Institut Supérieur des Etudes Technologiques en Communication de Tunis

Projet de fin d'études

REALISATION D'UN CIRCUIT DE SECURISATION DES COMMUNICATIONS RTC

Réalisé par

ELAYEB Mounir

CHETOUI Mohamed Lassaâd

TS – Télécommunications

Encadré par

TLILI Fethi

GHAZEL Adel

2001-2002

DEDICACE

Je dédie ce modeste travail

A mon père

Pour son amour, sa patience et ses considérables sacrifices pour me parvenir à ce niveau

A ma mère

Pour son grand amour, ses sacrifices et toute affection qu'elle m'a toujours offerte

A mes frères, surtout Ali et Abderrazzak

A mes sœurs

A tous mes amis

A tous ceux que j'aime.

A tous ceux qui m'aiment.

Med Lassaâd…

DEDICACE

Je dédie ce modeste travail

A l'âme de mon père

Au symbole de douceur, de tendresse, d'amour et d'affection ;

Ma chère mère

A ceux qui m'ont aidé, et m'ont crée le milieu favorable ;

Mes frères Ahmed et Khalifa

A tous mes frères

A ma sœur

A tous mes amis

A tous ceux que j'aime

A tous ceux qui m'aiment.

Mounir…

Remerciements

Ce travail a été réalisé à L'institut Supérieur Des Etudes Technologiques en Communication de Tunis dans le cadre de projet de fin d'études et sous la direction de nos encadreurs Mr. TLILI Fethi et Mr. GHAZEL Adèl..

Au terme de ce travail, nous profitons de cette occasion pour adresser nos vifs remerciement à nos encadreurs pour leur aide, leur disponibilité et leurs précieux conseils qui nous ont été d'un grand apport.

Nos remerciements s'adressent également à la direction de l'ISET'Com et celle de Sup'Com qui nous ont permis l'accès aux laboratoires où nous avons élaboré cette réalisation. De même nous remercions tous les enseignants qui ont conjugué leurs efforts pour nous donner une formation solide.

Nous tenons également à exprimer nos gratitudes aux présidents et aux membres de jury pour avoir accepter d'évoluer ce travail.

Enfin nous voudrions rendre hommage à toute personne n'ayant pas hésité de nous aider de prés ou de loin à la réalisation de ce projet.

CHETOUI Med lassaàd & ELAYEB Mounir

TABLE DES MATIERES

INTRODUCTION GENERALE **1**

CAHIER DE CHARGE **2**

Partie 1:GENRALITES **3**
Chapitre 1 : **4**
SIGNALISATION TELEPHONIQUE **4**
1-1 Définition 4
1-2 Descriptions de signaux 4
1-2-1 Appel 5
1-2-2 Numérotation 6
1-2-3 Envoi du signal d'appel (sonnerie) 6
1-2-4 Réponse de l'abonné demandé (décrochage) 7
1-2-5 Fin de communication (le demandeur raccroche) 7
1-2-6 Fin de communication (le demandé raccroche) 7
1-2-7 Le signal de rappel d'enregistreur 8
Chapitre 2 : **9**
TECHNIQUES DE CRYPTAGE **9**
2-1 Introduction 9
2-2 Le but de la sécurité 9
2-2-1 La confidentialité 9
2-2-2 La disponibilité des services 10
2-2-3 L'intégrité du système 10
2-2-4 Non-répudiation 10
2-3 Présentation du problème 10
2-4 Définition 11
2-5 Evolution de la cryptographie 11
2-5-1 Quarante années d'évolution 11
2-5-2 Description d'un système de cryptage 12
2-5-3 Panorama de la cryptographie moderne 13
2- 6 Terminologie 14
2-6-1 Permutation 15
2-6-2 Utilisation de clé 16
2-7 Les procèdes cryptographiques 16
2-7-1 Les substitutions 16
2-7-2 La transposition 18
2-8 Cryptosystèmes 18
2-8-1 Définition 18
2-8-2 Cryptosystéme à usage restreint 19
2-8-3 Cryptosystéme à usage général 19
2-8-3-1 Cryptosystéme à clé secrète 19
2-8-3-2 Cryptosystéme à clé publique 20
2-8-4 Cryptosystéme à clé symétrique (à clé secrète): 20
2-8-4-1 Définition 20
2-8-4-2 Avantages 21
2-8-4-3 Inconvénients 21

2-8-5 Cryptosystéme à clé asymétrique (à clé publique).....21
2-8-5-1 Définition.....21
2-8-5-2 Avantages.....22
a- Signature à clé secrète.....22
b- Détection des erreurs.....23
c- Fonction à sens unique.....23
2-8-5-3 Inconvénient.....24

Partie 2 :INTERFACE AVEC LA LIGNE TELEPHONIQUE……..…….25
Chapitre1 :.....26
DESCRIPTION THEORIQUE DE L'INTERFACE TELEPHONIQUE.....26
1-1 Définition et rôle de l'interface téléphonique.....26
1-2 Etage de filtrage.....28
1-2-1 Introduction.....28
1-2-2 Le filtre passe haut.....29
1-2-3 Filtre passe bas.....30
1-3 Etage de conversion.....31
1-3-1 Introduction.....31
1-3-2 Etude du convertisseur A/D (ADC 0809).....31
1-3-2-1 Description.....31
1-3-2-2 Caractéristiques de l'ADC 0809.....31
1-3-2-3 Brochage.....32
1-3-2-4 Principe de fonctionnement.....32
1-3-3 Etude du convertisseur DAC0800.....33
1-3-3-1 Description.....33
1-3-3-2 Brochage.....34
1-3-3-3 Caractéristiques.....34
1-3-3-4 Particularités.....35
1-4 Etage de sommation (montage additionneur-inverseur et inverseur).....35
1-4-1 Montage additionner inverseur.....35
1-4-2 Montage inverseur.....36
Chapitre2 :.....37
REALISATION PRATIQUE.....37
2-1 Introduction.....37
2-2 Schéma électronique de la carte.....37
2-2-1 Alimentation et composants utilisés.....37
2-2-2 La saisie de schéma.....39
2-2 Schéma de routage.....40
2-2-1 Plan de pose des composantes.....42
2-2-2 Routage.....43
2-4 Conclusion.....44

Partie 3: ETAGE FPGA……45
Chapitre 1 :.....46
DESCRIPTION DE L'ALGORITHME D.E.S.....46
1-1 Introduction.....46
1-2 Le Cryptage Symétrique : Le D.E.S.....46
1-2-1 Description.....46
1-2-2 Algorithme du DES.....50
1-2-3 Description des six étapes de l'algorithme.....51

1-2-3-1 Première étape....51
1-2-3-2 Deuxième étape....52
1-2-3-3 Troisième étape....52
1-2-3-4 Quatrième étape....52
1-2-3-5 Cinquième étape....53
1-2-3-6 Sixième étape....53
Chapitre 2 :....54
IMPLEMENTATION DE L'ALGORITHME DES SUR UNE CARTE FPGA 54
2-1 Introduction....54
2-2 Les organigrammes d'implémentation de l'algorithme de cryptage DES....54
2-2-1 Etapes de l'algorithme DES....55
2-2-1-1 L'expansion....56
2-2-1-2 la substitution....57
2-2-1-3 Permutation....61
2-2-2 Générateur des clés....62
2-2-3 Organigramme de DES....67
2-3 Description de l'implémentation par des circuits logiques....68
2-4 Application sur un circuit FPGA....70
2-4-1 Définition d'un FPGA....70
2-4-2 Implémentation du DES sur FPGA :....70
2-4-2-1 Version simplifiée de DES....71
2-4-2-2 Schéma de la version simplifiée....72

CONCLUSION GENERALE....73

BIBLIOGRAPHIE....74

ANNEXES……75

INTRODUCTION GENERALE

Historiquement, la cryptographie (les deux facettes de la cryptographie et de la cryptanalyse) a été presque exclusivement l'apanage des militaires des diplomates. Elle regroupe l'ensemble des méthodes et des techniques qui permettent de coder un message afin de le rendre incompréhensible pour quiconque non doté de moyen pour le déchiffrer. On parle alors de cryptage d'un message, et le code résultant prend le terme de cryptogramme. L'action de lui restituer sa forme originale s'appelle le décryptage.

Le réseau téléphonique commuté (RTC) par exemple, est en pleine expansion. En effet, il est utilisé par tout le monde quel que soit leur niveau et les intérêts de leurs communications. Une multitude d'activités se développe autour, entre lesquels il y'a des communications qui demandent une grande sécurité comme les militaires.

Dans ce cadre, nous nous proposons de réaliser un circuit d'interface téléphonique permettant le cryptage du signal de parole.

Afin d'atteindre les objectifs tracés, nous avons organisé notre rapport comme suit :

Une première partie qui contient des généralités sur la signalisation téléphonique et des généralités sur les techniques de cryptage.

Une deuxième partie traitera l'interface avec la ligne téléphonique. Dans cette partie on trouve une conception et dimensionnement de l'interface à réaliser, sa simulation sur le Circuit Maker et enfin les tests expérimentaux.

Une troisième et dernière partie qui contient l'étage FPGA, dans laquelle on va donner une description détaillée de l'algorithme DES, l'implémentation de cet algorithme sur un circuit programmable FPGA et enfin l'application à réaliser.

CAHIER DES CHARGES

Le projet visé répond à un besoin de certains utilisateurs de protéger le contenu de leurs communications contre toute intrusion malveillante et ceci en utilisant des techniques de cryptage.

Le travail à effectuer comporte les étapes suivantes :

- Etude des signaux de signalisation en RTC.
- Etude des techniques de cryptage et les algorithmes de cryptage.
- Conception et réalisation d'une interface téléphonique avec le réseau RTC.
- Etude et choix de l'algorithme de cryptage à implémenter sur un circuit FPGA.

PARTIE 1 :

GENERALITES

CHAPITRE 1 :

SIGNALISATION TELEPHONIQUE

1-1 Définition

La signalisation terminale est l'ensemble de signaux échangés entre un abonné et son centre de rattachement. Elle est entièrement échangée sur les deux fils de conversation de la ligne d'abonné.

.

Les lignes d'abonné étant, en permanence, alimentées en courant continu par le commutateur auquel elles sont rattachées, l'échange de signaux entre poste téléphonique et réseau fait largement appel aux possibilités offertes par cette alimentation, en particulier la variation du courant de ligne.

La plus grande partie des lignes téléphoniques du réseau devant pouvoir recevoir et émettre des appels (lignes mixtes), la signalisation terminale permet de traiter les appels de départ et les appels d'arrivée.
Le tableau 1.1 suivant illustre l'ensemble de signaux :

1-2 Descriptions de signaux

le tableau 1.1 les différents signaux téléphoniques :

Signification des signaux	**Nature du signal**		**Direction du signal**		
	Electrique	**Tonalité**	**Deur**	**Autocom**	**Dé**
Appel (décrochage)	Ligne bouclée		→		
Tonalité d'invitation à transmettre		440Hz permanente	←		
Numérotation	Décimal (rupture de boucle)	D.T.M.F	→		

Appel (sonnerie)	25 ou 50Hz /80 ou 100V 1,7/3,3s				
Retour d'appel (demandé libre)		440Hz 1,7/3,3s			
Réponse de l'abonné demandé (décrochage)	Ligne bouclée				
Tonalité de faux appel (occupation) si demandé occupé		440Hz 0,5s/0,5/s			
Fin de communication le demandeur raccroche	Rupture de la boucle				
Fin de communication le demandé raccroche	Rupture de la boucle				
Signal de rappel d'enregistreur	Rupture calibre de la boucle 200 à 320 ms				

Tab1.1 : Les différents signaux téléphoniques

1-2-1 Appel

Au repos, la ligne téléphonique est alimentée par une tension continue, mais le poste téléphonique s'oppose à la circulation du courant continu par une impédance très élevée. Le courant en ligne est alors nul, ou pour certains équipements terminaux spécifiques, inférieur de 2 à 3 mA : On dit alors que la ligne est ouverte. Le décrochage du combiné par le demandeur qui constitue le signal d'appel, se traduit par une diminution de l'impédance. Le courant continu en ligne atteint alors une valeur comprise entre 35 et 60 mA : on dit alors que la ligne est bouclée. La variation du courant de la ligne est détectée par l'autocommutateur qui engage alors les opérations nécessaires à la réception de la numérotation.

1-2-2 Numérotation

Le tableau1.2 représente le standard DTMF :

697Hz	**1**	**2**	**3**	**A**
770Hz	**4**	**5**	**6**	**B**
652Hz	**7**	**8**	**9**	**C**
941Hz	*****	**0**	**#**	**D**
	1209Hz	**1336Hz**	**1477Hz**	**1633Hz**

Tab1.2 : le standard DTMF

Un digit est défini par la somme de signaux sinusoïdaux de fréquences différentes. Les fréquences utilisées sont caractéristiques et leurs valeurs sont regroupées dans le tableau 1.2 Un 5 sera, par exemple, généré en additionnant deux signaux de fréquences 770 Hz et 1336 Hz. Les avantages de ce système sont multiples, les numéros de téléphone peuvent être composés très rapidement et peuvent être générés par des systèmes informatiques.

1-2-3 Envoi du signal d'appel (sonnerie)

Le signal d'appel consiste à l'envoi cadencé du courant alternatif à 25Hz (autrefois 50) en série sur la ligne ; ce courant se renferme à travers le système de détection d'appel, inclut dans le poste téléphonique constitué généralement par une

capacité. Cette alimentation alternative émise à la cadence de 1,7s de présence et de 3,3s d'absence, se superpose à l'alimentation en tension continue de la ligne.

1-2-4 Réponse de l'abonné demandé (décrochage)

Si la ligne d'abonné demandé est libre, au décrochage de ce dernier, la tonalité de retour d'appel disparaît et un signal électrique constitué par une inversion de la polarité de l'alimentation de la ligne peut être envoyé sur la ligne d'abonné demandeur. Si, par exemple, on trouvait la terre sur le fil **a** et la batterie sur le fil **b**. Ce signal n'est pas nécessaire si le demandeur n'a qu'un poste ordinaire et d'ailleurs certains autocommutateurs ne le fournissent pas systématiquement, mais il peut être utile pour des lignes d'abonnés et certains équipements spéciaux. Il est lié en général au début du paiement de la communication.

1-2-5 Fin de communication (le demandeur raccroche)

Le raccrochage de l'abonné demandeur est constitué par la suppression de la boucle présentée par le poste téléphonique. Etant de même nature que l'impulsion d'ouverture de cardan ou que le signal de rappel d'enregistreur, le raccrochage du demandeur ne peut être distingué que par registreur, le raccrochage du demandeur ne peut être distingué que par une condition de temps. L'ouverture de boule doit avoir une durée supérieure à 400ms pour être interprétée comme un signal de raccrochage du demandeur. Elle commande alors la remise au repos de tous les organes utilisés pour le commutateur.

1-2-6 Fin de communication (le demandé raccroche)

Si le demandé raccroche le premier, sa ligne est maintenue dans l'état de conversation tant que le demandeur n'a pas raccroché ou que le système de libération temporisé n'a pas agit. Un nouveau décrochage du demandé durant cette phase permet de ramener l'appel à la situation de conversation. Après le raccrochage du demandeur ou après la libération temporisée, la ligne appelée revient à l'état de repos.

1-2-7 Le signal de rappel d'enregistreur

Il permet, à partir de la phase de conversation, de retourner à la phase d'enregistrement. Il s'agit d'une rupture calibrée de conversation de retourner à la phase d'enregistrement. Il s'agit d'une rupture calibrée de la boucle présentée par le poste d'abonné, ce signal est utilisé en exploitation téléphonique pour traiter certains services qui nécessitent, pendant la phase de conversation, la fourniture d'informations numériques à partir du poste de l'abonné demandeur. On peut ainsi mettre en garde la communication en cours et établir une nouvelle connexion qui pourra ensuite être transférée en une conversation à trois participants qu'on appelle conférence.

CHAPITRE 2 :

TECHNIQUES DE CRYPTAGE

« la cryptographie, qui est l'art d'écrire des messages sous forme codée, est une discipline qui évoque dans l'esprit courant le monde obscur et secret de l'espionnage empreint de sensations de puissance » ***Xavier MARSAULT***

2-1 Introduction

Il est parfois sage de cacher certaines choses. Depuis l'aube de temps, le mystère ne cesse d'attirer l'homme. Doué de raison, il questionne la nature et lui demande ses papiers. Dés qui sont dissimulés au caché l'intéressent énormément, car ce celui qui dissimule en possède un tout aussi grand.

La cryptologie est une véritable science qui étudie le chiffrement et le déchiffrement d'information ; tandis que la cryptographie est l'utilisation des systèmes mis au point par des cryptologues. Elle intéresse de plus en plus les informaticiens dans la mesure ou l'on manipule des flots croissants de données qu'il est nécessaire de protéger.

2-2 Le but de la sécurité

La sécurité tente de maintenir cinq caractéristiques principales.

2-2-1 La confidentialité

Elle consiste à permettre à une personne de transmettre un message à un correspondant, en garantissant que personne d'autre ne pourra en prendre connaissance, le plus souvent en état de fraude passive, c'est à dire en écoute de l'information sur réseau. On distingue :

- La confidentialité intégrale où l'ensemble de données transmises doit être protégé.
- La confidentialité d'un champ spécifique où la protection est assurée pour quelques données incluses dans une transmission.

Il s'agit de permettre à une personne recevant un message d'être sûre de sa provenance, c'est pourquoi on appelle aussi ce procédé signature électronique. Donc il a pour but de garantir l'identité des correspondants. On peut distinguer deux types :

- L'authentification de l'entité homologue qui assure que l'entité réceptrice, qui est connectée, est bien celle annoncée. Son principal objectif est la lutte contre le déguisement.
- L'authentification de l'origine qui assure que l'entité émettrice est bien celle prétendue.

2-2-2 La disponibilité des services

Les services (poste téléphonique, fax) et les informations (données, parole) doivent être accessibles aux personnes autorisées quand elles en ont besoin.

2-2-3 L'intégrité du système

Les services et les informations (les paroles, données) ne peuvent être modifies que par les personnes autorisées quand elles en ont besoin.

2-2-4 Non-répudiation

Il y a deux types de non-répudiation :

- Les non-répudiations à l'origine des données qui fournissent au récepteur une preuve ou attestation empêchant l'émetteur de contester l'envoi ou le contenu d'un message effectivement reçu.
- Les non-répudiations de la remise qui fournissent à l'émetteur une preuve empêchant le récepteur de contester la réception ou le contenu d'un message effectivement remis.

