New Approach for Modifying DES Algorithm by Using Multiple Keys Depend on Heuristic Search Algorithm

Dr.Alaa K. Farhan
Computer Science, Universityof Technology/Baghdad
Email: Dralaa81.uotechnology.edu.iq
Dr.Suhad M.Kadhem
Computer Science, Universityof Technology/Baghdad
Noor Monem
Computer Science, Universityof Technology/Baghdad
Dena Saad
Computer Science, Universityof Technology/Baghdad

Received on: 24/4/2012 & Accepted on: 15/8/2012

ABSTRACT

In this paper, artificial search algorithm(breath algorithm) are used to design a symmetric key cryptography system based on DES algorithm,the LFSRs and breath algorithm are applied to generate a pseudo-random numbers sequence (PNS) which is used during the encryption process. The quality of PNSs highly depends on the set of LFSRs rule by selected the polynomial equation cells . This paper introduces a new method to enhance the performance of the Data Encryption Standard (DES) Algorithm. This is done by building a new structure for the 16 rounds in the original algorithm. This structure makes use of multiple secrete keys and the length of key is256-bits to process one block 256-bits of plain text.

Keywords: Pseudo-random sequence, LFSRs, heuristic search algorithm, Encryption algorithms, DES algorithm.

طريقة جديدة لتحسين خوارزمية التشفير DES باستخدام المفاتيح المتعددة بالاعتماد على خوارزمية البحث الموجه

الخلاصة

في هذا البحث تم استخدام مبدأ خوارزميات البحث الذكية لتصميم نظم تشفير متناظر اعتمادا على خوارزمية DES. تم تطبيق المنظومة متعددة الحدود وخوارزميات البحث الذكية لتوليد المفاتيح العشوائية المستخدمة في عملية التشفير. كفاءة المفاتيح العشوائية تعتمد على اختيار خلايا معادلة متعددة الحدود المستخدمة. تم اقتراح طريقة جديدة لتعزيز أداء الخوارزمية وذلك ببناء هيكلية جديدة للمقاطع الستة عشر التي تعتمدها الخوارزمية. هذه الهيكلية الجديدة تعتمد على استخدام عدة مفاتيح سرية بطول ٢٥٦ بت لمعالجة بلوك واحد من البيانات.

INTRODUCTION

Historically, cryptography arose as a means to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel. While providing privacy there remains a central goal, the field has expanded to encompass many others, including not just other goals of communication security, such as guaranteeing, integrity and authenticity of communications, but many more sophisticated and fascinating goals[1]. Cryptographyis a discipline of mathematics

https://doi.org/10.30684/etj.31.1B.10
2412-0758/University of Technology-Iraq, Baghdad, Iraq

and computer science concerned with information security and related issues, particularly encryption, authentication, and such applications as access Control [2]. Cryptography, as an interdisciplinary subject, draws on several fields. Prior to the early 20th century, cryptography was chiefly concerned with Linguistic patterns. Since then, the emphasis has shifted, and Cryptography now makes extensive use of mathematics, including topics from information theory, computational complexity, statistics, combinatory, and especially number theory [3]. Security has many facets. For a system to be secure, many factors must combined. For example, it should not be possible for hackers to exploit bugs, break into a system, and use an account. They shouldn't be able to buy off your system administrator. They shouldn't be able to steal your back-up tapes. These things lie in the realm of system security. The cryptographic protocol is just one piece of the puzzle. If it is poorly designed, the attacker will exploit that. For example, suppose the protocol transmits a password in the clear (that is, in a way that anyone watching can understand what it is), that is a protocol problem, not a system problem. In addition, it will certainly be exploited [2].

