

RAPPORT DU MINI PROJET

Implémentation de l'algorithme DES
sous FPGA



Réalisé par:

SOUAD CHKAIRI

Demandé par :

Mr. ELMOUMNI SOUFIANE

Table des matières :

Introduction	
Liste Des Figures.....	- 2 -
1- Définition de la cryptographie	- 4 -
2- Utilisations de la cryptographie	- 4 -
2-1 Les cartes bancaires	- 4 -
2-2 Les navigateurs Web	- 5 -
3- Algorithmes de Cryptographie DES (Data Encryption Standard)	- 5 -
3-1 Principe du DES	- 5 -
3-2 L'algorithme du DES	- 6-
4- Programmation VHDL	- 13-

Conclusion

Listes des figures

Figure 1: Cryptage et décryptage	- 3 -
Figure 2 : Cryptage et cartes bancaires	- 4 -
Figure 3: Les navigateurs web	- 5 -
Figure 4: Principe de DES	- 6 -
Figure 5 : schéma résumant les différentes parties de l'algorithme	- 12 -
Figure 6: RTL schematic	- 13 -
Figure 7: Aperçue du circuit DES	- 13 -

INTRODUCTION

La cryptographie, ou **l'art de chiffrer**, coder les messages, est devenue aujourd'hui une science à part entière. Au croisement des **mathématiques**, de **l'informatique**, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses...

La cryptographie étant un sujet très vaste, ce document se focalise essentiellement sur les méthodes de chiffrement dites modernes, c'est-à-dire celles étant apparues et utilisées après la Seconde Guerre mondiale. On passera en revue la saga du **DES** et de l'**AES**, en passant par le fameux **RSA**, le protocole le plus utilisé de nos jours. Ayant longtemps été l'apanage des militaires et des sociétés possédant de gros moyens financiers, la cryptographie s'est au fil du temps ouverte au grand public, et est donc un sujet digne d'intérêt. Toutes les méthodes de cryptographie seront présentées dans leur ordre chronologique d'apparition.

Notez cependant que ce document ne s'intitule pas cryptologie ! L'amalgame est souvent fait entre cryptographie et cryptologie, mais la différence existe bel et bien. La cryptologie est la "science du secret", et regroupe **deux branches** : d'une part, la **cryptographie**, qui permet de **coder les messages**, et d'autre part, la **cryptanalyse**, qui permet de les **décoder**.

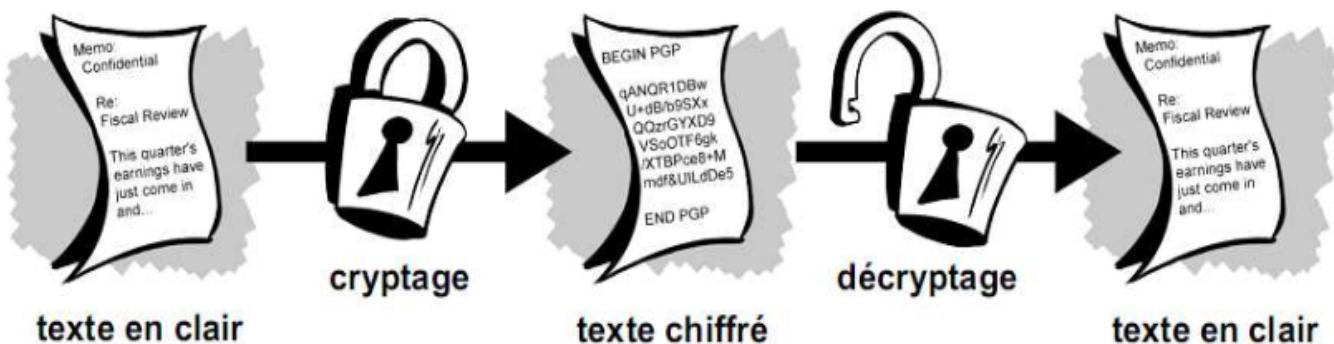


Figure 1: Cryptage et décryptage

1- Définition de la cryptographie:

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

Alors que la cryptographie consiste à sécuriser les données, la cryptanalyse est l'étude des informations cryptées, afin d'en découvrir le secret. La cryptanalyse classique 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.