2-3 Présentation du problème

Longtemps ce domaine est réservé pour les militaires et les ambassadeurs, la cryptographie c'est à dire l'art d'envoyer des messages secrets, s'impose aujourd'hui au grand public afin d'assurer la confidentialité des communications informatiques, ou celle des données stockées sur un disque dur d'ordinateur.

Les banquiers et les services commerciaux ont besoin quant à eux de disposer de protocoles de signatures, avant d'accepter un ordre de virement ou une commande. De ce point de vue, il est bien naïf d'accepter une commande téléphonique sur le simple énonce d'un numéro de carte bancaire.

2-4 Définition

La cryptographie est une science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle permet ainsi de stoker des informations confidentielles ou de le transmettre sur des réseaux non sécurisés, afin qu'aucune personne autre que le destinataire ne puisse la lire.

Alors que la cryptographie consiste à sécuriser les données, la cryptanalyse est l'étude des informations cryptées, afin d'en découvrir le secret. Le cryptanalyse implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance. Ces cryptanalystes sont également appelés des pirates.

La cryptologie englobe la cryptographie et la cryptanalyse.

Il y a deux types de cryptographie qui sont distingués dans le monde : la cryptographie qui empêche un petit enfant de lire vos fichiers et la cryptographie qui empêchera les grands gouvernements de lire vos fichiers. La cryptographie peut être faible au forte, la force de la cryptographie est mesurée par le temps et les ressources qui seront nécessaires pour retrouver le texte clair. La cryptographie forte est un texte chiffré qui est très difficile à déchiffrer sans la possession de l'outil de déchiffrement approprié.

2-5 Evolution de la cryptographie

2-5-1 Quarante années d'évolution

Les gens qui ont élaboré les techniques actuelles de cryptage à l'usage des informaticiens et pour la sécurité de leurs données ne sont pas ceux qui, au sortie de la

deuxième guerre mondiale, possédaient l'art et la connaissance cryptographiques. Il est aujourd'hui incontestable que la plupart des travaux de cryptanalyse réalisés par les militaires qui ont travaillé pendant la guerre sur la transmission et la rupture de messages codés demeurent encore inconnus et protégés. Depuis cette époque, des mathématiciens de toute part ont cherché à mettre au point des méthodes et des outils de plus en plus complexes et de plus en plus sûrs. Trouver des méthodes de cryptage d'une sûreté quasi-absolue occupe encore de nombreux chercheurs dans le monde, travaillant en premier lieu pour les militaires, mais aussi pour les banquiers et les industriels.

2-5-2 Description d'un système de cryptage

Pour envoyer une information secrète à un destinataire, on choisit un algorithme, une ou plusieurs clés de sécurité de son choix et un media de transmission (une personne, une lettre ou de réseau de communications téléphonique public ou privé). On peut créer des myriades d'algorithme qui demeure inconnu. Toute personne quelque peu initiée peut d'ailleurs mettre au point une méthode de cryptage honorable, et il s'agit du passe-temps favori d'un certain nombre d'amateurs plus ou moins avertis. On en examinera tout au long de cet ouvrage. Mais rien ne prouve la sûreté des codes produits par les amateurs, tant que des experts ne sont pas consultés.

2-5-3 Panorama de la cryptographie moderne

La figure 2.1 : représente le panorama de la cryptographie moderne

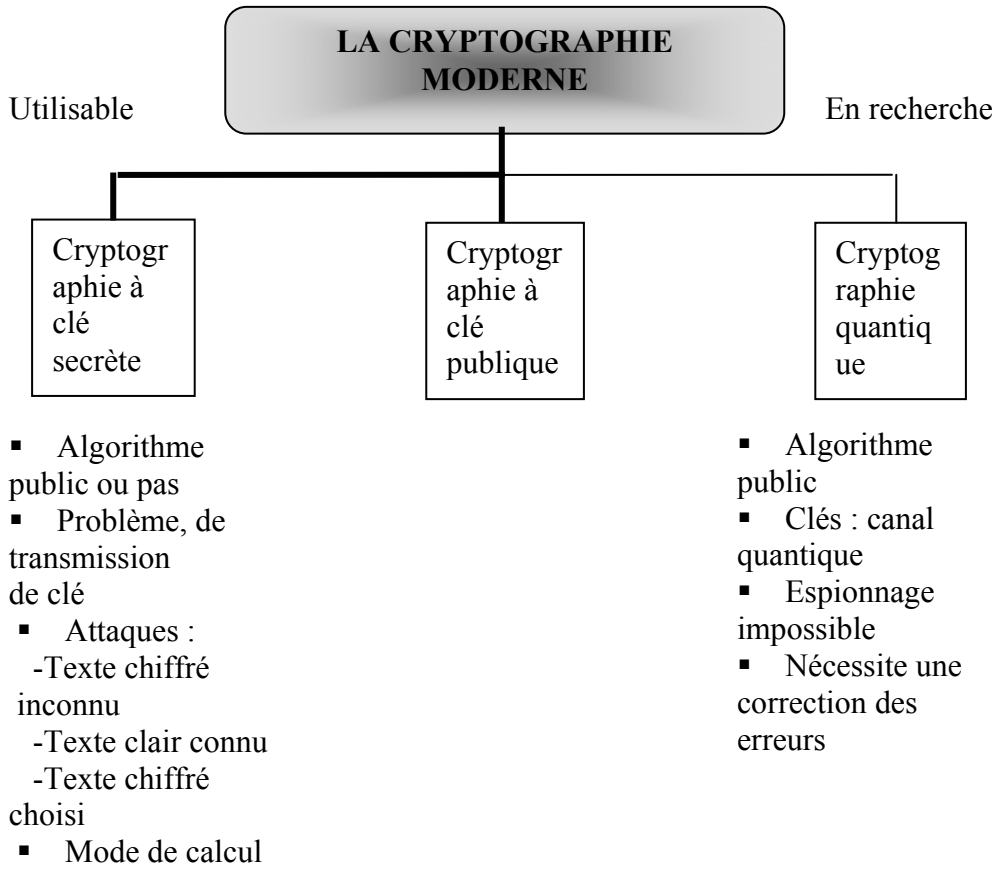


Fig.2.1 : Panorama de la cryptographié moderne

Le panorama représenté par la figure 2.1 fait appel à des notions qui seront expliquées par la suite. Les systèmes de cryptage les plus performants à l'heure actuelle (le DES par exemple) reposent sur des algorithmes publics (c'est à dire connus de tous) et souvent brevetés, ou seule une clé gardée secrète assure la confidentialité. Pour ces systèmes, il faut que seule la connaissance de la clé permette à un étranger de décoder le fichier crypté : en d'autres termes, il faut que les algorithmes soient très robustes pour que la cryptanalyse soit rendu impuissante.

Une autre approche, non-forcement disjoint à base de clés publiques, se positionne, désormais, dans le monde de la cryptologie des communications, sur réseaux comme la seule technique où la sécurité des données codées à bases de clés ne peut être compromise par l'inefficacité d'une tierce personne (le message de clé).

Une voie de recherche assez récente, qui apparaît très prometteuse, malgré les difficultés techniques auxquelles elle se heurte encore, est la cryptographie qualifiée de « quantique », parce qu'elle utilise comme véhicule de transmission de données un canal quantique.

2- 6 Terminologie

Comme on a défini le cryptage c'est le processus permettant de coder un message afin que sa signification ne soit pas évidente. Le décryptage est le processus inverse. Malgré des petites différences de signification, le terme codage, chiffrement et cryptage sont régulièrement substituées les une aux autres. On parlera donc de message clair « **P** » et le message chiffré « **C** » (voir figure 2.2). On notera « **E** » l'algorithme de codage, « **D** » son inverse pour obtenir enfin : **C** = **E**(**P**) et **P** = **D**(**C**), soit **P** = **D**(**E**(**P**)).

Fig.2.2 : Structure d'un système à chiffrement

Certains algorithmes de cryptage font appel à une clé pour que les messages chiffrés dépendent à la fois du message clair et des clés, si on dénote « **K** » la clé, on obtient :

C= **E**(**K**, **P**), ou on voit que E représente un ensemble d'algorithmes qui utilisent la même clé pour le codage et le décodage est appelé symétriques (figure : 2.3), on a donc **P** = **D**(**K**, **E**(**K**, **P**)). Les algorithmes asymétriques (figure : 2.4) utilisent deux clés différentes K_E et K_D de telle sorte que **P**= **D**($\mathbf{K_D}$, **E**($\mathbf{K_E}$, **P**)). Pour passer de **C** à **P**, il ne s'agit plus simplement d'inverser les étapes des E. Notons qu'un algorithme à clé est plus intéressant car même si l'algorithme tombe en de mauvaises mains, l'utilisation d'une clé non connue permet de garder la confidentialité.

Fig.2.3 : Structure d'un système à déchiffrement

Exemple

$c_i = E(p_i) = p_i + 3$

Soit pour tout l'alphabet :

Texte clair : A B C D E F G H I J … X Y Z

Texte codé : D E F G H I J K LM …A B C

L'utilisation de cette technique coderait donc le massage **P** «*somme*» en message C «*vrpph* », qui au premier abord n'a pas de lien direct avec le message clair de départ. Cependant, deux remarques peuvent déjà être faites. Aucune mention n'est faite sur le codage de l'espacement dans un message. Si celui-ci est traduit tel quel est, le message chiffré gardera la même séparation que l'original, la même découpe de mots, ce qui n'est avidement pas très sûr. Dès lors, la plupart des algorithmes effacent les espaces et pour la facilité de codage, découpent souvent les messages clairs en blocs de taille fixe. Comme deuxième remarque, insistons sur la répétition du « p » dans l'exemple précédent. Une telle répétition nous indique une voie de traitement. En effet, quelles peuvent être les lettres qui redoublent dans un mot si court ? Par un jeu d'essais, on pourrait passer par le « f », le «1», le « m » et éliminer une à une les voies qui nous induisent en erreur en traduisant le reste du mot.

2-6-1 Permutation

Une permutation est un réordonnement des éléments d'une série, qui peut s'énumérer ou s'exprimer sous la forme d'une fonction. On voit directement qu'une fonction de ce type peut aisément être utilisée pour le codage d'un message, le chiffrage de *César* en étant ailleurs un cas particulier.

2-6-2 Utilisation de clé

Dans ce cas-ci, la clé est le mot qui contrôle le codage. Les premières lettres de l'alphabet seront remplacées par celles du mot. Les autres utiliseront le reste de l'alphabet dans l'ordre. Plus la clé est longue, plus le décalage des lettres sera important, mais il faut toute fois noter qu'en général, les dernières lettres seront important étant donné que ces lettres ont en général une faible occurrence dans les différentes langues. Voici un exemple utilisant la clé « pain ».

Texte clair : A B C D E F … W X Y Z

Texte codé : p a i n b c … w x y z

2-7 Les procèdes cryptographiques

2-7-1 Les substitutions

Une façon de forcer le code d'un message consiste à utiliser une substitution de caractères. Seulement ce type de codage n'est pas conseillé en cryptanalyse car le message clair et le texte transformé par subincision ne change pas le contenue fréquentiel, donc on a une question qui se pose. Comment peut-on empêcher que la distribution de fréquence des lettres du message crypté ne reflète pas celle de la langue originale ? On peut, par exemple, coder les lettres de deux manières différentes. En français, si on code le « A » par un « V » e t le « X » par un « U », on obtiendra un message chiffré avec énormément de « V » et peu de « U ». Par contre, si on décide de coder le « A » par un « V » ou par un « U » et le « X » par un « U » ou par un « V », les deux distributions (U et V) vont se rassembler.

Pour combiner deux types de codage différents, on peut par exemple utiliser deux tables de traduction auxquels nous ferons appel une fois sur deux. Les lettres en position paire seront codées par l'une de deux tables alors que les impaires se seront codées par l'autre.

❖ ***Les tableaux de Vigenére :***

Afin d'aplanir la distribution d'occurrences, on peut choisir des permutations complémentaires. Bien entendu, même si c'est faisable, il n'est plus évident de trouver les deux bonnes permutations qui rendent la distribution la plus plane possible.

Une autre solution est d'étendre le nombre de permutations. En effet, plus le nombre de permutation augmente, plus la distribution a des chances de s'aplanir. Avec 26 permutations, chaque caractère peut être codé par n'importe quel autre. Un tableau de « ***Vigenére*** **»** est une collection de 26 permutations qui est, en générale, représenté sous forme de matrice 26x26 de ce type-ci.(Voir tableau2.1).

	a	**b**	**c**	**d**	**e**	**f**	**g**	**…**	**s**	**t**	**u**	**v**	**w**	**y**	**z**
A	a	b	c	d	e	f	g	…	s	t	u	v	w	y	z
B	b	c	d	e	f	g	h	...	t	u	v	w	y	z	a
C	c	d	e	f	g	h	i	...	u	v	w	y	z	a	b
D	d	e	f	g	h	i	j	...	v	w	y	z	a	b	c
E	e	f	g	h	i	j	k	...	w	y	z	a	b	c	d
F	f	g	h	i	j	k	l	…	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	…	z	a	b	c	d	e	f
…	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
V	v	w	x	y	z	a	b	…	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	…	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	…	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	…	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	...	s	t	u	v	w	x	y

Tab.2.1 : tableau de ***Vigenére***

Pour garder une trace des colonnes à utiliser, on fait généralement appel à une clé qu'on répète tout le long du message à coder. Si la clé est « isabelle », on ira voir dans la colonne « i » pour la première lettre à coder dans la colonne «s» pour le deuxième, si le message est plus grand que la clé, on répète la clé.

2-7-2 La transposition

La transposition est un réarrangement des symboles d'un message. Son but est donc la diffusion de l'information du message à travers tout le message chiffré et donc de séparer les motifs connus et récurrents.

La transposition en colonne est la permutation la plus connue. Les caractères sont séparés en bloc de k colonnes pour ensuite être envoyés par colonne. Un exemple reste plus parlant (k = 5) :

c_1 c_2 c_3 c_4 c_5

c_6 c_7 c_8 c_9 c_{10}

c_{11} c_{12} c_{13} c_{14} c_{15}

c_{16} c_{17} c_{18} …

Ensuite, on envoi le texte en lisant les colonnes :

c_1 c_6 c_{11} c_{16} c_2 c_7 c_{12} c_{17} …

Etant donné la technique utilisée, on peut remarquer qu'il est nécessaire de stoker tout le message avant de pouvoir l'envoyer crypté, il y'aura donc un certain délai avant la propagation du message. Aussi, la transposition en colonne est rarement utilisée pour des longs messages. Dans le cas où le nombre de caractères du message ne serait pas un multiple du nombre de colonnes, on ajoute en générale un caractère à faible occurrence aux colonnes trop courtes afin de pouvoir comprendre la transposition tout en détectant les caractères en trop.

2-8 Cryptosystèmes

2-8-1 Définition

Le but d'un cryptosystéme est de chiffrer un texte ou message clair en un texte chiffré incompréhensible appelé cryptogramme. Le destinataire légitime doit pouvoir déchiffrer le message. Mais en espion (cryptonyme ou descripteur) peut intercepter le cryptogramme, il faut donc qu'un cryptosystéme puisse empêcher le décryptage. Il faut faire une distinction entre le déchiffrement qui est effectué par le destinataire légitime et le décryptement effectué par un espion.

Il existe plusieurs types de cryptosystéme :

- ✓ A usage restreint.
- ✓ A usage général.
  - ❖ A clé secrète (ou symétriques).
  - ❖ A clé publique (ou asymétriques).

2-8-2 Cryptosystéme à usage restreint

C'est un cryptosystéme dont la sécurité ne repose que sur le secret de chiffrement et de déchiffrement. Ce type de cryptage n'est pas sécurisant, il est très souvent l'œuvre d'amateur. Il est donc très facile pour un cryptanalyste professionnels de percer à jour la méthode utilisée. De plus, il ne peut pas répondre aux besoins actuels des systèmes de communications entre un grand nombre d'utilisateurs. Rappelons que les codes, qui sont couramment utilisés en télécommunications, sont des crypto systèmes à usage restreint dont les méthodes sont connues.

2-8-3 Cryptosystéme à usage général

C'est un système dont la sécurité ne repose pas sur le secret des opérations de chiffrement et de déchiffrement mais sur une information appelée clé. Petit détail qui à son importance, les utilisateurs sont indépendants des concepteurs car la sécurité repose sur la clé, bien sûr cela ne veut pas dire qu'il y'a une sécurité absolue. Néanmoins la sécurité du système peut être accrue en gardant secret les opérations de chiffrement et de déchiffrement comme pour les applications militaires, par exemple.

2-8-3-1 Cryptosystéme à clé secrète

Dans ce système une clé (ou une combinaison de plusieurs) permet à la fois de crypter et de décrypter. Cela nécessite la gestion des clés car l'émetteur et le destinataire doivent connaître la clé. Il faut de plus établir une liaison sûre entre utilisateurs pour transmettre la clé. Remarquons que dans les réseaux de télécommunications actuels, le partage de clés entre chaque paire d'utilisateurs est impensable car le nombre de clés requises serait le carré du nombre d'utilisateurs. Le cryptosystéme à clé secrète le plus connu est le DES (Data Encryption Standard).

2-8-3-2 Cryptosystéme à clé publique

Pour contrer les difficultés d'un cryptosystéme à clé secrète, les cryptologues sont partis d'une observation fondamentale : Celui qui chiffre un message n'a pas besoin de pouvoir le déchiffrer. Ainsi chaque utilisateur crée une paire de clés à partir d'un algorithme connu et rend public une des deux clés. Une clé permet de chiffrer et une autre de déchiffrer. Il n'y a plus de problèmes de distribution des clés. Bien sûr, les opérations de chiffrement et de déchiffrement sont publiques. RAS (Rivest Shamir et Adelman) est l'exemple le plus connu d'un tel système.

2-8-4 Cryptosystéme à clé symétrique (à clé secrète):

2-8-4-1 Définition

Historiquement, les cryptosystémes à clé secrète ont été les premières à être mis au point pour assurer la protection des informations. Dans ce cryptosystéme, une clé permet à la fois de crypter et de décrypter. Cela nécessite la gestion des clés car l'émetteur et le destinataire doivent connaître la clé. Il faut de plus établir une liaison sûre entre utilisateurs pour transmettre la clé. Remarquons que dans les réseaux de télécommunications actuels, la partage de clé entre chaque paire d'utilisateurs est impensable car le nombre de clés requises serait le carré de nombre d'utilisateurs. Le cryptosystéme à clé secrète (symétrique) le plus connu est DES. (Voir figure2.4).