DATA ENCRYPTION STANDARD (DES)

Without doubt the first and the most significant modern symmetric encryption algorithm is that contained in the Data Encryption Standard (DES). The algorithm has been in wide international use, The Data Encryption Standard (DES), as specified in FIPS Publication 46- 3 [4], is a block cipher operating on 64-bit data blocks. The encryption transformation depends on a 56-bit secret key and consists of sixteen Feistel iterations surrounded by two permutation layers: an initial bit permutation *IP* at the input, and its inverse IP^{-1} at the output. The structure of the cipher is depicted in Figure (1). The decryption process is the same as the encryption, except for the order of the round keys used in the Feistel iterations.

The 16-round Feistel network, which constitutes the cryptographic core of DES, splits the 64- bit data blocks into two 32-bit words, LBlock and RBlock (denoted by L_0 and R_0). In each iteration (or round), the second word *Ri*is fed to a function***f***and the result is added to the first word *Li* . Then both words are swapped and the algorithm proceeds to the next iteration. The function *f* is key-dependent and consists of four stages:

1.Expansion (E). The 32-bit input word is first expanded to 48 bits by duplicating and reordering half of the bits.

2.Key mixing. The expanded word is XORed with a round key constructed by selecting 48 bits from the 56-bit secret key, a different selection is used in each round.

3. Substitution. The 48-bit result is split into eight 6-bit words which are substituted in eight parallel 6 × 4-bit S-boxes. All eight S-boxes, are different but have the same special structure.

4. Permutation (P). The resulting 32 bits are reordered according to a fixed permutation before being sent to the output.

The modified RBlock is then XORED with LBlock and the resultant fed to the next RBlock register. The unmodified RBlock is fed to the next LBlock register. With another 56 bit derivative of the 64 bit key, the same process is repeated.Full details of DES are given in Algorithm (1) [5].