2- Utilisations de la cryptographie

2-1 Les cartes bancaires

Les banques font partie des premiers utilisateurs de systèmes cryptographiques. Les cartes bancaires possèdent trois niveaux de sécurité :

- **Le code confidentiel** : c'est la suite de chiffres à mémoriser et à saisir à l'abri des regards indiscrets.
- **La signature RSA** : permet de vérifier l'identité de la carte sans avoir besoin de secrets; en d'autres termes, cette vérification peut se faire sans connexion à un centre distant.
- **L'authentification DES** : apporté une preuve de légitimité de la carte, et se fait par connexion à un centre distant.



Figure 2 : Cryptage et cartes bancaires

2-2 Les navigateurs Web:

Les navigateurs, ou browsers, tels que Mozilla Firefox ou Internet Explorer, utilisent le protocole de sécurité SSL (Secure Sockets Layers), qui repose sur un procédé de cryptographie par clé publique : le RSA.



Figure 3: Les navigateurs web

3- Algorithmes de Cryptographie DES (Data Encryption Standard)

3-1 Principe du DES

Le Data Encryption Standard (DES) est un algorithme de cryptographie qui a été sélectionné comme un standard pour la Federal Information Processing Standard (FIPS) pour les États-Unis en 1976, mais qui a connu un succès international par la suite.

Il s'agit d'un système de chiffrement symétrique par blocs de 64 bits, dont 8 bits (un octet) servent de test de parité (pour vérifier l'intégrité de la clé). Chaque bit de parité de la clé (1 tous les 8 bits) sert à tester un des octets de la clé par parité impaire, c'est-à-dire que chacun des bits de parité est ajusté de façon à avoir un nombre impair de '1' dans l'octet à qui il appartient. La clé possède donc une longueur « utile » de 56 bits, ce qui signifie que seuls 56 bits servent réellement dans l'algorithme. L'algorithme consiste à effectuer des combinaisons, des substitutions et des permutations entre le texte à chiffrer et la clé, en faisant en sorte que les opérations puissent se faire dans les deux sens (pour le déchiffrement). La combinaison entre substitutions et permutations est appelée **code produit**.

La clé est codée sur 64 bits et formée de 16 blocs de 4 bits, généralement notés k1 à k16. Etant donné que « seuls » 56 bits servent effectivement à chiffrer, il peut exister 256 (soit 7.2×10^{16}) clés différentes !

3-2 L'algorithme du DES

Les grandes lignes de l'algorithme sont les suivantes :

- Fractionnement du texte en blocs de 64 bits (8 octets) ;
- Permutation initiale des blocs ;
- Découpage des blocs en deux parties: gauche et droite, nommées G et D ;
- Étapes de permutation et de substitution répétées 16 fois (appelées rondes) ;
- Recollement des parties gauche et droite puis permutation initiale inverse.

Mécanisme :