Ce dernier remonte à 1974, il est d'origine IBM. Son principe est très simple puisqu'il est basé sur deux opérations simples de cryptage : la transposition et la substitution. Ces deux opérations sont très simples, sont en fait les opérations de base de manipulation de bits ce qui permet facilement d'intègres DES dans un circuit électronique.

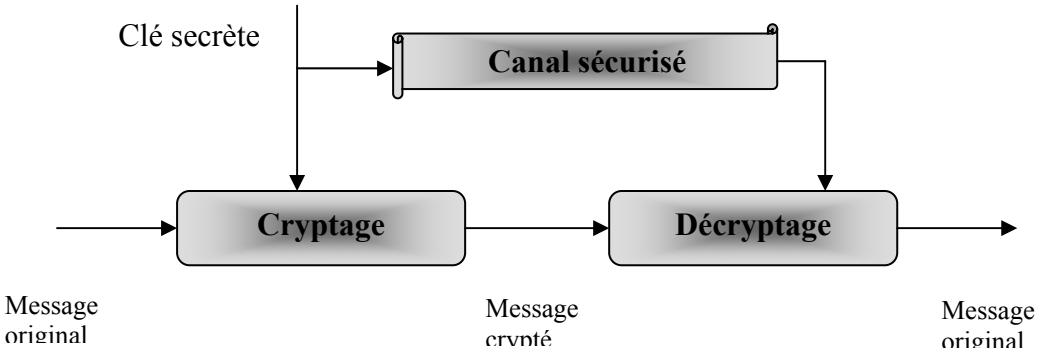


Fig.2.4 Cyptosystéme à clé secrète

2-8-4-2 Avantages

Le chiffrement à clé symétrique a des avantages : il est très rapide, utile pour chiffrer des données électroniques. Cependant, le chiffrement conventionnel est un moyen de transmission de données sécurisées peut être assez onéreux simplement en raison de la difficulté de la distribution de la clé. Pour qu'un chiffrement conventionnel, les utilisateurs doivent se mettre d'accord sur une clé et la garder secrète entre eux.

2-8-4-3 Inconvénients

Le cryptage symétrique présente quelques inconvénients par exemple. Les deux parties doivent partager le secret d'une clé commune. Par extension, si on a **n** correspondants, il faut donc maintenir **n** clés secrètes. On utilisant la même clé pour deux correspondants différents ceci entraîne que chacun serait en mesure de consulter le message de l'autre. Le cryptage symétrique pose en outre un problème d'authentification de l'émetteur et le récepteur d'échange électronique.

L'authentification via un système à clé secrète nécessite le partage de secret et parfois d'avoir recours en un troisième acteur. De cette façon, une personne envoyant des messages peut les répudier en prétextant que la clé dévoilée par une des parties.

- N'assure pas l'intégrité.
- N'assure pas l'authentification ; n'assure pas la non-répudiation.
- Des problèmes des distributions des clés.

Le problème de cryptographie symétrique est un problème continuel, c'est pour cela qu'un autre système cryptographique fait son apparence à savoir la cryptographie à clé publique.

2-8-5 Cryptosystéme à clé asymétrique (à clé publique)

2-8-5-1 Définition

Dans les systèmes cryptographiques à clé asymétrique, tout le monde possède deux clés complémentaires, une clé publique que l'on distribue et une clé secrète. Chaque clé déverrouille le code produit par l'autre clé. Le fait de connaître la clé publique ne permet pas d'en déduire la clé secrète correspondante. La clé publique

peut être publiée et largement disséminée sur un réseau de communication. Ce procédé permet de préserver le respect de la vie privée sans avoir besoin d'un canal sécurisée, nécessaire aux systèmes cryptographiques traditionnels. Toute personne peut utiliser la clé de son destinataire pour lui envoyer un document codé, celui ci utilisera cette propre clé secrète correspondante pour décoder le document. Personne, en dehors du destinataire, ne peut le décrypter, car personne d'autre n'a accès à cette clé secrète. Même la personne qui a codé le message n'est pas en mesure de le crypter.

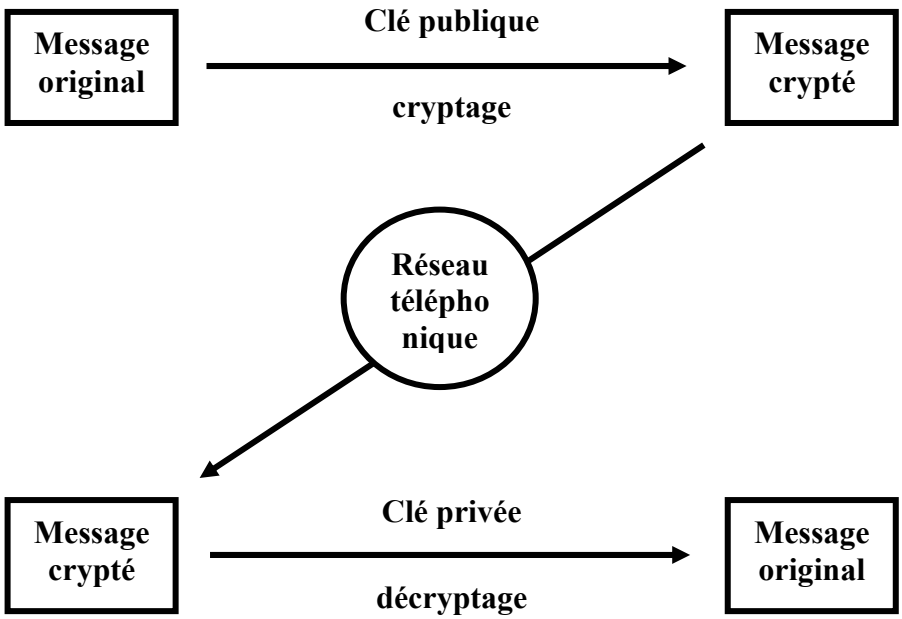


Fig.2.5 : Cryptographie à clé publique

2-8-5-2 Avantages

Le premier avantage de la cryptographie asymétrique (à clé publique) est d'accroître la sécurité tout en restant très commode : en effet les clés privées n'ont jamais besoin d'être transmise. Un autre avantage majeur de la cryptographie à clé publique est qu'il peut être utilisé pour les signatures digitales.

a- Signature à clé secrète

L'authentification des messages est également possible. La clé secrète de l'envoyeur peut être utilisée pour coder un message, de cette façon il le signe. Ceci

crée une signature numérique du message, que le destinataire (ou n'importe qui d'autre) peut vérifier en utilisant la clé publique de l'expéditeur afin de décoder. Ceci prouve que l'expéditeur est bien la personne qui à l'origine du message et que le message n'est pas modifié dans l'intervalle par personne d'autre, puisque l'expéditeur est le seul qui possède la clé secrète qui a fait la signature. Tout contre façon d'un message signé est impossible, de même l'expéditeur ne peut pas désavouer sa signature par la suite.

b- Détection des erreurs

La signature électronique a l'avantage sur la signature naturelle de valider aussi bien l'identité du signataire que le contenu du message. Aussi longtemps que l'on utilise une fonction de hachage, il n'y a pas de possibilité de prendre la signature d'une personne sur un document et de l'attribuer à un autre document.

Le plus petit changement dans un message entraînera un échec dans la vérification de la signature. Donc la signature électronique permet de s'assurer de l'intégrité du document mais dans le cas ou la vérification de la signature a échoué, on ne peut pas définir facilement si cela est du à une erreur de transmission ou à une manœuvre de piratage.

c- Fonction à sens unique

Une fonction à sens unique est une fonction mathématique qui est beaucoup plus facile à résoudre dans un sens que dans l'autre. Par exemple, on peut résoudre cette fonction en une seconde mais retrouver la fonction pour laquelle on peut trouver la solution inverse facilement pour certains valeurs mais pas pour d'autres.

Les clés publiques sont basées sur des fonctions à sens unique à trappe. La clé publique donnes des informations sur le cas particulier de la fonction. La clé privée quant elle donne des informations à propres de la trappe, n'importe qui connaissant la trappe peut résoudre la fonction que dans le sens « avant ».

Le sens « avant » est utilisée pour le cryptage et la vérification de signature, la direction inverse est utilisée pour le décryptage et de génération de signature.

Dans presque tous les systèmes de clés publiques, la taille correspond à la taille des données entrées dans la fonction à sens unique. Plus la clé est longue plus la difficulté de résolution des deux sens est importante pour une personne ne connaissant pas le trappe.

Tout le système de cryptage sont basés sur des fonctions à sens uniques, mais aucune de ces fonctions n'a été démontrée comme étant réellement une fonction à sens unique, cela signifie qu'il est théoriquement possible de trouver un algorithme de décryptage très rapide même pour une personne ne possédant pas le trappe. Si cela arrivait la cryptographie basée sur les fonctions à sens unique deviendrait obsolète. D'un autre coté si l'on pouvait démontrer que certaines fonctions étaient réellement à sens unique cela ouvrait des possibilités non exploitées à ce type de cryptographie.

2-8-5-3 Inconvénient

L'inconvénient principal de cryptage à clé publique est que ce système est relativement lent d'où la plupart des cryptages par clé privée sont plus rapides que ceux utilisant une clé publique.

PARTIE 2 :
INTERFACE AVEC LA LIGNE TELEPHONIQUE

CHAPITRE1 :

DESCRIPTION THEORIQUE DE L'INTERFACE TELEPHONIQUE

1-1 Définition et rôle de l'interface téléphonique

D'après, le premier chapitre de la généralité, nous avons vu que le signal téléphonique est compris dans une bande de fréquence (300Hz – 3400Hz) qui contient deux types des signaux : le signal de signalisation qui occupe la bande 300Hz – 500Hz, et le signal de parole qui occupe la bande 500Hz – 3400Hz. De ce fait il faut trouver une solution pour la séparation de ces deux signaux, puisque le module de cryptage ce fait seulement sur le signal de parole.

Nous proposons, comme solution, l'utilisation d'un bloc de filtrage (voir figure 1.1). Un filtre passe bas avec une fréquence de coupure f_c égale à 500Hz pour faire passer les signaux de signalisation et un filtre passe haut de même fréquence de coupure pour faire passer les signaux de parole.

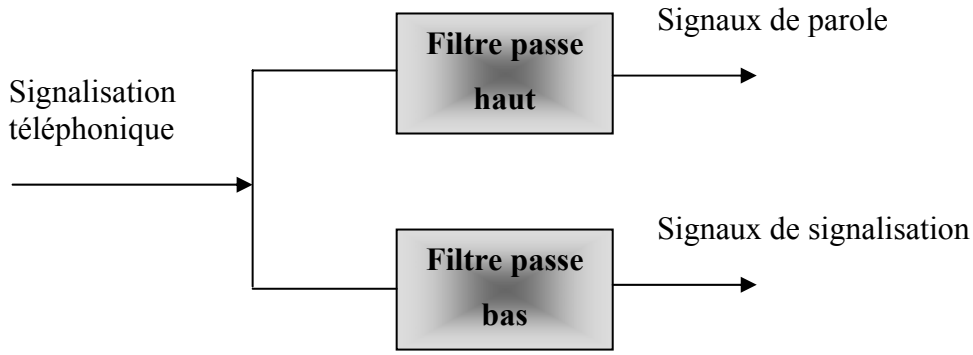


Fig.1.1 : Séparation de la parole et la signalisation

De même, pour crypter un signal, il faut qu'il soit numérique. De ce fait, nous faisons une conversion analogique numérique à l'aide d'un convertisseur A/N, et inversement après le chiffrement du signal, il faut une autre fois faire une conversion numérique analogique à l'aide d'un convertisseur numérique analogique pour le pouvoir le transmettre sur le réseau RTCP.

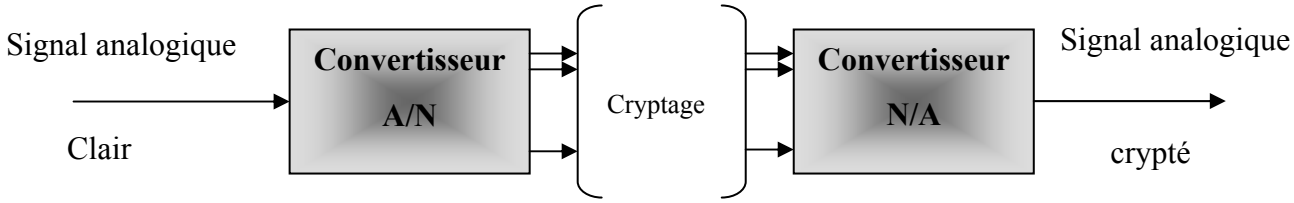


Fig.1.2 : Etage de conversion

A la fin, il faut sommer les deux signaux, signaux de signalisation et le signal de parole, pour cela nous avons utilisé un sommateur inverseur et un inverseur pour faire rendre le signal à son état initial.

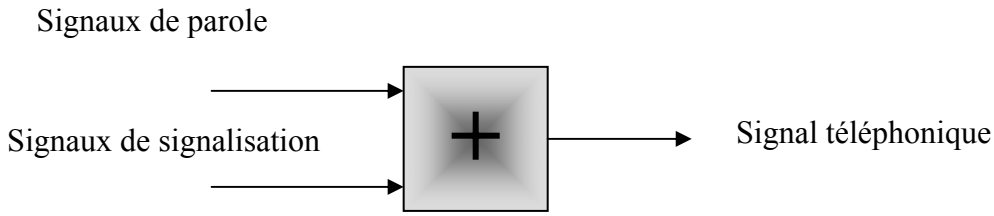


Fig.1.3 : Etage de sommation

Ainsi, notre interface téléphonique se compose par trois étages (voir figure 1.4)

- Etage de filtrage.
- Etage de conversion.
- Etage de sommation.

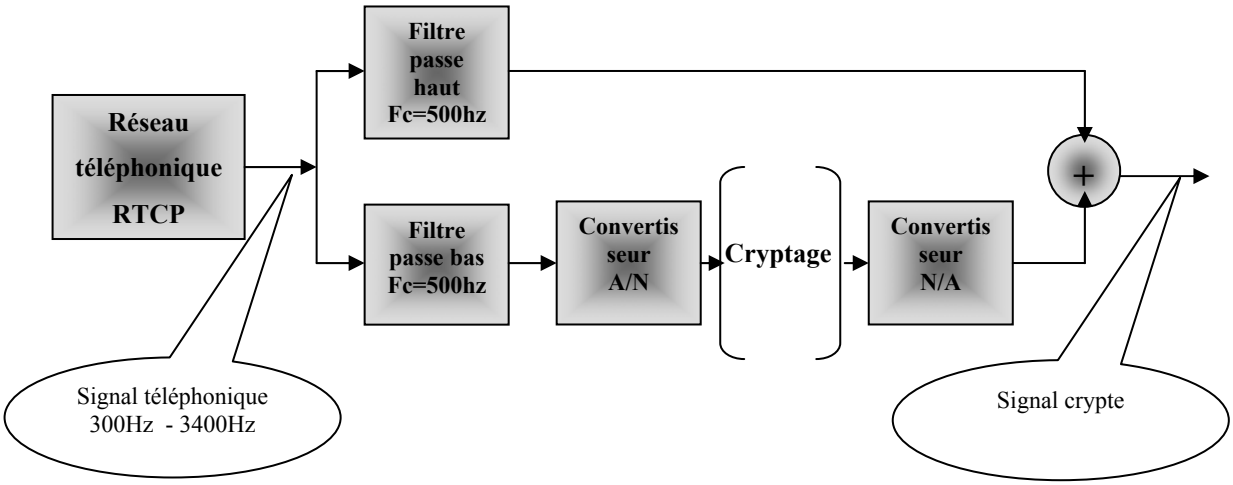


Fig.1.4 : synoptique d'interface téléphonique

1-2 Etage de filtrage

1-2-1 Introduction

Les filtres actifs sont réalisés avec des réseaux RC placés en liaison ou dans la boucle de contre réaction d'un amplificateur opérationnel. Les filtres actifs ont les avantages suivants :

- ❖ Impédance de sortie très faible.
- ❖ Suppression de bobinage en particulier sur filtres HF nécessiteraient en filtres passifs des bobines d'inductance encombrantes et difficiles à fabriquer.
- ❖ Obtention de forts coefficients de sur tension avec des composants de tolérances très faibles.

Les filtres actifs (ou filtres électroniques) présentent des performances très séduisantes : pas de limite dans les fréquences de coupure ; facilité de mise au point ou de modification de fréquence ; miniaturisation ; bonne stabilité ; pas de perte d'insertion, le rapport signal de sortie sur signal d'entré étant en principe ajusté pour être égal à l'unité.

Il existe trois catégories principales des filtres actifs :

❖ Le filtre passe haut qui laisse passer toutes les fréquences supérieures à la fréquence de coupure choisie f_c et élimine toutes les fréquences inférieures.

❖ Filtre passe bas qui laisse passer toutes les fréquences inférieures à f_c choisie et élimine toutes les fréquences supérieures.

❖ Filtre passe bonde qui laisse passer toutes fréquences compris entre deux fréquences de coupure f_{c1} et f_{c2}

1-2-2 Le filtre passe haut

La figure.1.5 : présente un filtre actif passe haut conçu autour d'un circuit intégré amplificateur opertionnel ; la détermination des composants se fait de la manière suivante :

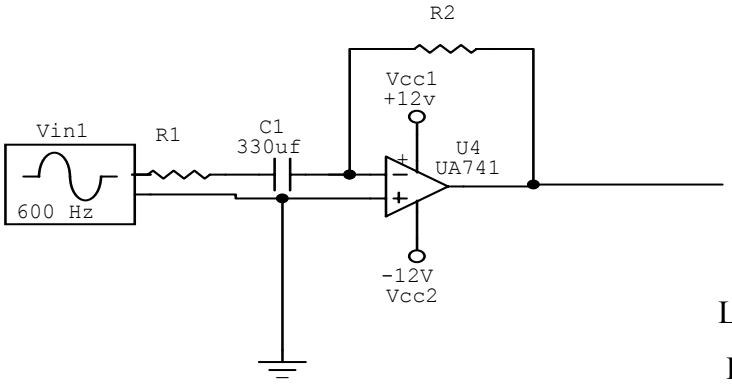


Fig.1.5 : Filtre actif passe haut

Liste de composants

R1 = 1Ω

R2 = 1Ω

C1 = 330µF

Choisir R1 et R2 afin que l'entrée inverseuse (-) soit polarisée correctement. On donne une valeur convenable à la résistance R1 déterminée par l'expérience et on calcul R2 à l'aide de l'expression de fréquence de coupure $\boldsymbol{f_c}$ **=1/(2Π R2c).** (pour notre exemple f_c= 500Hz) dont :

$\boldsymbol{f_c}$ est exprimée en Hz.

