948

3. C. E. Shannon, « A mathematical theory of communication, » bell syst. Tech. J., vol. 27, pp. 379-423 and 623-656, july 1948

4. M. Joindot et A. Glavieux, « Introduction aux Communications Numériques », Collection Pédagogique de Télécommunication, Ellipses, 1995

5. Maxime Guillaud : Thèse de Doctorat « Techniques de transmission et de modélisation de canal pour les systèmes de communications multi antennes » (2005)

6. Hoang Le-Huy. Introduction à Matlab et Simulink, Manuel de département de génie électrique et de génie informatique, université de Laval, Qc, Canada, 1998.

7. Michel Crucianu « transmission de l'information » support de cours (E3i, 2001-2002) Université de Tours

8. M. Michelson and A. H. Levesque, « Error-Control techniques for digital communications », wiley-interscience

9. Marc Uro, Pierre Lecoy « technologie des télécommunications » éditions hermès 1995

12. Jc Bic- Duponteil-j c Imbeaux « Eléments de communication numérique » éditions Dunod (2 volumes)

13. ELG 3520 Analyse de signaux et de systèmes
par Martin Bouchard, août 2002
Manuel requis : Signals and Systems, Oppenheim et Willsky

14. C Macchi - J F Guilbert téléinformatique Editions Dunod

15. John G Proakis Mc Graw Hill « digital communication » (la bible)

16. Simon Haykin Mc « Digital communications » Master university wiley

17. Anne Migan Dubois « revue télécommunications transmission numérique en bande de base » (2005) (Université Pierre et Marie Curie)

18. Joël le roux « Illustrations de la notion d'entropie dans les deux théorèmes de Claude Shannon en théorie de l'information », Leroux@essi. Fr, april 2002

19. S. MORAND
communications numériques « traitement et transmission d'informations numériques télécommunications, téléinformatique, multimédia
UFR Sciences et Techniques Besançon DESS SMTII

20. cours de réseaux et systèmes
DI GALLO Frédéric CNAM BORDEAUX 1999-2000

21. Introduction aux techniques de chiffrement et de securite – Cnam limoges, cycle c, 2003-2004

22. Bruce Schneier (wiley), cryptographie appliquee, 1996,

23. Rijndael et l'AES Pierre-Alain Fouque e-mail: pierre-alain. Fouque@c-s. Fr

24. Jean-Louis Poss « introduction a la cryptographie » version 1. 0 juin 2003

25. Michel Crucianu « transmission de l'information » support de cours E3i, (2001-2002) (université de tours réseaux)

26. Florent Dupont : Module R1, Réseaux et transmission de données Couches basses UCB Lyon1 Licence IUP Génie Informatique option Réseaux – Informations 1999

27. Pierre Comon : Communication Numérique 1
www.i3s.unice.FR / comon 3 décembre 2003

28. Implémentation de IDEA sur la famille de processeurs IA-64
Jacques-Olivier Haenni EPFL - DI – LSL 7 juin 2000

29. Projet Enseirb « Bases de transmissions numérique et modulations numériques »

30. G. Couturier « modulations numériques » Dept Geii Iut - universite de Bordeaux

31. Modélisation VHDL-AMS haut niveau d'un système de transmission de puissance et de données par lien inductif
Richard Perdriau_, Anne-Marie Trullemans, Mohamed Ramdani_
Ecole Supérieure d'Electronique de l'Ouest
DICE - Laboratoire de Microélectronique - Université Catholique de Louvain
2003

32. G. Couturier « Maquette modulateur-demodulateur BPSK et QPSK » département

de génie informatique - IUT (Bordeaux)

33. Anne Migan Dubois (lgep) « revue de télécommunications transmission numérique en bande de base »

34. Michel Terre « modulation d'une chaîne de caractères en 8 PSK »(version 3.0) mars 2003 (terre@cnam. Fr)

35. Ahmed Agarbi – Abdessamad Mouhane « projet 2eme à télé communications avis v. 32 bis (9600 it/s » , (communications numériques) 2004

36. Introduction aux techniques de chiffrement et de securite – cnam limoges, cycle c, 2003-2004 **« un algorithme symetrique : l'IDEA »**

37. Aurelian Constantinescu « advanced digital communication numérique avancés » - module 2 –

38. X. Lai. « On the Design and Security of Block Ciphers ». Number 1 in ETH Series in Information Processing. Hartung-Gorre Verlag Konstanz, 1992.

39. cryptage des données (Cuefa 2001-2002).Cours de compléments réseaux

La cryptologie moderne

40. Anne Canteaut Françoise et Lévy-dit-Véhel
INRIA _Ecole Nationale Supérieure
Projet CODES des Techniques Avancées 2003

41. R. Gautier, G. Burel, J. Letessier, and O. Berder. « Blind estimation of scrambler offset using encoder redundancy ». In Proceedings of IEEE Asilomar Conference on Signals, Systems and Computers, volume 1, pages 626–630, Pacific Grove (CA), USA, 2002

42. SympA'6 Besançon, 19 - 22 juin 2000
6ème Symposium sur les Architectures Nouvelles de Machines
« Une comparaison entre quelques implantations logicielles et matérielles de l'algorithme de chi_rement IDEA »
Jean-Luc Beuchat1, Jacques-Olivier Haenni1, Christof Teuscher1, Francisco J. Gómez2, Hector Fabio Restrepo1 et Eduardo Sanchez1
1 Laboratoire de Systèmes Logiques, Ecole Polytechnique Fédérale de Lausanne CH _ 1015 Lausanne, Suisse
2Escuela Técnica Superior de Informática, Universidad Autónoma de Madrid E _ 20849 Madrid, Spain

43. Mlle Zine leila thèse de magistère « simulation d'un canal satellite pour une transmission numérique » 2002 université de BLIDA

44. Jean-Pierre DELMAS, Roger Amberti, Yann Meurisse, Marc Uro
« communications numériques » corrigé d'exercices.

45. Daemen et V. Rijmen , < The Rijndael block cipher >,

http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael-ammended.pdf.

46. Jean-Philippe Gaulier « Analyse des algorithmes analystes concourant pour le futur standard AES » Par Conservatoire National des Arts et Métiers Centre Régional Associé de Limoges

47. Julien Guillet
Thèse de doctorat « Caractérisation et modélisation spatio-temporelles du canal de propagation radioélectrique dans le contexte MIMO » l'Institut National des Sciences Appliquées de Rennes 2004

48. Principaux algorithmes de cryptage
Rolland Balzon Philippe
Department of Computer Science SEPRO Robotique 11 juillet 2002

.