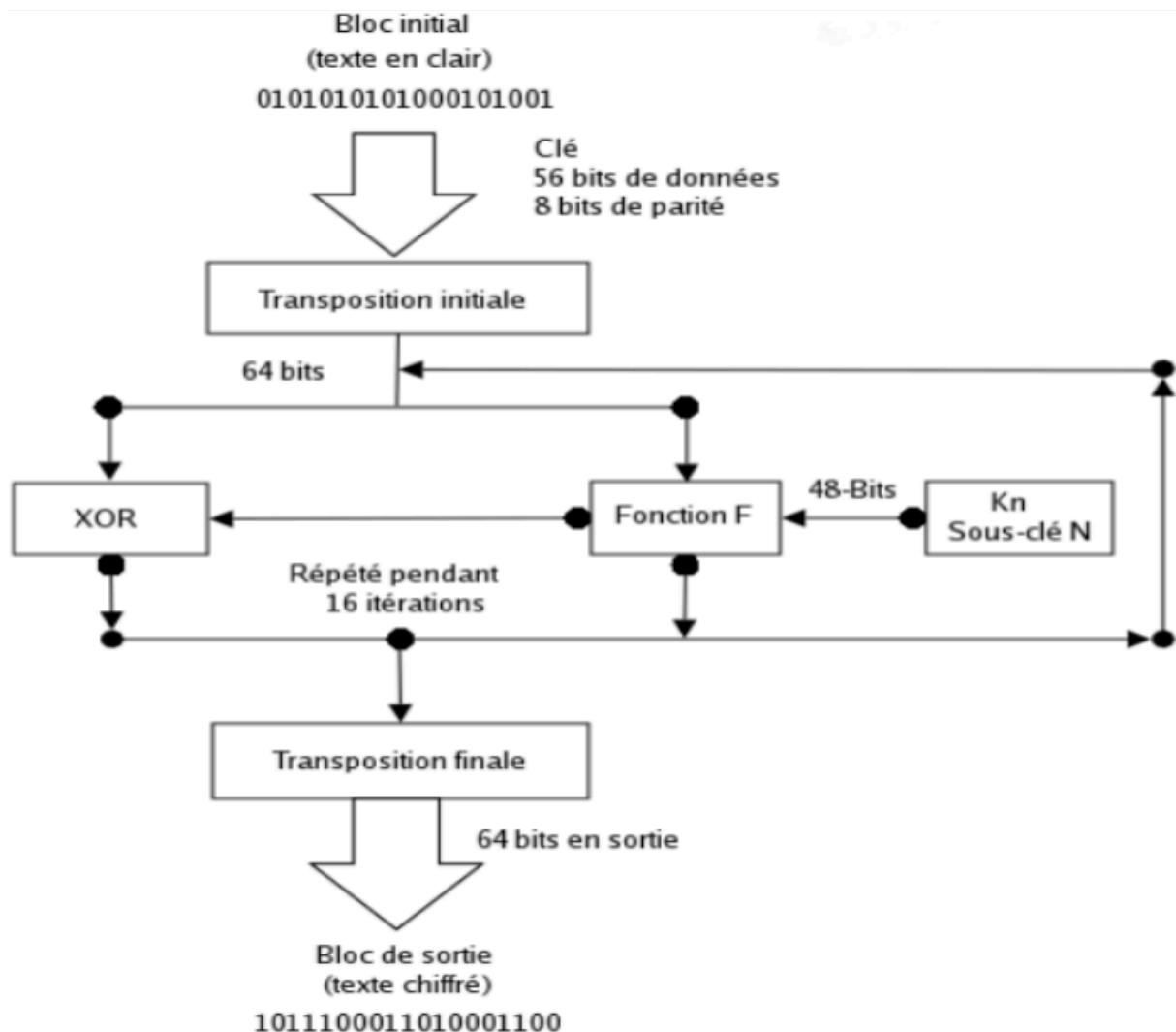


Figure 4: Principe de DES

A. Fractionnement du texte en blocs de 64 bits (8 octets)

Dans un premier temps le message en clair est découpé en blocs 64 bits.

B. Transposition initiale

Chaque bit d'un bloc subit une permutation selon l'arrangement du tableau ci-contre c'est-à-dire que le 58ème bit du bloc se retrouve en 1ère position, 50ème en seconde position, etc...

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

C. Scindement en bloc de 32 bits:

Le bloc de 64 bits est scindé en deux blocs de 32 bits notés G et D. On notera G₀ et D₀ l'état initial de ces deux blocs.

G ₀	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8

D ₀	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5

On remarque que G₀ contient tous les bits pairs du message initial et D₀ tous les bits impairs.

D. Rondes:

Les blocs Gi et Di sont soumis à un ensemble de transformations appelées rondes. Une ronde est elle-même composée de plusieurs étapes :

➤ Fonction d'expansion :

Les 32 bits du bloc D0 sont étendus à 48 bits grâce à une table d'expansion dans laquelle 32 bits sont mélangés et 16 d'entre eux sont dupliqués.

Ainsi, le 32ème bit devient le premier, le premier devient le second... Les bits 1,4,5,8,9,12,13,16,17,22,21,24,25,28,29 et 32 sont dupliqués et disséminés pour former un bloc de 48 bits que l'on nommera D'0 .