R est exprimée en ohm (Ω).

C est exprimée en Farad (F).

Les autres relations sont :

AV = Vsortie/Ventrée (gain en tension).

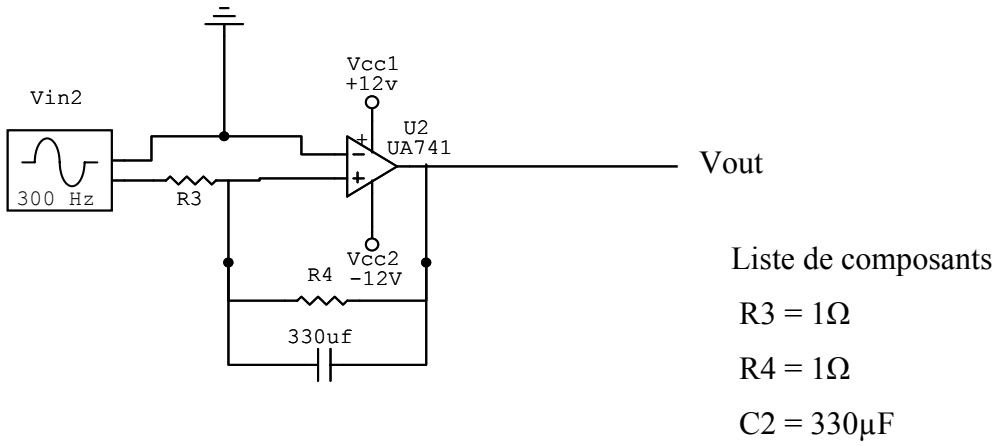
AV(dB) = 20 log (Vsortie/Ventrée) (gain en tension en dB).

Wc = 1/(R2c) = 2Π*f*c (en rd/s) (pulsation de coupure).

Les grandeurs **AV**, **Wc**, ***f*c** sont choisies d'avance en tenant compte de la bande de fréquence à éliminer.

1-2-3 Filtre passe bas

La figure 1.6 : présente un filtre actif passe bas dont la méthode de détermination réside dans l'expérience suivante :



Liste de composants

R3 = 1Ω

R4 = 1Ω

C2 = 330µF

Fig.1.6 : Filtre actif passe bas

Comme précédemment on fixe les valeurs de **AV**, **Wc**, f_c.

Pour notre exemple on a fixé C (330µF) puis on détermine R4 à partir de la fréquence de coupure f_c.

Remarque

La résistance R3 est choisie égale à R4 pour faciliter la dimensionnement.

1-3 Etage de conversion

1-3-1 Introduction

Un convertisseur analogique / numérique (CAN) est un circuit permettant de transformer en valeurs numériques une tension analogique.

Les convertisseurs numériques / analogiques permettent de restituer un signal analogique à partir d'un signal numérique.

1-3-2 Etude du convertisseur A/D (ADC 0809)

1-3-2-1 Description

Les ADC 0808 et 0809 sont des circuits monolithiques CMOS comportant un convertisseur A/D 8 bits, un multiplexeur 8 canaux et un circuit de contrôle. Le convertisseur est à approximations successives mettant en œuvre, outre la logique de contrôle, un réseau R//2R de résistances, un réseau de commutateurs analogiques (Switch) ainsi qu'un comparateur.

Le multiplexeur 8 voies permet d'accéder directement à chacun des 8 signaux analogiques selon le code binaire des adresses 'A2 Al A0' = 'C B A' présenté à l'entrée du décodeur d'adresse interne du composant. Le code des adresses est verrouillé sur une impulsion au niveau haut appliquée sur 1'entrée ALE.

1-3-2-2 Caractéristiques de l'ADC 0809

- Bonne précision vue sa résolution sur 8 bits.
- Vitesse de conversion 100µs.
- Interface aisée avec tous les microprocesseurs.
- Entrée analogique de 0 à 5v.
- Plage de température de -40ºC à +85ºC.
- Multiplexage de 8 canaux analogiques.
- Faible consommation 15mW.

1-3-2-3 Brochage

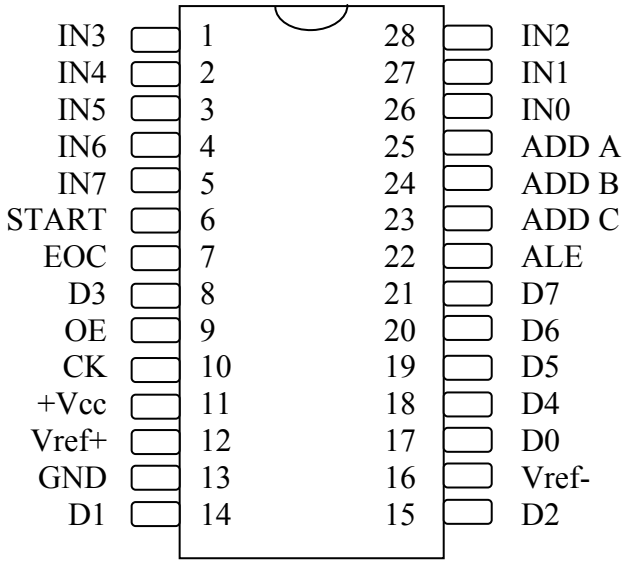


Fig.1.7 : Boîtier de circuit intégré ADC 0809

- IN0 à IN7 : Les lignes correspondantes aux 8 canaux analogiques.
- D0 à D7 : 8 bits de la sortie numérique.
- ADD A, ADD B, ADD C : Les lignes d'adresse qui sélectionnent le canal désiré.
- START : La ligne autorisant l'écriture des données analogique à convertir.
- ALE : La ligne de validation de l'adresse en cours.
- OE : La ligne autorisant la lecture des données résultant de la conversion.
- EOC : Un signal qui indique la fin de conversion.
- CLK : L'entrée d'horloge extérieure qui commande la conversion
- Vref+ et Vref- : Les tensions de référence.

1-3-2-4 Principe de fonctionnement

L'ADC 0809 a pour erreur totale sans ajustement –1 LSB. Son principe de fonctionnement utilise la technique de conversion par approximations successives à détection de seuil.

Le multiplexeur analogique sélectionne un parmis les 8 signaux des canaux d'entrée déterminée par le décodeur d'adresse, l'initialisation est assurée par les impulsions de START. La duré entre deux périodes est de 32 périodes de l'horloge. La conversion peut être interrompue par une nouvelle impulsion de START avant la fin de 64 périodes de l'horloge.

Sélection des entrées analogiques

entrées analogiques sélectionnées	C	B	A
IN0	**0**	**0**	**0**
IN1	**0**	**0**	**1**
IN2	**0**	**1**	**0**
IN3	**0**	**1**	**1**
IN4	**1**	**0**	**0**
IN5	**1**	**0**	**1**
IN6	**1**	**1**	**0**
IN7	**1**	**1**	**1**

Tab1.1 : les entrées analogiques des ADC 0809

Le code numérique '**N**' de sortie pour une valeur quelconque de la tension d'entrée $\mathbf{V_{IN}}$ s'obtient par :

$$\mathbf{N = [(V_{IN} - V_{REF-})/ (V_{REF+} - V_{REF-})] \times 256 \pm \text{précision absolue}}$$

1-3-3 Etude du convertisseur DAC0800

1-3-3-1 Description

La série DAC 0800 sont des circuits monolithiques convertisseurs D/A 8 bits à grande vitesse (100ns). Utilisé comme multiplicateur DAC, ses performances supérieures à 40 pour 1 sur le courant de référence sont possible.

Les DAC0800 possèdent deux sorties complémentaires de courant permettant 20V crête à crête de sortie. La référence pleine échelle, meilleure que 1LSB élimine la correction dans la plupart des cas et les linéarités supérieures à 0,1% minimisant les accumulations d'erreurs.

1-3-3-2 Brochage

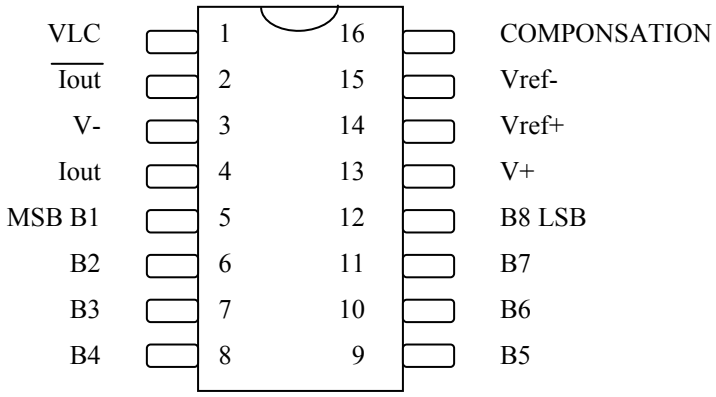


Fig.1.8 : Boîtier de circuit intégré DAC0800

- VLC : «threshold control» ligne qui permet le contrôle de conversion.
- $\overline{\text{Iout}}$: Ligne correspond à la sortie analogique inversée.
- Iout : Ligne correspond à la sortie analogique non-inversée.
- V-, V+ : Les tensions d'alimentation.
- B1, B2, B3, B4, B5, B6, B7, B8 : Les lignes correspondent aux 8 canaux numériques d'entrée.
- Vref-, Vref+ : Les tensions de référence.

1-3-3-3 Caractéristiques

- Tension d'alimentation ±18V ou 36V.
- Puissance dissipée 500mW.
- Tension de référence différentielle d'entée V^- à V^+.
- Plage de référence en mode commun V^- à V^+.
- Courant de référence d'entrée 5mA.
- Entrée logique V^- à V^+ plus 36V.
- Température de fonctionnement –65°C à +150°C..
- Température d'une broche (soudage, 10s) 300°s.

1-3-3-4 Particularités

- Grande vitesse d'établissement du courant de sortie : 100ns.
- Erreur pleine échelle : ±1LSB.
- Non-linéarité quelle que soit la température : ±0,1%.
- Dérive du courant plein échelle : ±10ppm/°C.
- Grande excursion de sortie : -10V à +18V

1-4 Etage de sommation (montage additionneur-inverseur et inverseur)

1-4-1 Montage additionner inverseur

Le circuit additionneur est donné par la figure 1.9 qui nous permet de faire le mélange de signaux de parole crypté et de signaux de signalisation

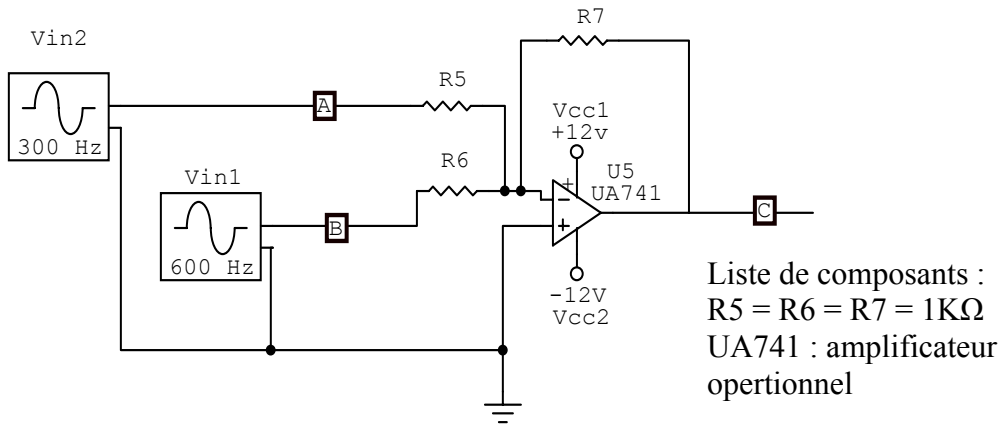


Fig.1.9 : Montage de l'additionneur inverseur

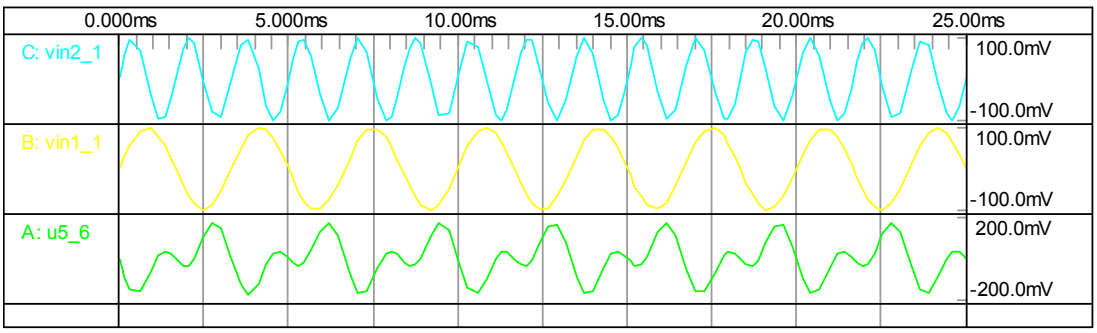
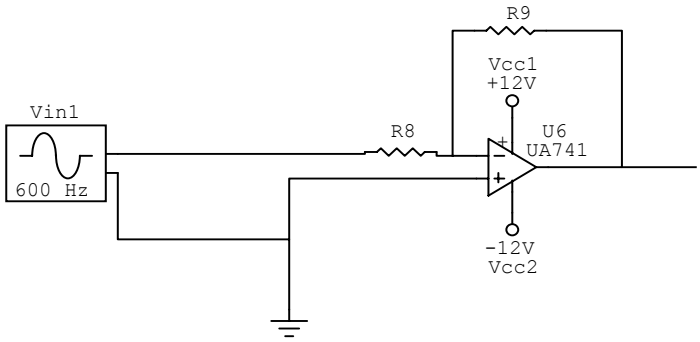


Fig.1.10 : Simulation du montage de l'additionneur inverseur

1-4-2 Montage inverseur

C'est le montage de base amplificateur opérationnel. L'entrée non inverseuse est reliée à la masse ; le signal d'entrée est relié à l'entrée inverseuse par une résistance R_8, et la sortie est reliée à cette entrée par une résistance R_9.



Liste de composant :
R8 = R9 = 1KΩ
UA741 : amplificateur opertionnel

Fig.1.11 : Montage de l'inverseur

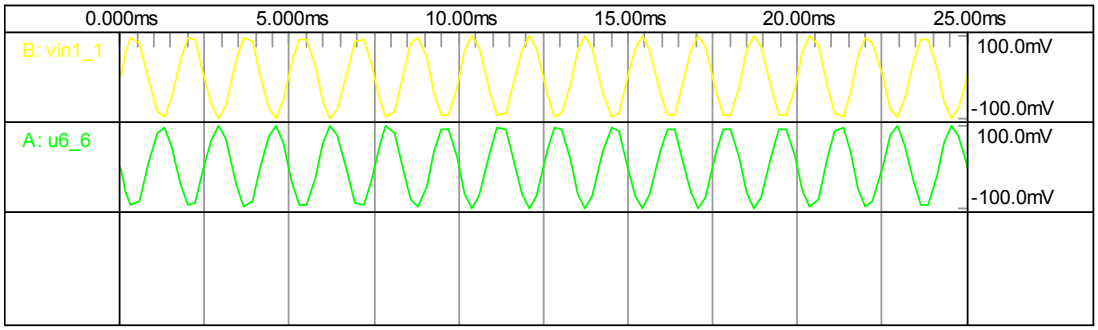


Fig.1.12 : Simulation du montage inverseur

CHAPITRE2 :

REALISATION PRATIQUE

2-1 Introduction

Dans cette partie nous nous proposons d'établir une étude pratique des différents étages. Nous débuterons par décrire les différentes étapes de réalisation de la carte. Nous terminerons par des essais et des mesures nécessaires pour le bon fonctionnement de la carte électronique.

Différentes étapes sont abordées pour mener à terme la réalisation de la carte électronique. Ainsi on a effectué :

- La saisie du circuit électronique et sa simulation en utilisant comme logicielle « CIRCUIT MAKER »
- Le routage effectué par la même logicielle (le CIRCUIT MAKER).
- L'implantation et la soudure des composants sur le support en cuivre.

2-2 Schéma électronique de la carte

2-2-1 Alimentation et composants utilisés

Les différents blocs de la carte nécessitent diverses tensions pour alimenter les circuits utilisés.

- Une tension continue de +12V et –12V pour faire alimenter les circuits de l'amplificateur UA741.
- Une tension continue de +5V et –5V pour faire alimenter les circuits de convertisseurs ADC 0809 et DAC 0800

Les composants utilisés pour notre schéma électronique sont des amplificateurs, des résistances, des capacités, et des convertisseurs. (Voir liste de composants).

Fig.2.1 : Schéma bloc de carte électronique

Liste des composantes :

- Résistances :

R1 = R2 = R3 = R4= 1Ω

R5 = R6 = R7 = R8 = R9 = 1KΩ

- Capacités :

C1 = C2 = 330µF

- Amplificateurs opertionnels :

4 x UA741

- Convertisseur :

ADC 0809 : convertisseur analogique numérique à 8 bits de sortie.

DAC 0800 : convertisseur numérique analogique à 8 bits d'entrée.

2-2-2 La saisie de schéma

La saisie de schéma électrique est faite à l'aide du logiciel « CIRCUIT MAKER ». Il s'agit de choisir les différents composants utiles de la bibliothèque, ceci on ouvrant la bibliothèque (***Browse***), on choisit les composants voulus. Une fois placée, on effectue les différentes liaisons.

Il arrive qu'on ne trouve pas le composant voulu, il faut alors procéder à sa création. (**Exemple** : pour notre schéma électrique on a fait la création des deux convertisseurs ADC 0809 et DAC 0800).

La figure 2.1 montre les différentes fenêtres de CIRCUIT MAKER ainsi que la page de saisie des schémas.