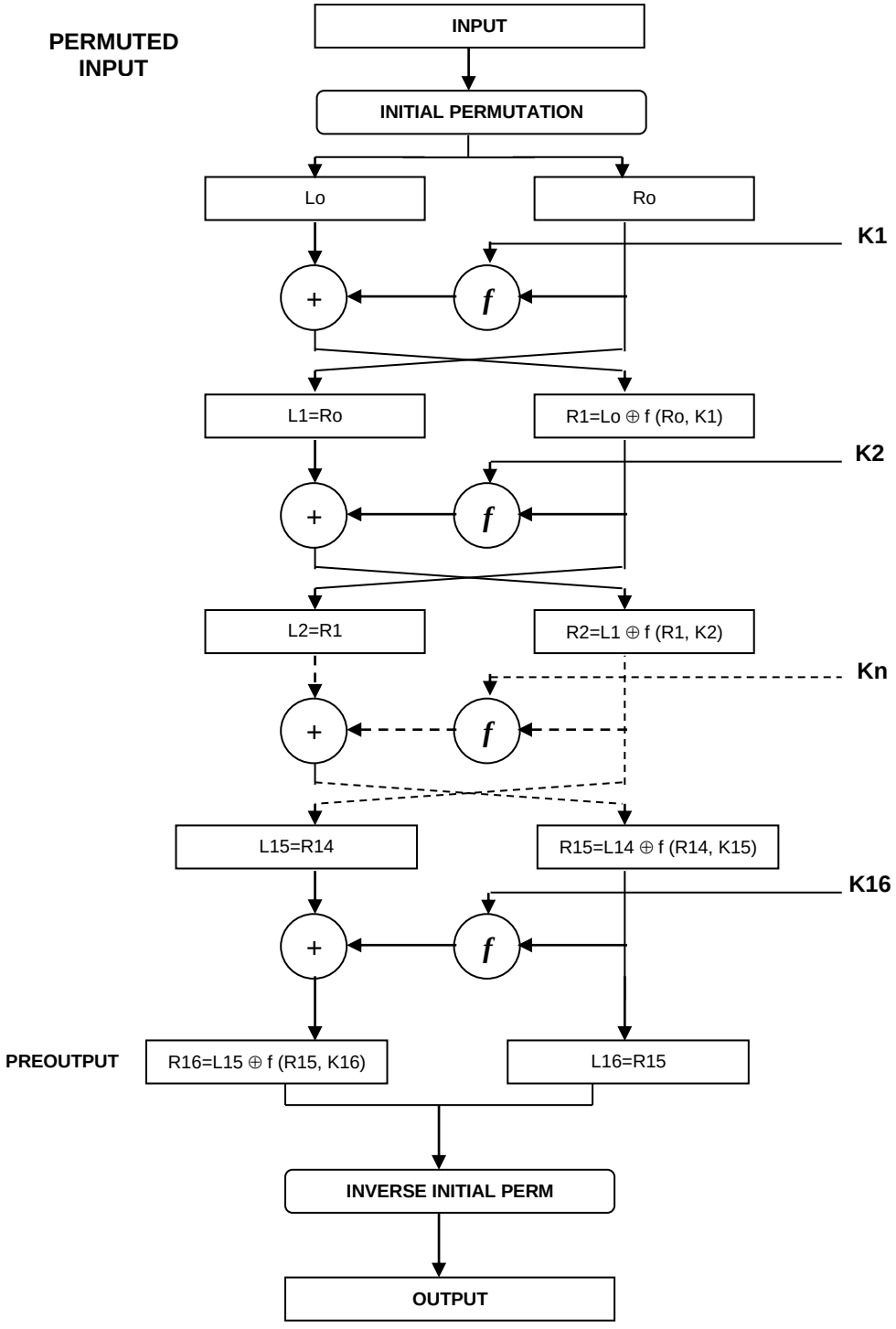


Figure (1): DES computation path.

Algorithm (1): Data Encryption Standard (DES)

INPUT: plaintext m1 . . . m64; 64-bit key K=k1 . . . k64 (includes 8 parity bits).
OUTPUT: 64-bit ciphertext block C=c1 . . .c64.
1. (key schedule) Compute sixteen 48-bit round keys Ki, from K.
2. (L0, R0) ← IP(m1, m2,. . .m64) (Use IP Table to permute bits; split theresult into left and right 32-bit halves L0=m58m50 . . . m8,R0=m57m49 . . . m7)
3. (16 rounds) for i from 1 to 16, compute Li and Rias follows:
3.1. Li=Ri-1
3.2. Ri = Li-1 ⊕*f* (R i-1, Ki) where *f*(Ri-1, Ki) = P(S(E(Ri-1) ⊕ Ki)), computed as follows:
(a) Expand Ri-1 = r1r2 . . . r32 from 32 to 48 bits, T ←E(Ri-1).
(b) T' ← T ⊕ Ki . Represent T ' as eight 6-bit character strings: T '= (B1 . . . B8)
(c)T " ← (S1(B1), S2(B2), . . . S8(B8)). Here Si(Bi) maps to the 4-bit entry in row r and column c of Si
(d)T"' ← P(T"). (Use P per table to permute the 32 bits of T"=t1t2 . . . t32, yielding t16t7 . . . t25.)
4. b1b2 . . . b64 ← (R16, L16). (Exchange final blocks L16, R16.)

DIFFUSIONAND CONFUSION [6]

The terms diffusion and confusion were introduced by Claude Shannon to capture the two basic building blocks for any cryptographic system . Shannon's concern was to thwart cryptanalysis based on statistical analysis. The reasoning is as follows. Assume the attacker has some knowledge of the statistical characteristics of the plaintext. For example, in a human-readable message in some language, the frequency distribution of the various letters may be known.Or there may be words or phrases likely to appear in the message (probable words). If these statistics are in any way reflected in the cipher text, the cryptanalyst may be able to deduce the encryption key, part of the key, or at least a set of keys likely to contain the exact key. In what Shannon refers to as a strongly ideal cipher, all statistics of the cipher text are independent of the particular key used. Shannon suggests two methods for frus- trating statistical cryptanalysis: diffusion and confusion. In diffusion, the statistical structure of the plaintext is dissipated into long-range statistics of the cipher text.