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

➤ OU exclusif (XOR) avec la clef :

DES procède ensuite à un OU exclusif entre D'0 et la première clef k1 générée à partir de la clef K (que doivent se partager émetteur et destinataire) par l'algorithme de cadencement des clefs que nous décrirons plus bas. Nous appellerons D"0 le résultat de cette opération.

➤ Boîtes de substitution :

D"0 est découpée ensuite en 8 blocs de 6 bits, noté D"0i. Chacun de ces blocs passe par des boîtes de substitution(S-boxes), notées généralement Si. Les premier et dernier bits de chaque D0i déterminent la ligne de la fonction de substitution, les autres bits déterminent la colonne. Grâce à cela la fonction de substitution « choisit » une valeur codée sur 4 bits (de 0 à 15). Voici la première boîte de substitution :

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

Soit D0i égal à 010101 , les premiers et derniers bits donnent 01, c'est-à-dire 1 en binaire. Les bits autres bits donnent 1010, soit 10 en binaire. Le résultat de la fonction de substitution est donc la valeur située à la ligne n°1, dans la colonne n°10. Il s'agit de la valeur 6, soit 0110 en binaire.

Chacun des 8 blocs de 6 bits est passé dans la boîte de substitution correspondante. Voici les autres S-Boxes :

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

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

On obtient donc en sortie 8 blocs de 4 bits. Ces bits sont regroupés pour former un bloc de 32 bits.

➤ Permutation :

Le bloc de 32 bits subit une permutation dont voici la table :

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

➤ OU exclusif :

Le bloc de 32 bits ainsi obtenu est soumis à un OU exclusif avec le G0 de départ pour donner D1 et le D0 initial donne G1.

L'ensemble de ces étapes est itérée seize fois.

E. Transposition initiale inverse:

Au bout des seize itérations, les deux blocs G16 et D16 sont « recollés » pour reformer un seul bloc de 64 bits puis subit-la transposition initiale inverse selon l'arrangement du tableau ci contre. On obtient alors le bloc initial chiffré.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

F. Reconstruction du message chiffré:

Tous les blocs sont collés bout à bout pour obtenir le message chiffré.

G. Algorithme de cadencement des clefs:

Nous allons décrire l'algorithme qui permet de générer à partir d'une clef de 64 bits, 8 clefs diversifiées de 48 bits chacune servant dans l'algorithme du DES.

De prime abord les clefs de parité sont éliminées pour obtenir une clef de 56 bits. Ce bloc subit une permutation puis est découpée en deux pour obtenir 2 blocs de 28 bits décrits par les matrices ci-dessous :

40	8	48	16	56	24	64
39	7	47	15	55	23	63
38	6	46	14	54	22	62
37	5	45	13	53	21	61

40	8	48	16	56	24	64
39	7	47	15	55	23	63
38	6	46	14	54	22	62
37	5	45	13	53	21	61

Ces deux blocs subissent une rotation à gauche, c'est-à-dire que les bits en seconde position prennent la première position, ceux en troisième position la seconde, celle en première position la dernière...

Les 2 blocs sont regroupés pour faire un bloc de 56 bits qui passe par une permutation fournissant un bloc de 48 bits représentant la clef k_i :

14	17	11	24	1	5	3	28	15	6	21	10
13	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	57	45
44	49	39	56	34	53	46	42	50	36	29	32

Des itérations de l'algorithme permettent de donner les 16 clefs utilisées dans l'algorithme du DES.