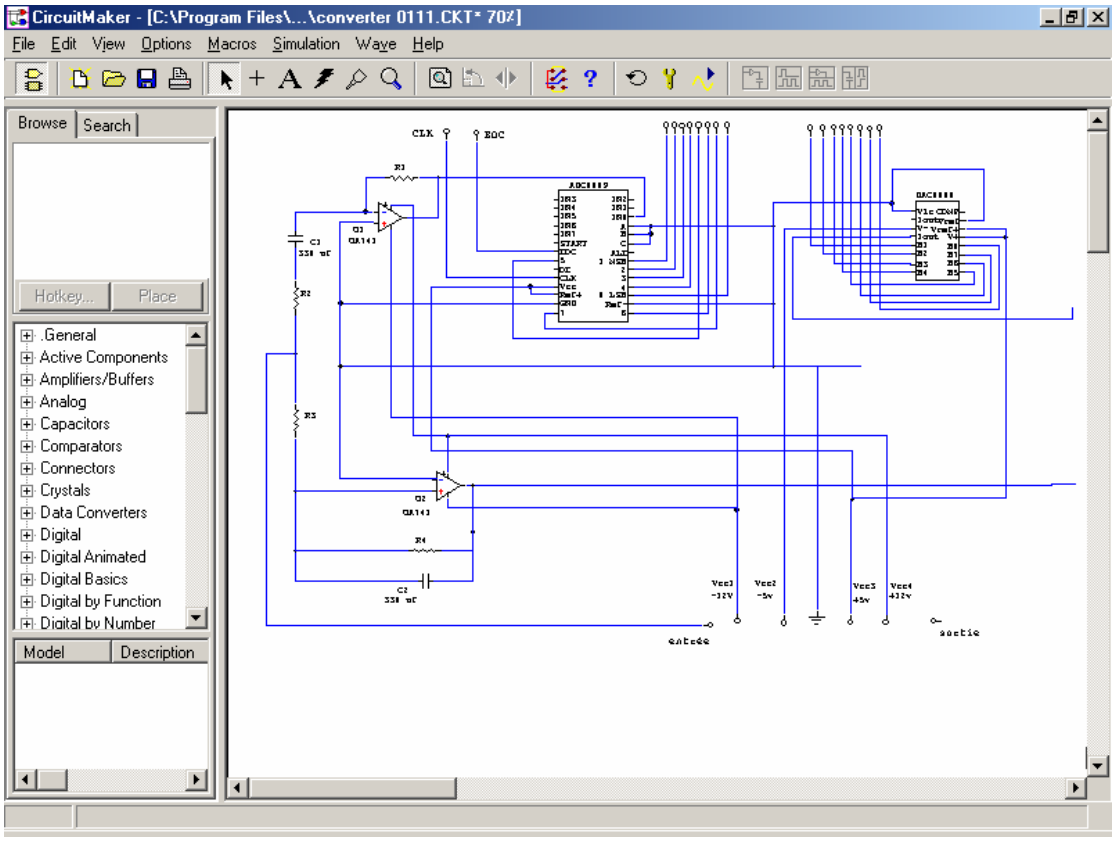


Fig.2.2 : Fenêtre de CIRCUIT MAKER pour la saisie de schéma

2-2 Schéma de routage

Le circuit imprimé illustre l'emplacement des composants et les différentes STRAP. Cette opération s'appelle routage. Elle est réalisée en utilisant le « TRAX MAKER ». Il s'agit d'établir la même étape que le saisie de schéma effectué dans « CIRCUIT MAKER ».

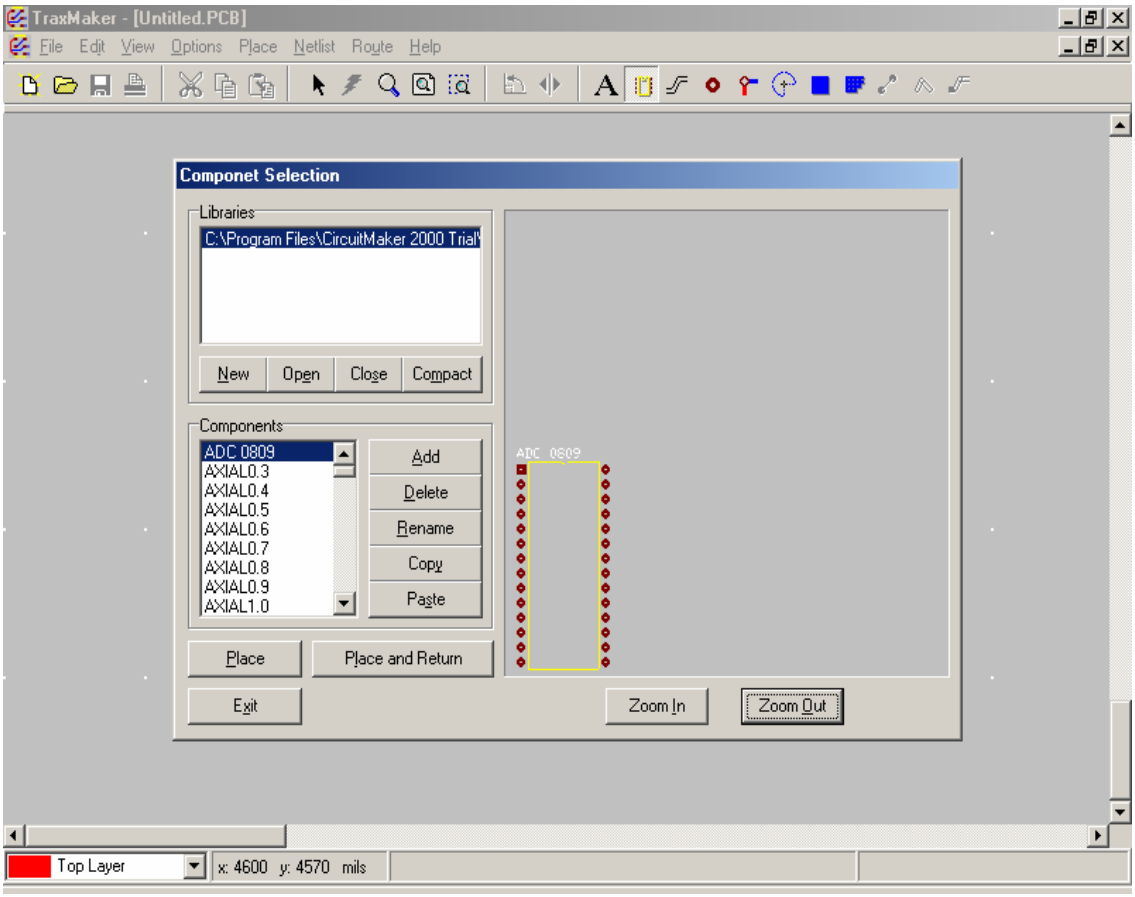


Fig2.3 : Principe d'utilisation de TRAX MAKER

Pour faire le routage, on fait placer les composants puis, dans le menu ***Route***, on clique sur ***Board.***

Remarque : ce logiciel fait le routage en double face pour cette raison on a fait le schéma de routage manuellement.

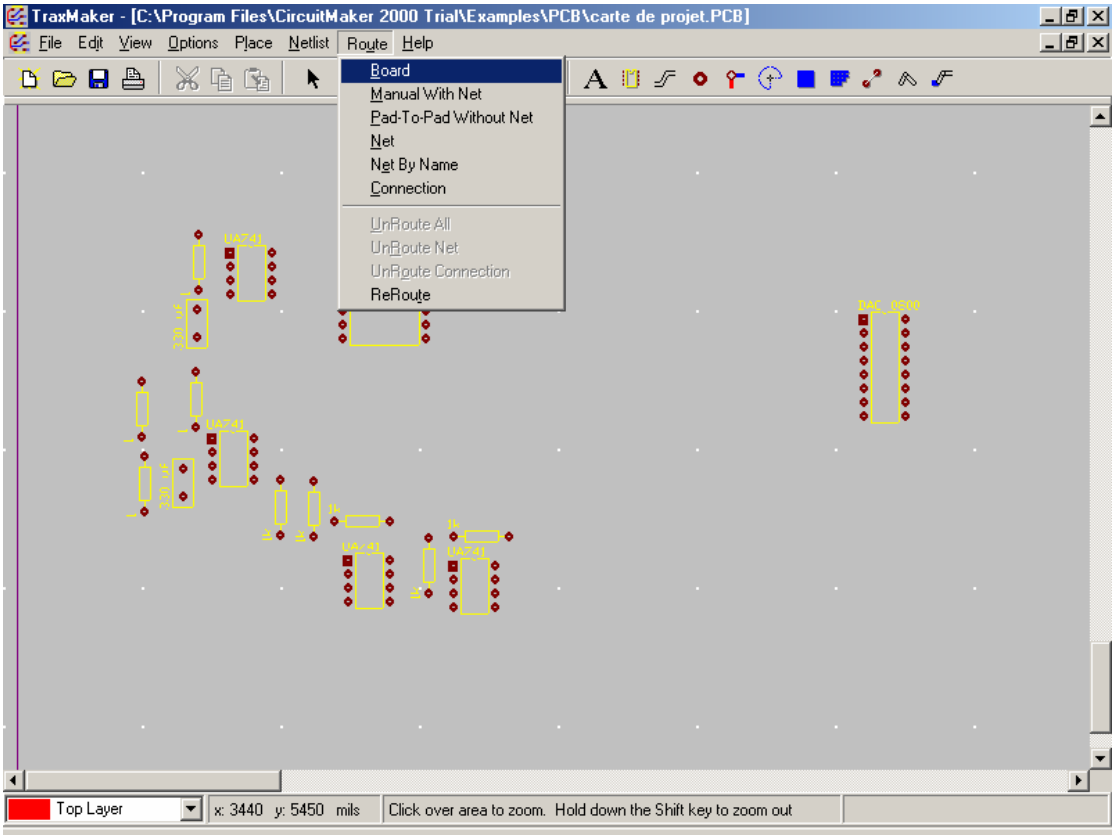


Fig.2.4 : principe de routage de TRAX LAKER

2-2-1 Plan de pose des composantes

Lors de l'emplacement de différents circuits, il est conseillé d'éviter l'encombrement des composantes. Cela peut inhiber le routage de certaines liaisons. De plus, il vaut mieux éloigner les résistances et les capacités des circuits intégrés pour faciliter le routage à travers les pattes des circuits intégrés.

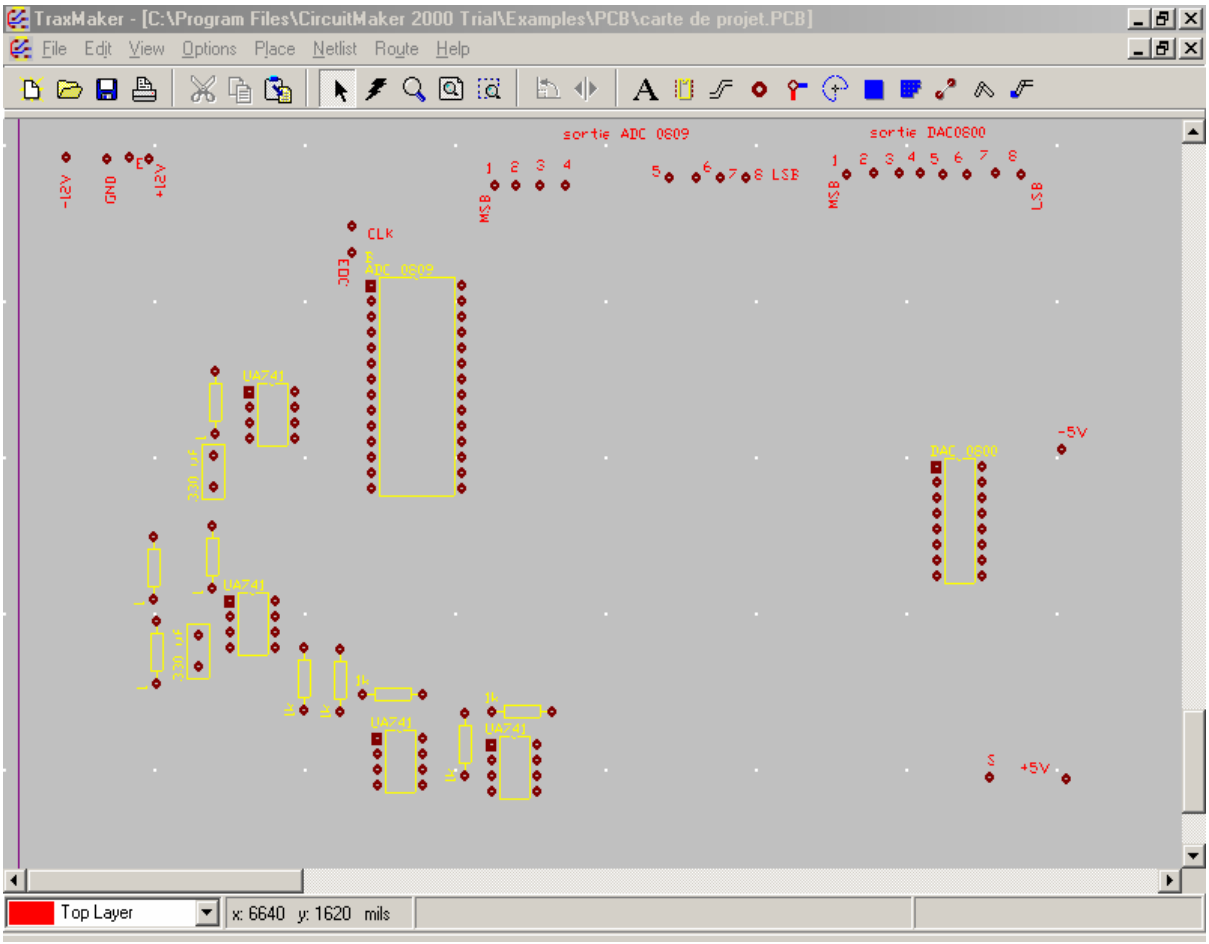


Fig2.5 :Plan de pose des différentes éléments

2-2-2 Routage

Après avoir choisir la disposition convenable des différents composants, on effectue le routage

Remarque : le routage de circuit électrique par le logiciel « TRAX MAKER » donne un résultat de routage double face. En effet, on a fait le routage de notre circuit manuellement. (voir le figure 2.6)

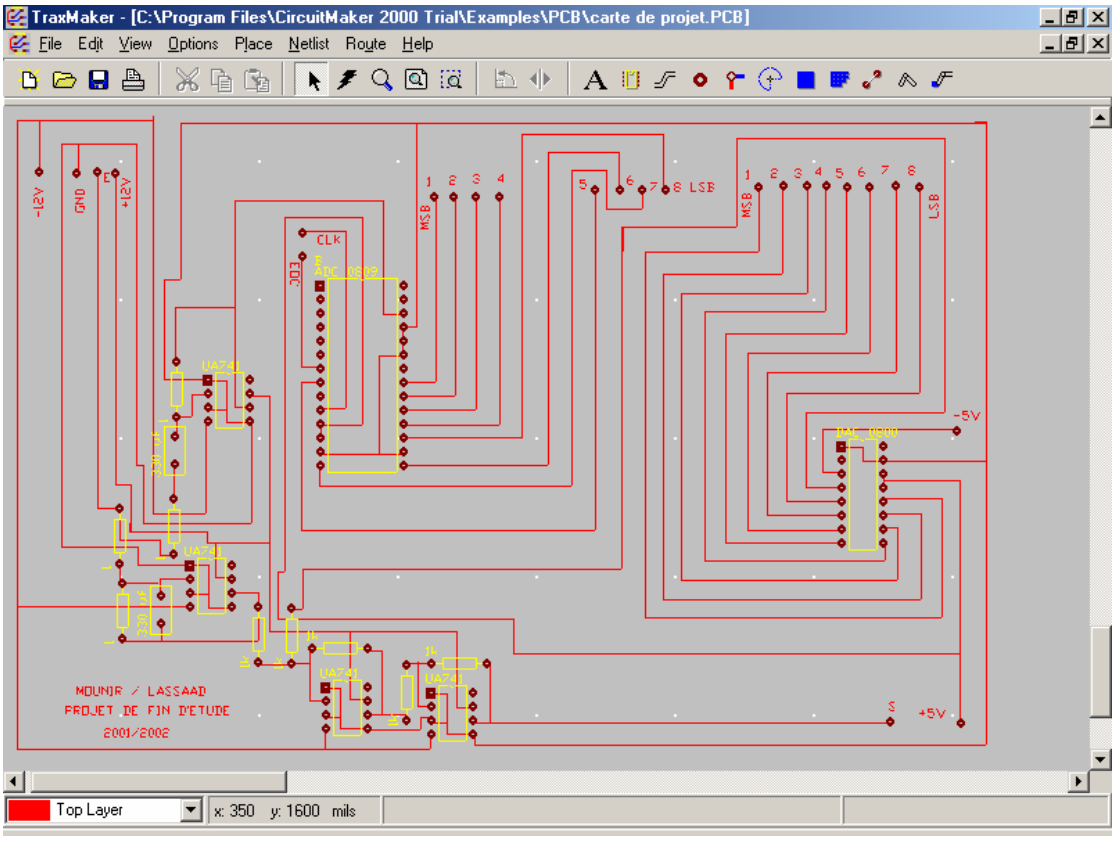


Fig.2.6 Schéma de routage

2-4 Conclusion

Dans cette partie on a procédé à réaliser la carte électronique de l'interface téléphonique. De même, des essais et des mesures permettant de vérifier le bon fonctionnement de la carte électronique ont été effectués.

PARTIE 3:
ETAGE FPGA

CHAPITRE 1 :

DESCRIPTION DE L'ALGORITHME D.E.S

1-1 Introduction

Le D.E.S. (Data Encryption Standard), c'est-à-dire Standard de Chiffrement de Données) est un standard mondial depuis plus de 15 ans. Bien qu'il soit un peu vieillissant, il résiste toujours très bien à la cryptanalyse et reste un algorithme très sûr.

Au début des années 70, le développement des communications entre ordinateurs a nécessité la mise en place d'un standard de chiffrement de données pour limiter la prolifération d'algorithmes différents ne pouvant pas communiquer entre eux. Pour résoudre ce problème, L'Agence Nationale de Sécurité Américaine (N.S.A.) a lancé des appels d'offres. La société I.B.M. a développé alors un algorithme nommé « Lucifer », relativement complexe et sophistiqué. Après quelques années de discussions et de modifications, cet algorithme, devenu alors D.E.S., fut adopté au niveau fédéral le 23 novembre 1976.

1-2 Le Cryptage Symétrique : Le D.E.S

1-2-1 Description

Le cryptage à clé symétrique utilise des clés de cryptage et de décryptage identique (figure 1.1).Les deux interlocuteurs doivent donc partager le secret de la clé commune. La mise en service d'une nouvelle clé suppose une communication secrète entre A et B. Pour assurer cette communication, il est donc nécessaire de crypter la nouvelle clé, évidemment sans utiliser l'ancienne. Le cryptage symétrique n'est efficace que s'il est complété par une méthode de communication des clés bien sécurisées.

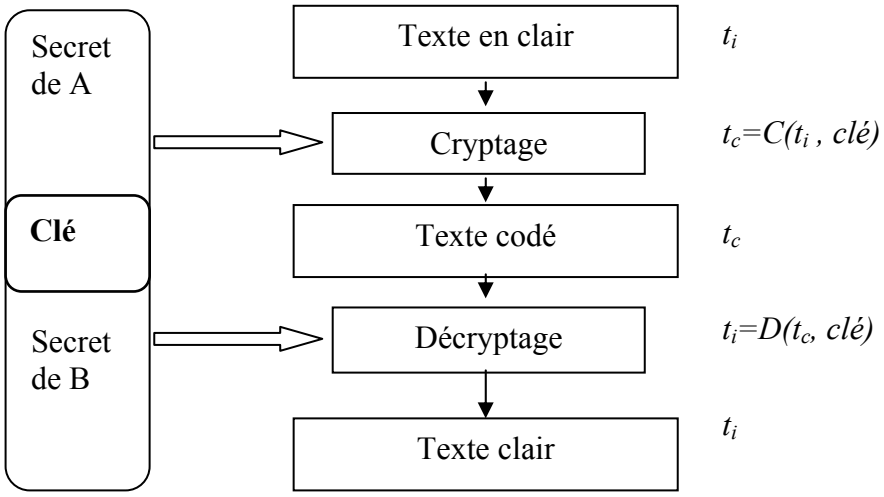


Fig.1.1 : Hiérarchie de fonctionnement de l'algorithme D.E.S

Les algorithmes de cryptage symétriques sont généralement fondés sur deux types d'opérations élémentaires : la transposition et la substitution. Pour illustrer d'une façon simplifiée ces deux opérations, prenons l'exemple du cryptage d'un mot français dans sa forme alphabétique. La transposition est un changement de l'ordre des caractères du mot, la substitution est un changement d'alphabet, obtenu par une transposition de l'alphabet lui-même.

Exemple : on applique une transposition du mot initial "CRYPTAGE", puis une substitution d'alphabet pour obtenir le cryptage final.

C R Y P T A G E
Y C T R E P G A

1 Transposition

A BC D E F G H I J K L M N O P Q R S T U V W X Y Z
KC D A L W R F N G Y V J P S X B O U Z M H I Q T E

2 Transposition

T R Z O L X D K

3 Cryptage final

Fig.1.2 : Transposition et substitution

La nature et l'ordre des opérations de transposition et de substitution sont déterminés par la clé. Elles sont évidemment effectuées sur le code binaire.

Le DES ("Data Encryption Standard") est le cryptage symétrique le plus connu. Il est constitué par une suite complexe d'opérations de type substitution ou transposition. Ce cryptage est très utilisé. Il est disponible sur la plupart des équipements. De nombreuses améliorations des algorithmes ont permis en outre de disposer de programmes, voir de composants qui le réalisent avec de bonnes performances. Cet algorithme a fait l'objet de nombreuses critiques, ne serait ce que parce que l'on a fait un standard, mais aussi pour sa fragilité devant une attaque "professionnelle" (la clé de 56 positions binaires est peut être insuffisante). Le DES n'est plus certifié par le gouvernement américain depuis 1988, mais il reste pour longtemps le standard de fait.

Le DES est un code à bloc de 64 bits. Le fichier clair est donc découpé en blocs de 64 bits qui sont traités les uns après les autres. Les blocs cryptés qui en ressort à la même taille que le bloc clair. Le codage repose ainsi sur une transformation de blocs de 8 octets de texte clair jusqu'à ce qu'il soit entièrement transformé en texte codé.

Cette transformation s'opère selon le principe suivant :

- Le bloc de texte clair (64 bits) subit d'abord une permutation initiale (IP).
- Puis on réitère 16 fois une certaine transformation. A chaque pas, on change les paramètres individuels (on utilise 16 clés partielles déduites de la clé de l'utilisateur).
- Enfin, on applique IP^{-1}, l'inverse de la permutation initiale.

On remarque que la clé privée utilisée pour crypter le message est également de longueur de 64 bits.

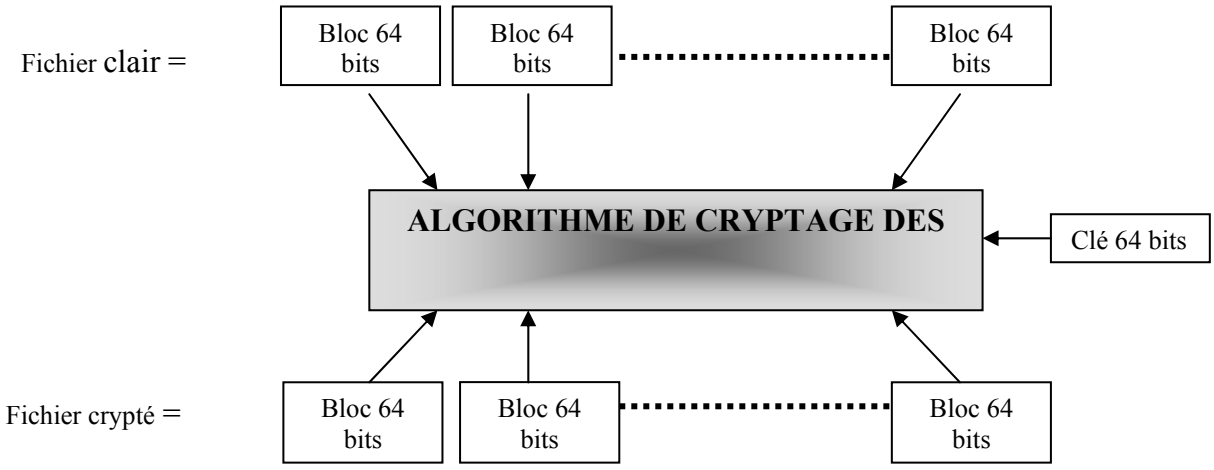


Fig1.3 : Synoptique de chiffrement en algorithme DES

Le DES est un algorithme auquel on donne en entrée : un bloc de texte clair ou chiffré de 64 bits (8 caractères) plus une clé de 64 bits +un offset (0 et 1) indiquant le mode chiffrement ou déchiffrement du bloc. Il en sort des blocs de 64 bits, qui représente le bloc d'entrée, soit chiffré en fonction de l'offset donné en entrée.

Le DES est donc un système de chiffrement par blocs de 64 bits, et à clé secrète de 64 bits.

1-2-2 Algorithme du DES

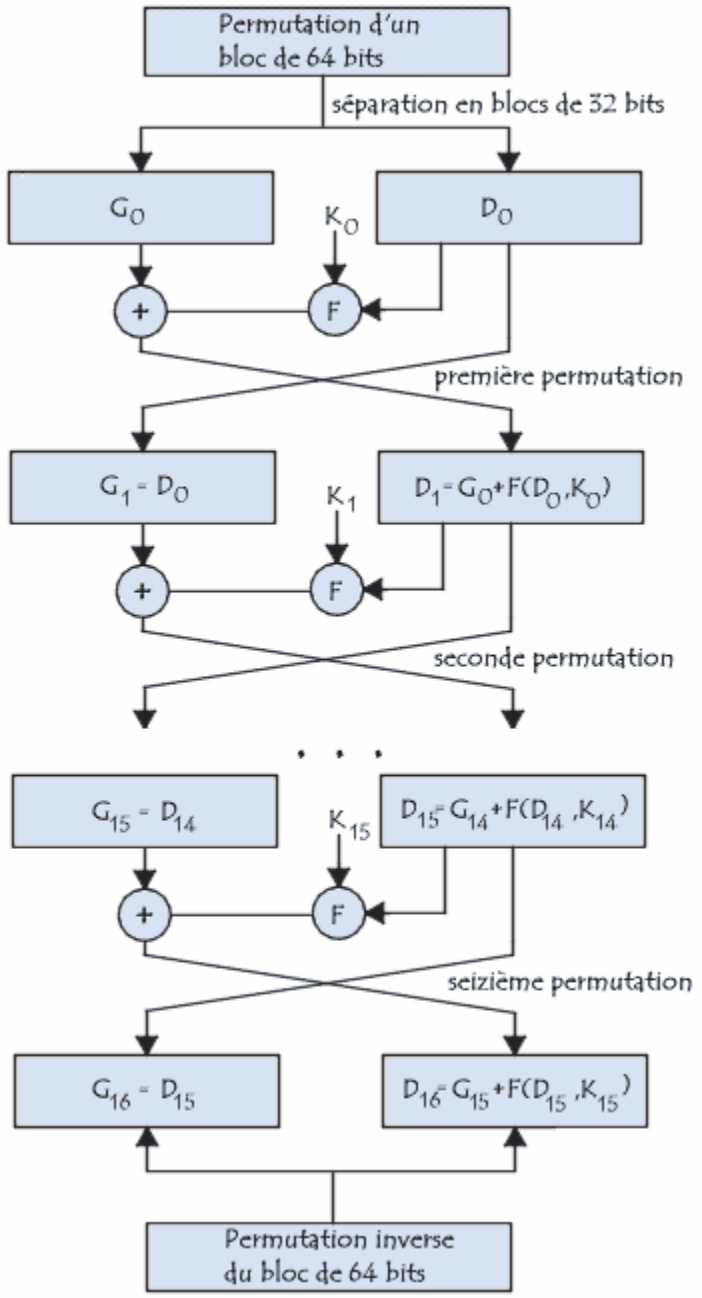


Fig.1.4 : Algorithme de chiffrement DES

1-2-3 Description des six étapes de l'algorithme

Le figure 1.5 représente les six étapes effectuer par un rang de l'algorithme DES

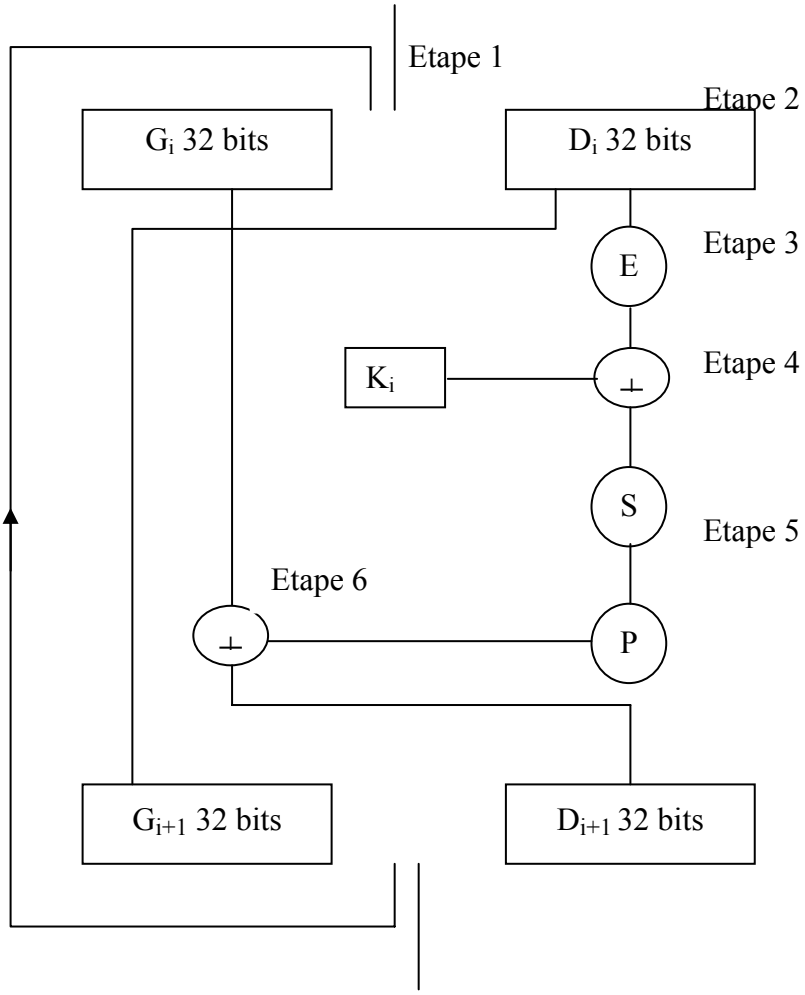


Fig.1.5 : Les opérations de cryptage au niveau d'un bloc

1-2-3-1 Première étape

chaque bloc de 64 bits de fichier clair subit une permutation IP_0, qui n'a lieu que lors de première itération, puis est scindée en deux blocs de 32 bits G_0 et D_0 :

$$(b_1, b_2 \ldots\ldots\ldots\ldots b_{64}) \longrightarrow B= (b_{58}, b_{50}, b_{42}, \ldots\ldots\ldots\ldots b_K, b_{K-8}, \ldots.) \longrightarrow (G_0, D_0)$$

1-2-3-2 Deuxième étape

Les 32 bits de D_0 entrent dans une table de sélection de bits E, où ils sont mélangés et répétés. On obtient 48 bits, soit 16 de plus que le sous-bloc initial D_0.

$D_0 \longrightarrow B' = (b_{32}, b_1, b_2, b_3, b_4, b_5, b_4, b_5, b_6, b_7, b_8, b_9, b_8, b_9, \ldots\ldots)$

1-2-3-3 Troisième étape

On calcule la clé K_1 à partir de la clé d'origine K. les 48 bits de B' sont transformés par ou-exclusif avec K_1 : $B' \oplus K_1$.

1-2-3-4 Quatrième étape

Le résultat de l'étape précédente est décomposé en 8 blocs D_{0i} de 6 bits chacun. Chaque bloc D_{0i} s'écrit en binaire (bit_1, bit_2, bit_3, bit_4, bit_5, bit_6). Cette décomposion permet de calculer une position dans une table de sélection S à 8 blocs de 16 colonnes et 4 lignes. Le nombre binaire (bit_1 bit_6) représente le numéro de ligne « x », et nombre binaire (bit_2 bit_3 bit_4 bit_6) le nombre de colonne « y ». Une fois la position (x,y) trouvée, on substitue au bloc D_{0i} le bloc de 4 bits déterminé par son adresse (x,y) dans la table. On obtient donc au total 32 bits.

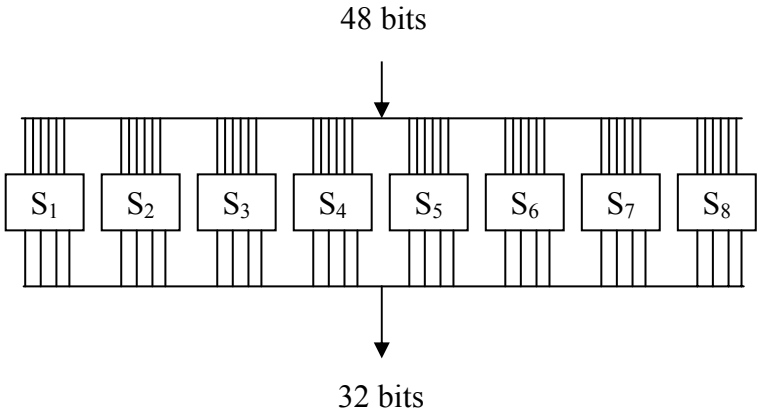


Fig.1.6 : L'étape de substitution

1-2-3-5 Cinquième étape

le résultat de l'étape 4 subit une nouvelle permutation P. les 32 bits précédents sont permutés de la manière suivante :

$(b_1, b_2 \ldots, b_{32}) \longrightarrow$ bits (16, 7, 20, 21, 29, 12, 28, 17, 1, 15, 23, 26, 5, 18, 31, 10, 2, 8, 24, 14, 2, 27, 3, 9, 19, 13, 30, 6, 22, 11, 4, 25).

1-2-3-6 Sixième étape

Le résultat de l'étape 5 est soumis à un XOR avec G_0 pour former D_1. Puis on pose $G_1 = D_0$. Ainsi s'achève la première itération.

Ensuite, on répète 14 fois la procédure décrite précédemment, de l'étape 2 à l'étape 6, on prenant comme clé K_i. Par contre, la seizième itération ne se termine pas tout à fait comme les précédentes : Les blocs de gauche et de droite étant permutés ainsi : $D_{16} = D_{15}$ et $G_{16} = G_{15} \oplus F(D_{15}, K_{15})$

Enfin, le résultat subit la permutation inverse IP^{-1}.

CHAPITRE 2 :

IMPLEMENTATION DE L'ALGORITHME DES SUR UNE CARTE FPGA

2-1 Introduction

Dans ce chapitre, nous allons décrire les différents modules de l'algorithme de cryptage DES. Cette description nous donne une idée claire sur le principe de fonctionnement des modules à implémenter ainsi qu'une vision proche et dirigée de notre implémentation sur un circuit FPGA.

A cet effet, nous intéresserons à donner les organigrammes d'implémentation de l'algorithme DES et la description de l'implémentation par des circuits logiques.

Enfin, nous allons évaluer la faisabilité de cette implémentation. Cette évaluation doit tenir compte de la disponibilité des circuits FPGA et la possibilité d'implémentation de l'algorithme DES.

2-2 Les organigrammes d'implémentation de l'algorithme de cryptage DES

Le fonctionnement de ce type de cryptage se fait d'une manière séquentielle. En effet, l'algorithme comprend essentiellement 16 étages qui se diffèrent par la clé obtenue à partir d'un générateur de clé.

On s'intéresse dans notre implémentation à deux éléments essentiels qui constituent la quasi-totalité de l'algorithme.

Ces deux éléments sont :

- Etapes de l'algorithme DES : élément de base de l'algorithme.
- Générateur de clé qui se charge de générer de 16 clés différentes qui seront utilisées pour les 16 étages.

2-2-1 Etapes de l'algorithme DES

La réalisation de cette opération consiste à implémenter en assemblant le dispositif indiqué par la figure 2.1.

.