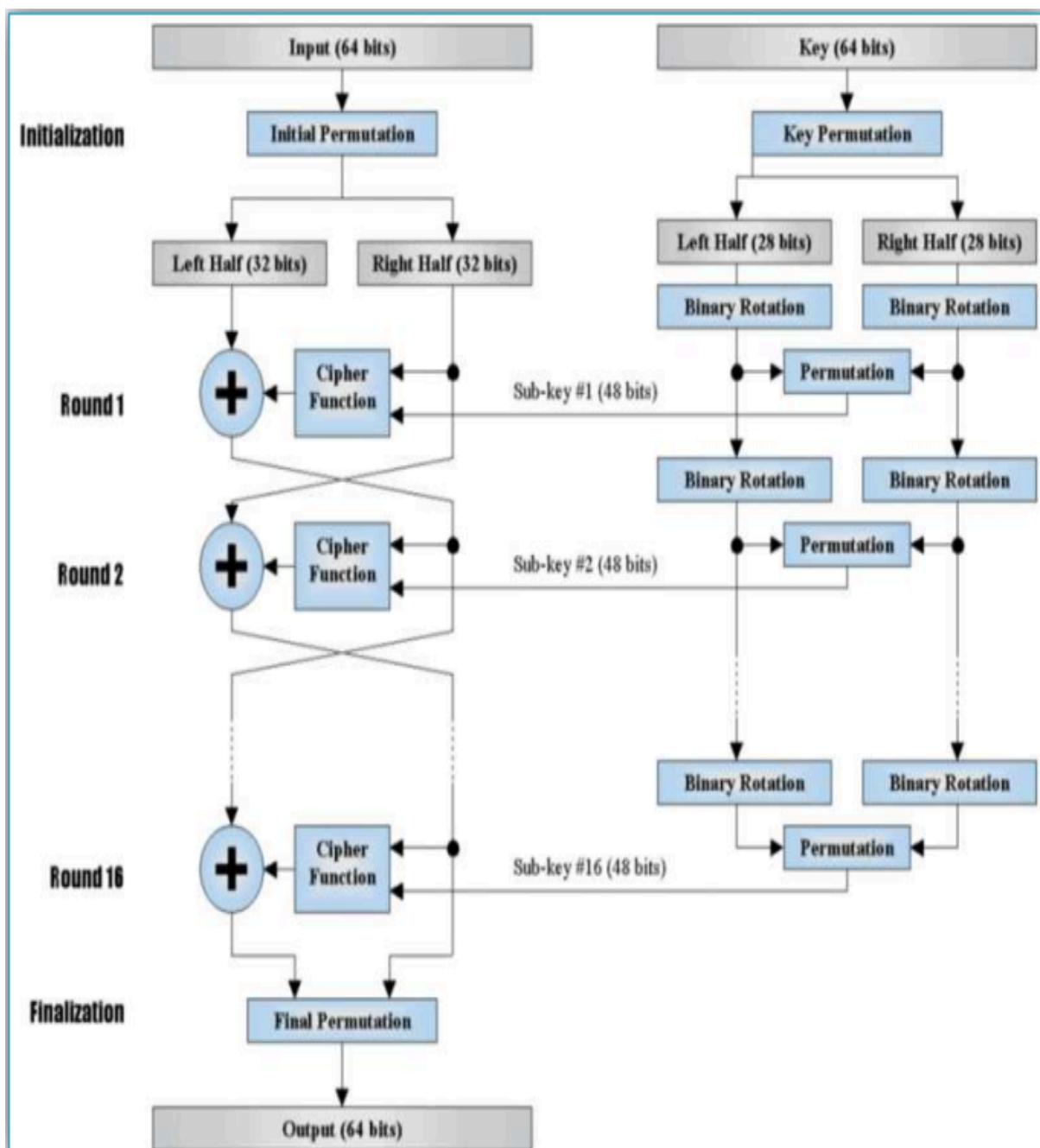


Figure 5 : schéma résumant les différentes parties de l'algorithme

4- Programmation VHDL:

Source VHDL (voir, l'annexe ou le programme sous Xilinx ISE)

➤ Schéma RTL:

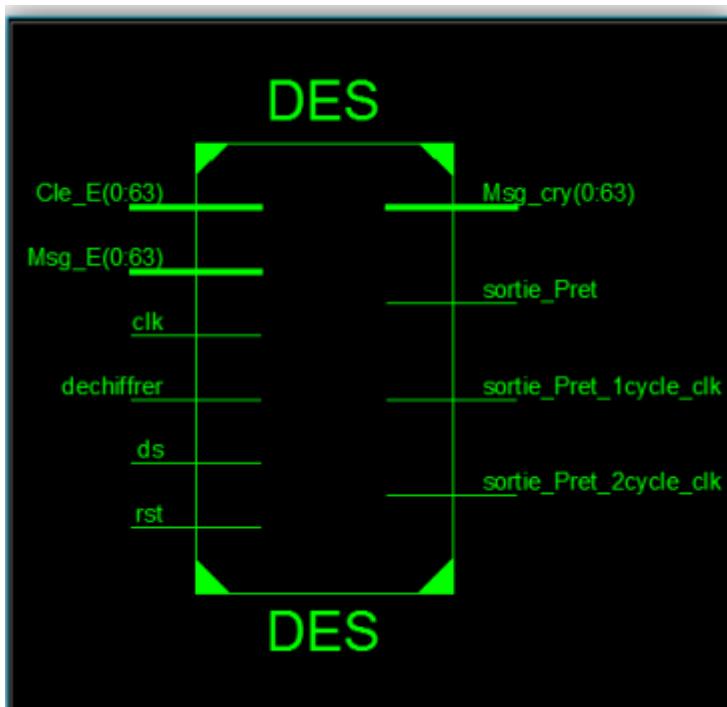


Figure 6: RTL schematic

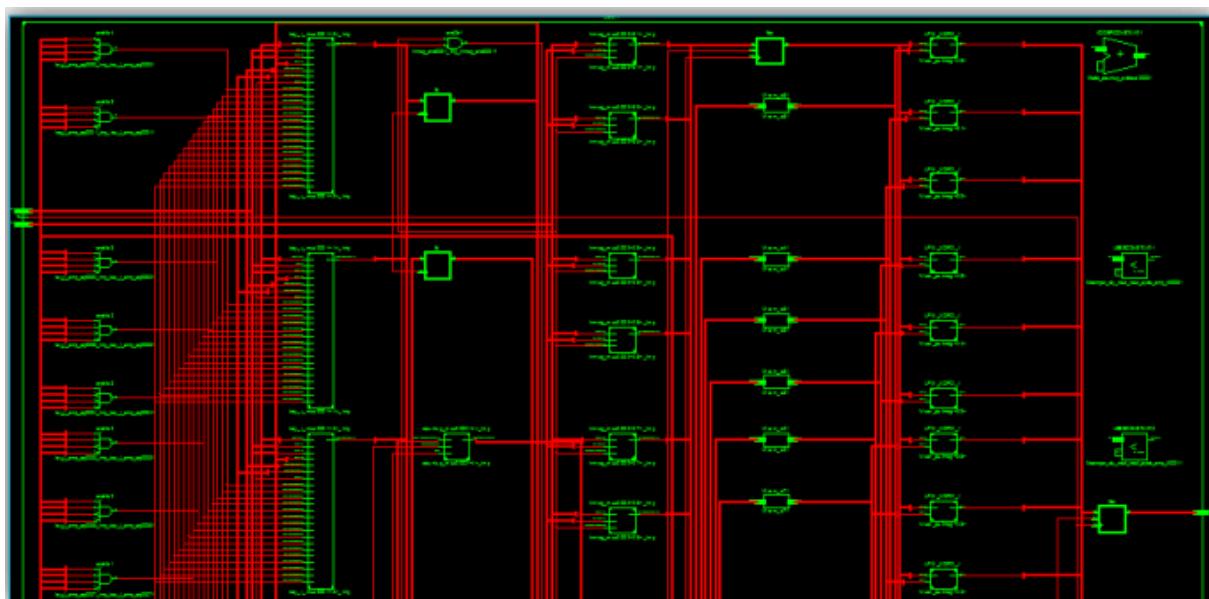


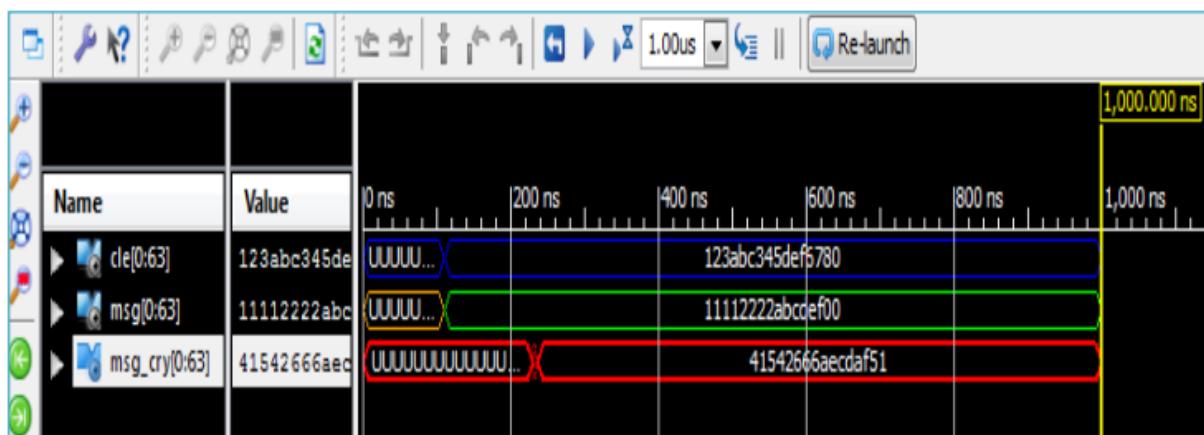
Figure 7: Aperçue du circuit DES

➤ **Test et Simulation :**

On prend : message « 123abc345def6780 »

Clé « 11112222abcdef00 »

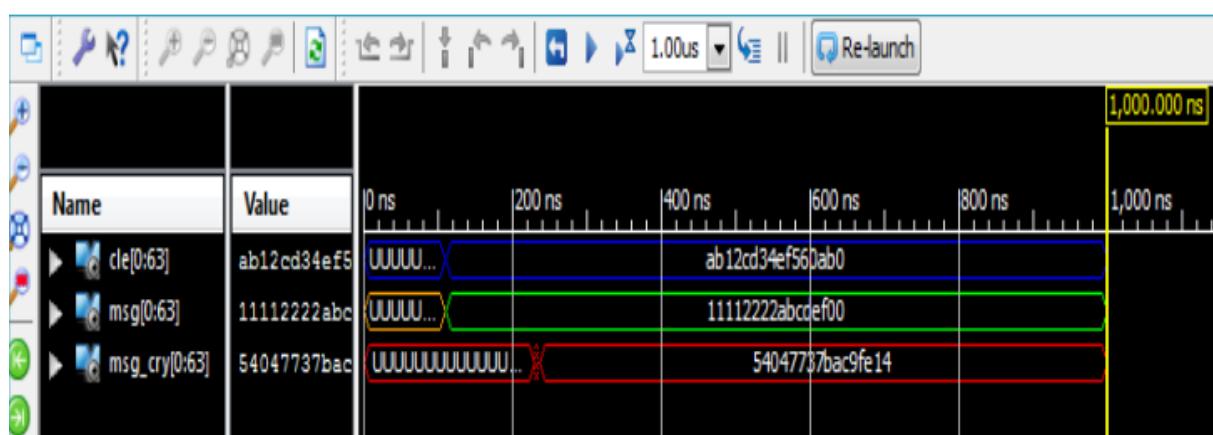
Résultat de simulation :



Message crypté : « 41542666aecdaf51 »

On change la Clé « ab12cd34ef560ab0 »

Résultat de simulation :



Message crypté : « 54047737bac9fe14 »

CONCLUSION :

Le DES l'un des crypto-systèmes les plus connus à clefs privées, n'est tout autant que RSA pas invulnérables à toutes les attaques qu'il peut subir régulièrement. En effet de nombreuses attaques sont déjà arrivées par le passé à venir à bout des algorithmes qui composent le DES, malgré le fait qu'il était considéré comme l'un des moyens de chiffrement les plus sûrs. Mais les attaques incessantes qu'il subissait, ont eu raison de DES et ont montré au grand jour ses faiblesses.

Aujourd'hui, le D.E.S. est fortement menacé par les puissances de calcul des ordinateurs. Il n'est en effet pas impossible de balayer la plupart des clés pour casser le code. Un nouveau système, le A.E.S. (Advanced Encryption Standard) est prévu pour le remplacer, d'où l'intérêt d'augmenter la sécurité de DES par le T DES [Triple DES (aussi appelé 3DES)] qu'est un algorithme de chiffrement symétrique par bloc, enchaînant 3 applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec 2 ou 3 clés DES différentes.