La figure 2.1 représente le fonctionnement de l'étage ***i*** de l'algorithme DES ($1 \leq i \leq 16$). Pour cet étage, le bloc d'entrée est constitué de deux paquets de taille 32 bits chacun, ces deux paquets sont nommés $\mathbf{G_{(i-1)}}$ **et** $\mathbf{D_{(i-1)}}$ alors que le bloc comprend deux paquets

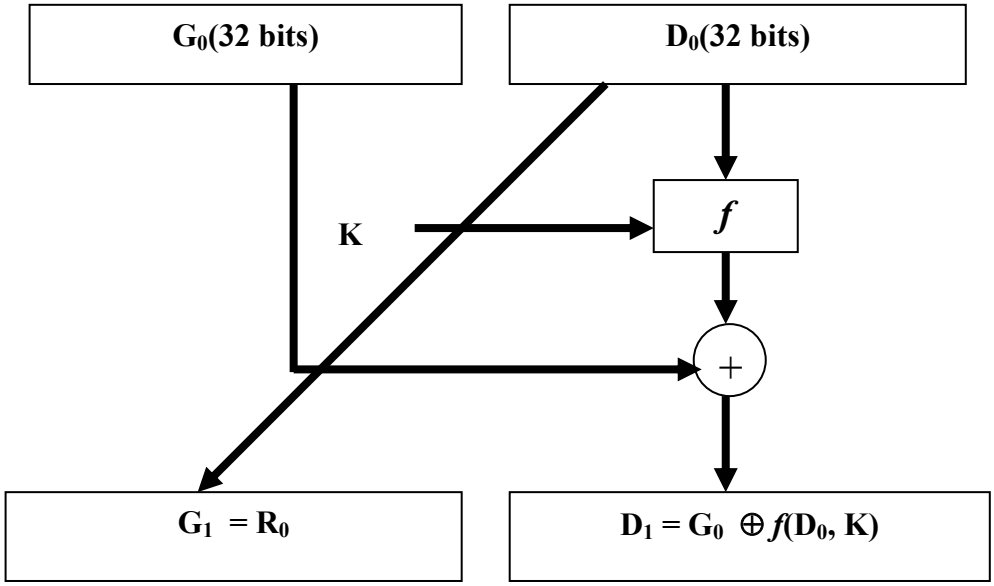


Fig.2.1 : Principe de réalisation d'un étage DES

De taille 32 bits nommés G et d ces deux derniers sont obtenus à partir de bloc d'entrées suivant les étapes intermédiaires suivantes :

2-2-1-1 L'expansion

L'opération d'expansion comme l'indique son nom consiste à ajouter des bits au paquet d'entré.

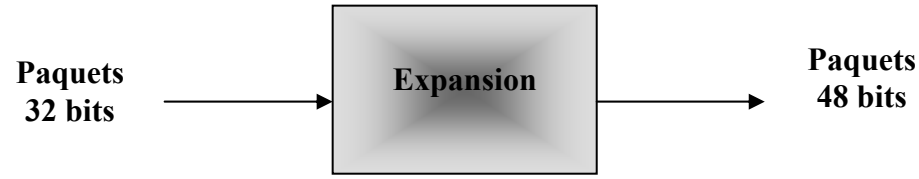


Fig.2.2: Étage d'expansion

Les bits du paquet d'entrées sont notés de bit 1, bit 2, bit 3, …,bit 32. Les organigrammes des bits du paquet après l'expansion obéissent à la règle indiquée par le tableau 2.1:

Par exemple si on a en entré :

D0 = 1101 1100 0001 1111 0001 0000 1111 0100

D C 1 F 1 0 F 4

32	**1**	**2**	**3**	**4**	**5**
4	**5**	**6**	**7**	**8**	**9**
8	**9**	**10**	**11**	**12**	**13**
12	**13**	**14**	**15**	**16**	**17**
16	**17**	**18**	**19**	**20**	**21**
20	**21**	**22**	**23**	**24**	**25**
24	**25**	**26**	**27**	**28**	**29**
28	**29**	**30**	**31**	**32**	**1**

Tab.2.1: configuration d'expansion

Le paquet résultat de l'expansion D0 est donné par :

E(D0) = 011011 111000 000011 111110 100010 100001 011110 101001

2-2-1-2 la substitution

Son rôle essentiel est d'obtenir 32 bits à partir d'un paquet d'entré de 48 bits. Elle apparaît donc comme opération inverse de l'expansion mais diffère de celle ci au niveau de principe même de l'opération (voir figure 2.3).

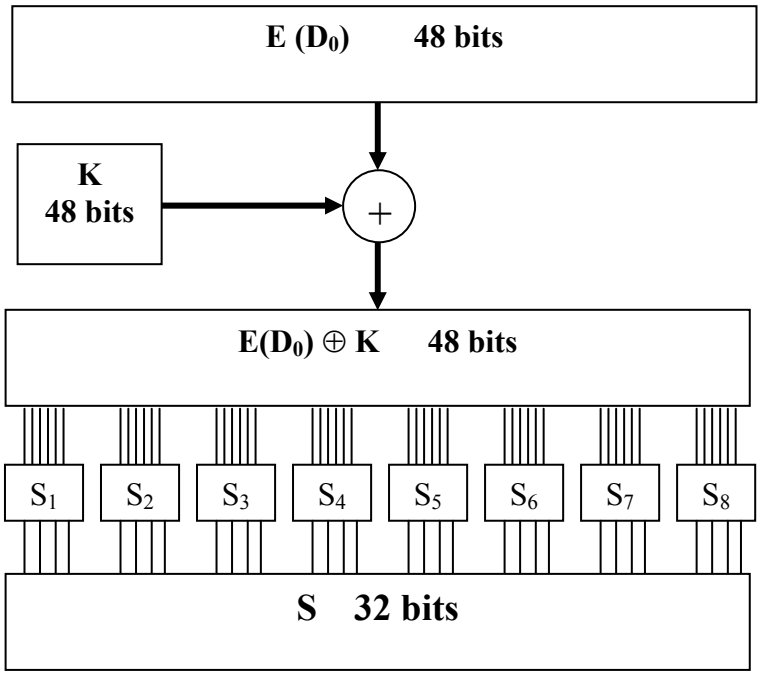


Fig.2.3 : Principe de substitution

Le bloc de 48 bits en entré est divisé en 8 mots de 6 bits. Chaque mot est envoyé dans une S-BOX, où il sert d'indice pour déterminer le mot de 4 bits qui va se substituer à lui.

A partir du mot de 6 bits en entré : D5 D4 D3 D2 D1 D0 on obtient le numéro de ligne « D5 D0 » et le numéro de colonne « D4 D3 D2 D1 ».

Le tableau 2.2 expose les configurations de substitution.

S1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Tab.2.2 : Configuration de substitution

L'opération S_i permet de donner 4 bits en sortis à partir de 6 bits en entrée sans perte de généralité, considérons la configuration S_i. Cette dernière est représenté par une matrice de 4 lignes et 16 colonnes et ne comprend que des valeurs décimales entre 0 et 15 (entre 0 et F en hexadécimal et entre 0000 et 1111 en binaire).

Le principe de cette opération est bien expliqué par l'exemple suivant :
Supposant qu'à l'entrée de S_1 on a 6 bits qui sont $a_0\ a_1\ a_2\ a_3\ a_4\ a_5$, à la sortie on prend la valeur sur 4 bits de la matrice de S_i cette valeur insertion de la ligne numéro ($a_0\ a_5$) et de la ligne ($a_1\ a_2\ a_3\ a_4$).

La matrice de S_1 est représenté par la matrice de substitution du tableau 2.3.

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
5	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Tab.2.3 : Tableau S1

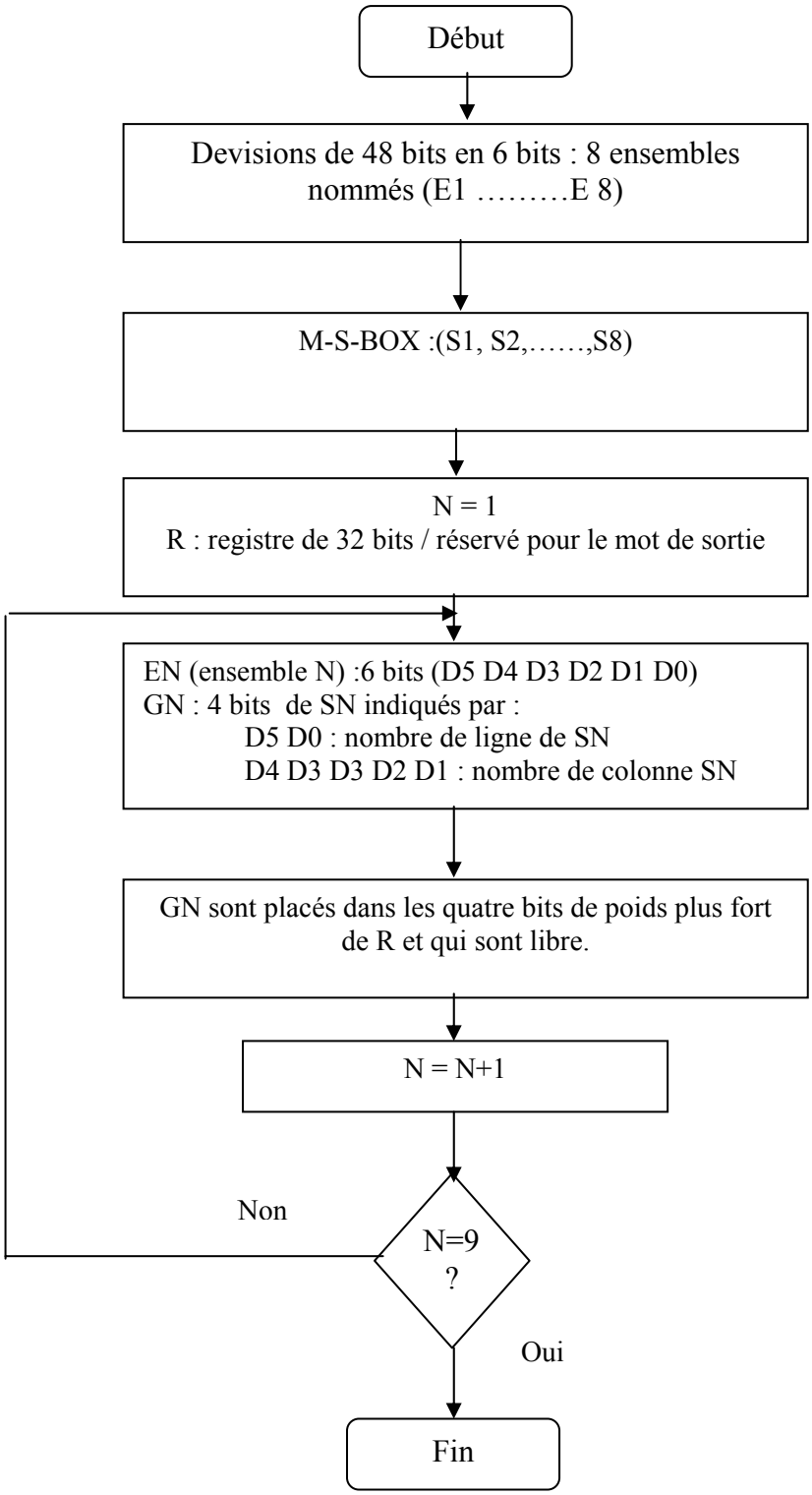


Fig.2.4 :Organigramme de substitution
(fonctionnement de S-BOX)

Remarque

- **S-BOX :** Un circuit qui assure l'étape de substitution.
- **M-S-BOX :** Mémoire de S-BOX contient l'ensemble de caractère de tableau 2.3.

2-2-1-3 Permutation

Cette opération est comme son nom l'indique consiste à permuter l'ordre des bits en entrées pour obtenir un nouvel ordre aux sorties. Elle manipule un paquet de taille 32 bits en entrée, ces bits sont nommés de 1 à 32. Après permutation l'ordre des bits est représenté par la règle indiqué par le tableau.2.4.

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Tab.2.4 : Paquet après permutation

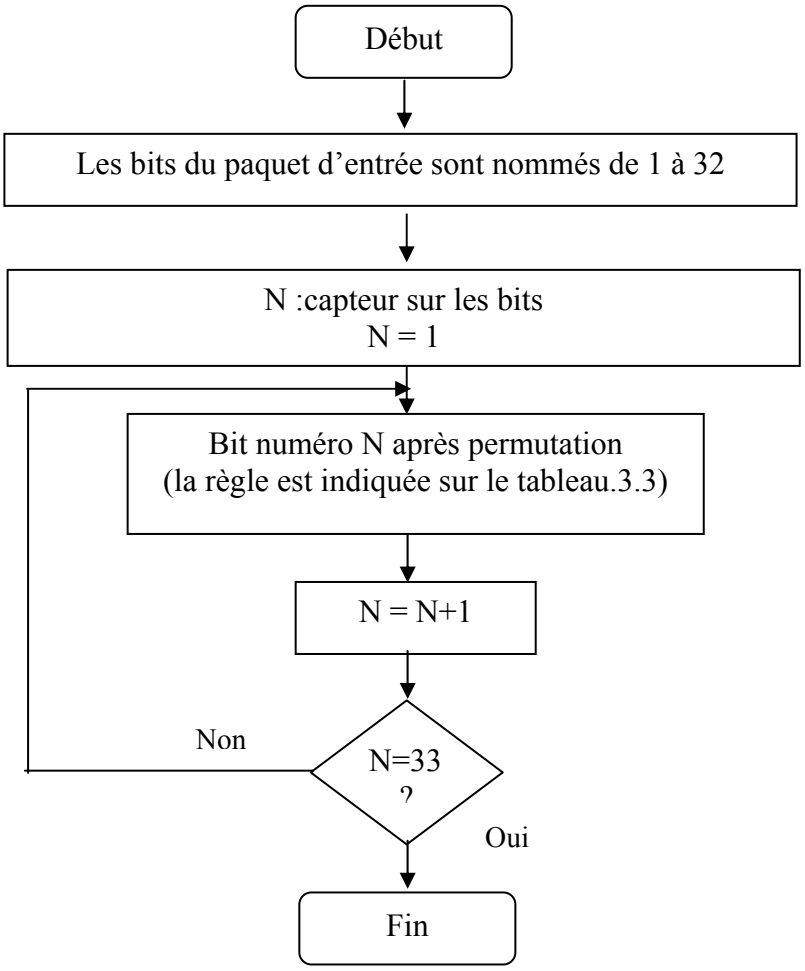


Fig.2.5 : Organigramme de permutation

2-2-2 Générateur des clés

On remarque d'après l'étude fait dans le paragraphe 2.2.1 que dans chaque étage on utilise une clé K*i* ($1 \leq Ki \leq 16$). Ces déférentes clés sont obtenues à partir d'un générateur de clé dont le principe est décrit par la figure2.6.

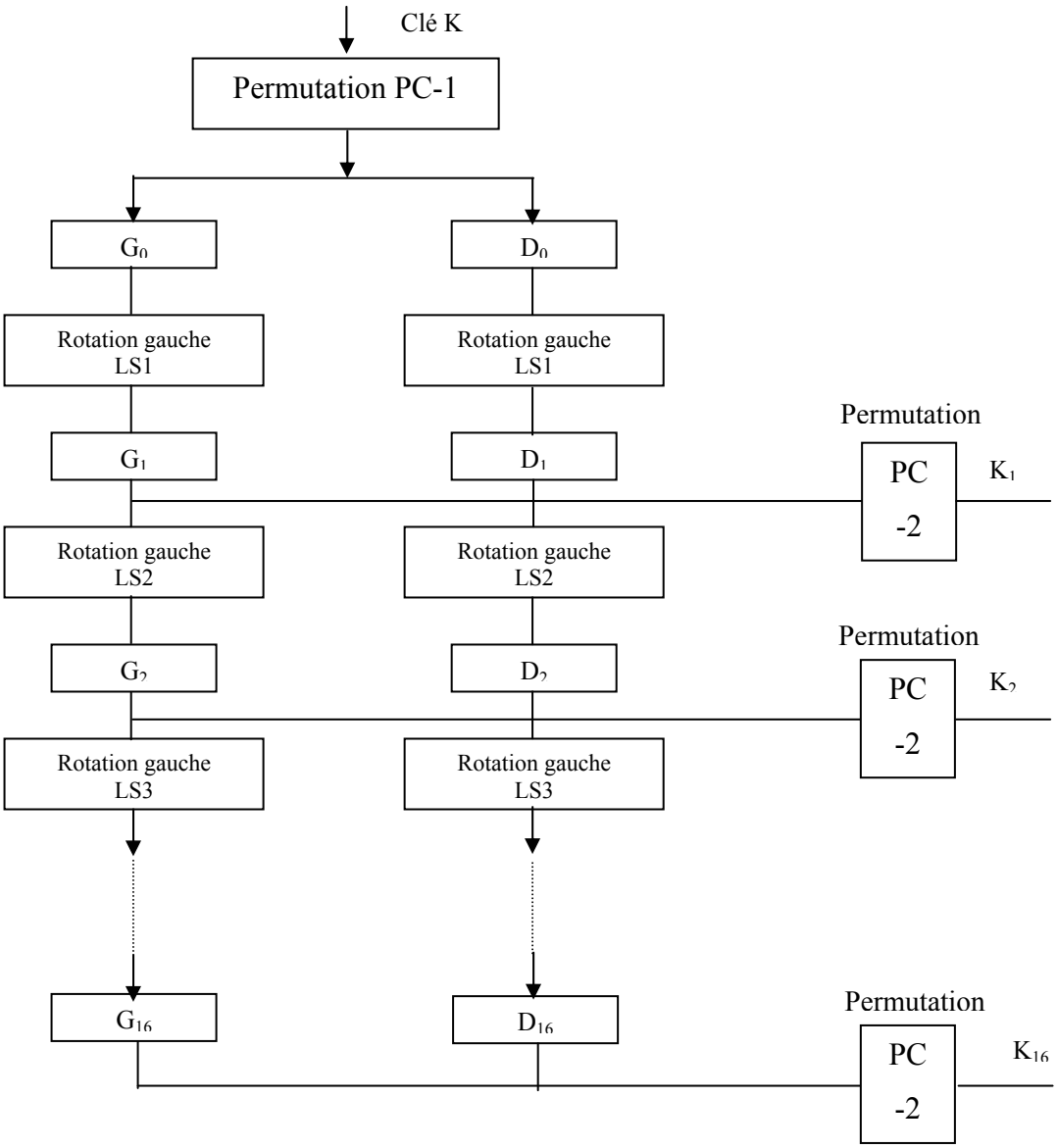


Fig.2.6 : Générateur des clés

D'après la figure 2.6, la génération de clé se fait d'une manière séquentielle. En effet, la génération des clés K_i est liée étroitement à la clé K_{i-1}. Cette suite récurrente est basée sur le terme initial K_i, ce dernier étant de taille 64 bits.

Pour déterminer une clé K_i, on réalise les opérations suivantes :

- Choix arbitraire d'une clé K_o de taille 64 bits.
- Calcule de deux paquets D_o et G_o de taille 28bits chacune. Ces deux paquets sont obtenus suite à une permutation PC – 1 dont la règle est représentée par le tableau 2.5.
- Génération des D_i et des G_i ($1 \leq K_i \leq 16$) : obtenus respectivement suite à une rotation gauche de D_{i-1} et de C_{i-1}.

57	49	41	43	45	17	9
1	58	50	42	47	29	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
5	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Tab.2.5 : Table de permutation PC-1

- Evaluation des K*i* se fait à partir de D*i* et de C*i* après l'opération PC-2 ce dernier est représenté par la règle indiqué par le tableau 2.6.

14	17	11	24	1	5
3	28	15	16	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Tab.2.6 : Table de permutation PC-2

Pour faciliter la compréhension de l'organigramme, on manipule les données suivant la notion suivante :

- K : Clé initiale de taille 64 bits.
- PC-1 : Permutation 1.
- D_i et G_i : Deux paquets de taille 28 bits chacun.
- RG : Rotation gauche.
- PC-2 : Permutation 2.

A partir de ces notions, l'organigramme de générateur de clé est illustré par la figure 2.7.

L'organigramme de DES est obtenu suite à une simple concaténation de deux modules : étage et générateur de clé. Il reste à noter que le module étage se répète 16 fois et chaque étage utilise une clé parmi les 16 clés générées.

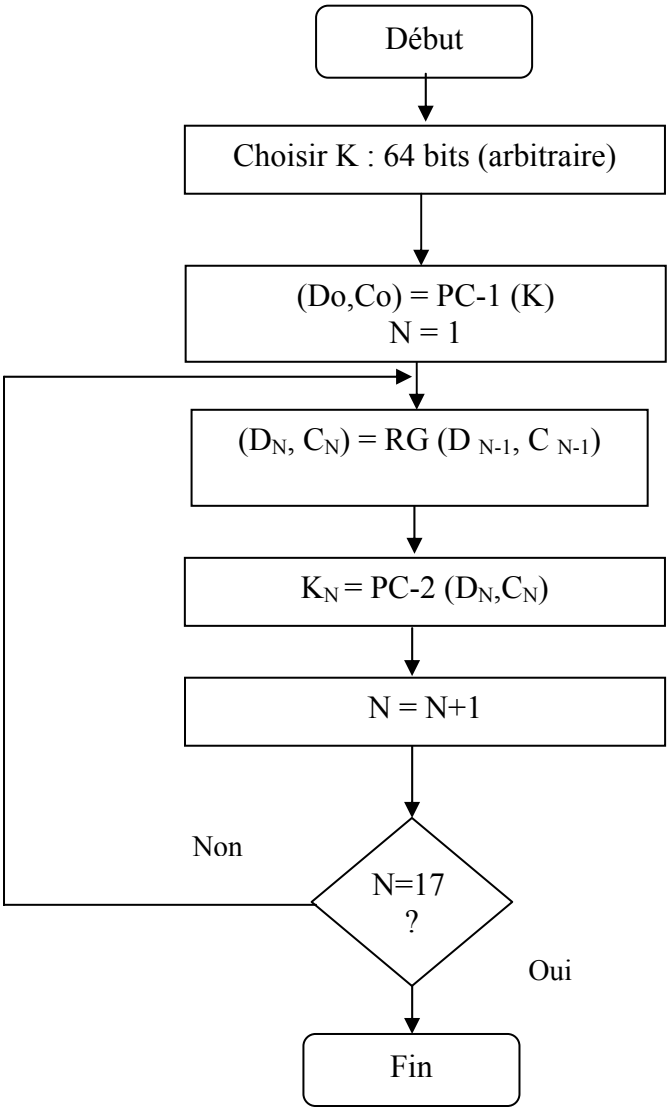


Fig.2.7 : Organigramme d'un générateur de clé

2-2-3 Organigramme de DES

La figure 2.8 représente l'organigramme complète de l'algorithme DES.

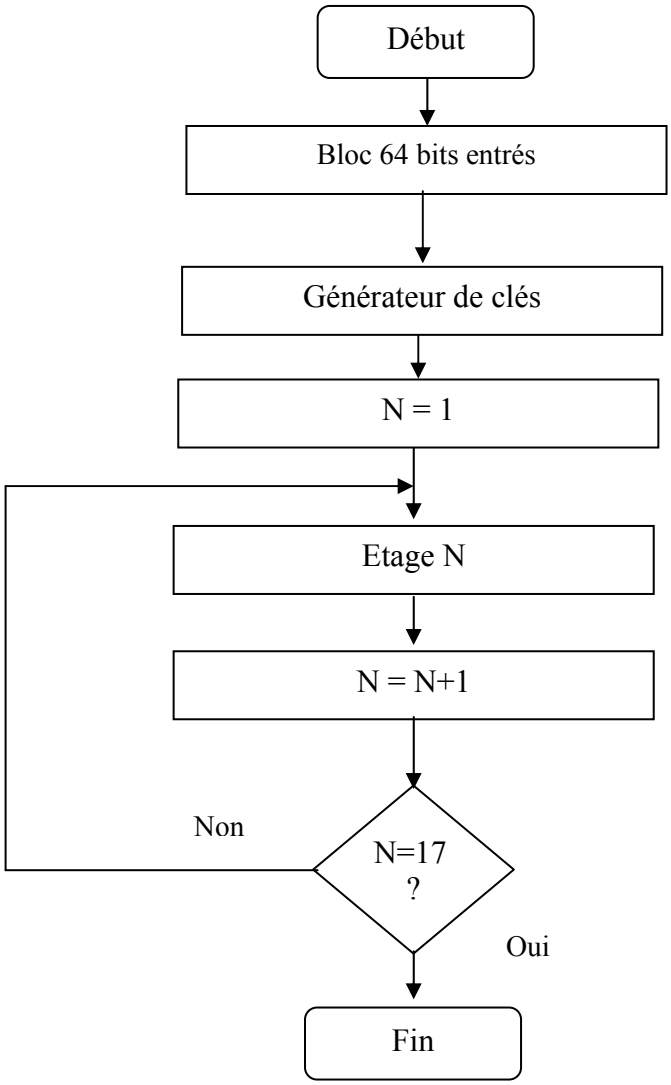


Fig.2.8 : Organigramme de l'algorithme DES

Remarque :

L'opération de décryptage est réalisée par le même dispositif que celui de cryptage sauf que l'ordre des clés K*i* ($1 \leq Ki \leq 16$) sera inversé. Par exemple dans l'étage 1 en utilise la clé K_{16}.

2-3 Description de l'implémentation par des circuits logiques

Après la conversion analogique numérique, le signal sortant va attaquer l'étage du circuit logique chargé de crypter notre signal. La broche EOC (End Of Conversion) relie les deux étages et génère une impulsion après chaque conversion, cette broche est branchée à un compteur qui contrôle le nombre de conversion nécessaire au démarrage du fonctionnement de l'algorithme.

La première impulsion de l'EOC indique que l'ADC a effectué une première conversion, le compteur commence le comptage des impulsions, et à travers ses sorties, donne une indication aux Demultiplexeurs (Demux) signalant le début de la conversation. Alors les Demux reçoivent les bits sortant de l'ADC de la manière suivante : Le premier Demux reçoit le premier bit (le bit de poids plus faible), le $2^{ième}$ reçoit le deuxième bit, …, le $8^{ième}$ reçoit le huitième bit (le bit de poids plus fort) comme l'indique la figure 2-9. Ce phénomène se répète huit fois de suite, jusqu'à ce que chaque Demux reçoit son huitième bit pour donner à sa sortie huit bits de telle façon que le premier Demux donne les huit bits de poids le plus faible, le deuxième les huit bits de poids qui suit,…et le huitième Demux donne les huit bits de poids plus fort. Le compteur est alors remis à zéro. Ce phénomène se répète jusqu'à la fin de la communication.

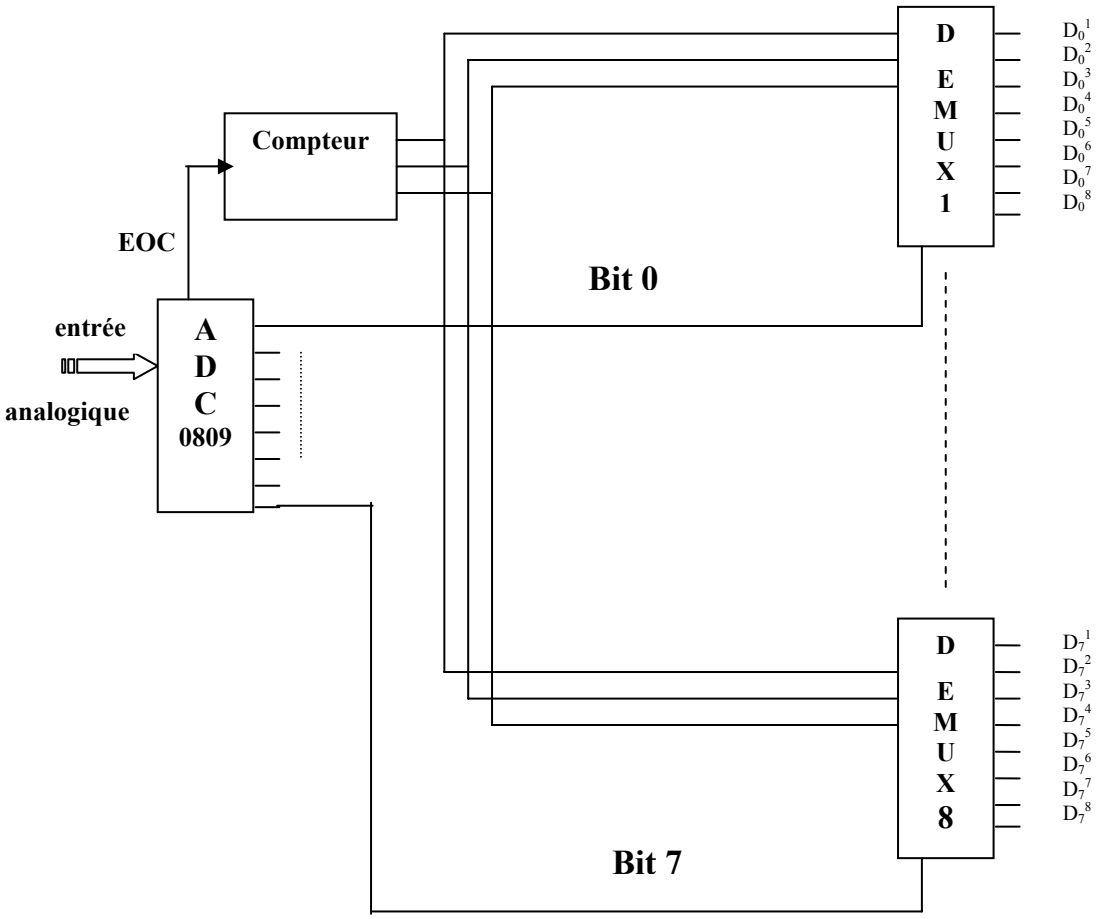


Fig.2.9: Passage de l'information entre l'interface et le circuit logique

Pour reformer les huit caractères (64 bits) d'entrée, on va rassembler les premiers bits de sortie de Demux ensemble, pour le premier caractère, les deuxièmes pour rassembler le deuxième caractère et ainsi de suite jusqu'au huitième caractère. Puis on va attaquer les étapes de l'algorithme DES :

Ce bloc va subir une permutation IP, cette permutation a été simplifiée pour faciliter l'implémentation. Elle consiste à faire une rotation de 32 bits de la manière suivante:

$$B = b_1b_2b_3\ldots\ldots\ldots\ldots..b_{31}b_{32}b_{33}\ldots\ldots\ldots\ldots\ldots\ldots\ldots b_{62}b_{63}b_{64}$$

$$B' = b_{33}b_{34}\ldots\ldots\ldots\ldots\ldots\ldots b_{63}b_{64}b_1b_2b_3\ldots\ldots\ldots\ldots..b_{31}b_{32}$$

Ce bloc permuté de 64 bits sera scindé en deux blocs de 32 bits : G_0 et D_0. Les 32 bits de D_0 vont subir une sélection qui consiste à obtenir un bloc de 48 bits à partir de D0 (voir paragraphe 1-2-3-2 de cette partie).

Les 48 bits obtenus seront transformés par Ou-Exclusif avec la clé qui se compose elle aussi de 48 bits. Les 48 bits obtenus à la sortie, seront décomposés en 8 blocs de 6 bits chacun pour attaquer un S-BOX qui nous donnera à sa sortie 32 bits sous forme de 8 blocs de 4 bits chacun.

Le S-BOX fonctionne suivant les règles indiquées au paragraphe 1-2-3-4.

Le bloc de 32 bits obtenu à la sortie de S-BOX sera transformé par Ou-Exclusif avec les 32 bits du bloc G_0 pour donner en sortie le bloc D_1 avec $D_1 = G_0 \oplus F(D_0, K_0)$. Cependant G_1 reçoit le bloc D_0 sans aucune modification. Le bloc de sortie de cette itération sera $B'' = G_1 D_0$ (on juxtapose G_1 et D_1).

2-4 Application sur un circuit FPGA

2-4-1 Définition d'un FPGA

Les FPGA (Field Programmable Gate Array) sont des composants VLSI entièrement configurables et programmables à volonté ce qui permet d'accélérer notablement certaines phases de calculs. L'avantage de ce genre de circuit est sa grande souplesse qui permet de les réutiliser à volonté dans des algorithmes différents en un temps très court (quelques millisecondes). Le progrès de ces technologies permet d'avoir des composantes toujours plus rapides et à plus haute intégration, favorisant la programmation des applications importantes.

2-4-2 Implémentation du DES sur FPGA :

D'après la description introduite dans le paragraphe 2-3, on remarque que l'implémentation de l'algorithme DES sur un circuit FPGA dépasse le nombre de CLB (Configurable Logic Blocks) d'un circuit FPGA XC 4003 EPC 84 dont nous disposons au laboratoire et comme solution, nous sommes amenés à proposer une version simplifiée qui se limite à une seule itération et qui utilise au départ des données de taille 8 bits.

2-4-2-1 Version simplifiée de DES

Nous allons considérer à l'entrée un bloc de 8 bits et nous allons appliquer le même principe de DES. Ces 8 bits vont d'abord suivre une permutation selon une rotation de 4 bits

$$(b_0b_1b_2b_3b_4b_5b_6b_7 \longrightarrow b_4b_5b_6b_7\, b_0b_1b_2b_3)$$

Ce bloc va être scindé en deux sous blocs de 4 bits chacun : G_0 ($b_4b_5b_6b_7$) et D_0 ($b_0b_1b_2b_3$). Ces derniers vont subir une sélection de bits, où ils sont mélangés et répétés de la manière suivante :

Avant la sélection : $b_0b_1b_2b_3$

Après la sélection : $b_3b_0b_1b_2b_3b_0$

Ces bits seront transformé par un Ou-Exclusif bit à bit avec la clé K, qui se compose de 6 bits (k_0 k_1 k_2 k_3 k_4 k_5). Les 6 bits de sortie (a_0 a_1 a_2 a_3 a_4 a_5) vont permettre de calculer une position dans une table de sélection S de 16 colonnes et de 4 lignes. Le nombre binaire a_0 a_5 donne le numéro de la ligne « x » et le nombre binaire a_1 a_2 a_3 a_4 donne le numéro de la colonne « y ». Une fois la position (x, y) trouvée, on substitut à la sortie le bloc de 4 bits déterminé par son adresse (x, y) dans la table.

Pour pouvoir réaliser cette tache, on a crée un circuit qu'on a appelé TS-BOX qui effectue toutes les tâches décrites. Ce circuit est programmé en utilisant le langage VHDL (Very high speed integrated circuits Hardware Description Langage) qui est un langage puissant permettant l'écriture succincte de code décrivant des circuits logiques complexes. (Voir annexe 3)

Les 4 bits de sortie de TS-BOX sont soumis à un XOR avec G_0 pour former D_1, et G_1 reçoit le bloc D_0. Ainsi, s'achève le cryptage et on obtient à la sortie le bloc $C = G_1\, D_1$ (on juxtapose G_1 et D_1).

2-4-2-2 Schéma de la version simplifiée

Le schéma de circuit logique qu'on a implémenté sur un circuit FPGA XC 4003 CPL (Voir annexe 4) est donnée par la figure 2.10 :

Fig.2.10 : Schéma de circuit logique simplifié

CONCLUSION GENERALE

Dans le cadre de notre projet de fin d'études, nous avons réalisé une interface téléphonique qui permet la protection du signal de parole par l'algorithme de cryptage DES

Sur le premier plan, c'est à dire, les généralités, on a abordé plusieurs notion. En premier lieu, on a étudié la signalisation téléphonique de point de vue caractéristique électrique et en deuxième lieu la cryptographe en générale, les cryptosystéme à clé secrète et à clé publique.

Sur le deuxième plan, qui s'occupe de l'interface téléphonique, on a fait une étude sur le filtrage pour séparer la signalisation et l'information, la conversation analogique / numérique et numérique / analogique ainsi que la sommation des deux signaux de signalisation et de signal de parole crypté

Sur le troisième plan, on a fait une étude approfondie sur l'algorithme DES et les étapes de l'implémentation sur un circuit FPGA.

Enfin, nous pouvons dire que ce travail n'est qu'une simple participation de notre part dans le domaine de sécurité sur le RTCP, et nous souhaitons bien que ce projet soit repris et amélioré par d'autres étudiants vu que ce domaine est toujours en perpétuel développement.

BIBLIOGRAPHIE

Document bibliothèque :

- **Mémoires de fin d'étude:**
  - **Tltre :** Développement de modules d'intégration de tokens dans une plate forme PKI.
    Réalisé par : GANMY Faycel & TOUJANI Mehrez
- **Livres :**
  - **Titre :** Compression et cryptage des données multimédias (2eme édition revue et augmentée) « XAVIER Marsault ».
    Auteur : XAVIER Marsault
  - **Titre :** Les télécommunications francaise « 1982 ».
    Réalisé sous la direction de : MARCEL Lacont.
    Assisté de : DANIEL Codé.
  - **Titre :** Memotech électronique (composants)
    Auteurs : J.C. CHOUVEAU.
    G. CHIVALIER.
    B. CHIVALIER
  - **Titre :** Initiation à la cryptographie
    Auteur : GILLE Dubertret
    Edition : vibert 1998 Paris

Sites Internet :

- http:/www.swiss.ai.mit.e.di/bal/pks-toplev.html
- http:/www.Forum.securiteinfo.com
- http://www.guetali.fr/home/creole/cours/Conversion%20de%20donn%C3%A9es%20(CNA).doc.

ANNEXES