Substitution: Each plaintext element or group of elements is uniquelyreplaced by a corresponding cipher text element or group of elements.

Permutation: A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

SEARCH TECHNIQUE TYPES [7, 8]

Usually types of intelligent search are classified into three classes; blind, heuristic and random search. Blind search is a technique to find the goal without any additional information that help to infer the goal, with this type there is no any

consideration with process time or memory capacity. In the other side the heuristic search always has an evaluating function called heuristic function which guides and controls the behavior of the search algorithm to reach the goal with minimum cost, time and memory space? While random search is a special type of search in which it begins with the initial population that is generated randomly and the search algorithm will be the responsible for generating the new population bases on some operations according to a special type function called fitness function.

A. Blind Search

There many search strategies that come under the heading of blind search (also called uniformed search). The term means that they have no additional information about states beyond that provided in the problem definition. All they can do is generate successors and distinguish a goal state from a non goal state .Thus blind search strategies have not any previous information about the goal nor the simple paths lead to it. However blind search is not bad, since more problems or applications need it to be solved; in other words there are some problems give good solutions if they are solved by using depth or breadth first search.

B. Breadth First Search

Is a simple strategy in which the root node is expanded first, then all the successors of the root node are expanded next, then their successors, and so on. In general all the nodes are expanded at a given depth in the search tree before any nodes at the next level are expanded. Breadth first search can be implemented by calling TREE-SEARCH with any empty fringe that is a first-in-first-out (FIFO) queue, assuring that the nodes that are visited first will be expanded first. In other words, calling TREE-SEARCH (problem, FIFO-QUEUE) result in a breadth first search. The FIFO queue puts all newly generated successors at the end of the queue, which means that shallow nodes are expanded before deeper nodes.

PROPOSED OF NEW APPROACH FOR MODIFYING DES ALGORITHM

In this approach the design different from fistel model by using difference functions as s-box, IP, $IP^{-1}$and split into 4 channels we will explain a new approach of block Cipher of DES Algorithm and this new approach will have 16 round and use a key of length 64bits that will be expand into 256 bits, in the first round we will take a plain text of 32 character and change it into binary form by taking each character and change it into 8 bits that represent the ASCII of character and as a result we will have 256 bits ,These 256 bits will then split into four blocks each block of 64 bits and these blocks will enter into an initial permutation and the result will be a new four blocks we will name the blocks as (LL, LR, RL, and RR) where LL represents left-left, LR represent left-right, RL represent right-left and RR represents right-right. Then we take LL and LR and make a swap between them and as a result we will have a new LL and new LR then LR will be xored with first 64 bits of the key and the result will be combined with LL and make 128 bits , these 128 bits will take only the bits that have even position and xor with the second 64 bits of the key and result a new 128 bits then we will split into two blocks of 64 bits and each of these blocks will enter in the inverse permutation and result a new two blocks of 64 bits and again we will combine them as 128 bits and then we back to the RR and RL .RL will enter into suggestion function and will result a new RL of 64 bits and combined it with RR and will result a new 128 bits these 128 bits then enter in the s-box with the remaining of the key 128 bits and result a new 128 bits and we will split it into two blocks of 64 bits and these blocks

will enter in the inverse of permutation and results of these blocks will be combined to make a new 128 bits and this 128 bits will be again combined but with 128 bits the final result of LL and LR after the exit of the inverse permutation and will result a 256 bits these 256 bits is the output of the first round and these 256 bits will then enter to the algorithm as a new plaintext for the second round and so on until the 16 round will finish we will get then a 256 bits that is the cipher text of the first block of the plaintext that enter at the first time and to encipher anew block of plaintext these operation will repeated again and enter new plaintext into 16 rounds and result a new cipher text and combine these cipher with the previous cipher text after change These bits into string by taking 8 bits and make a character and so on until 256 will end and the result will be 32 characters as show in the Figure(2).

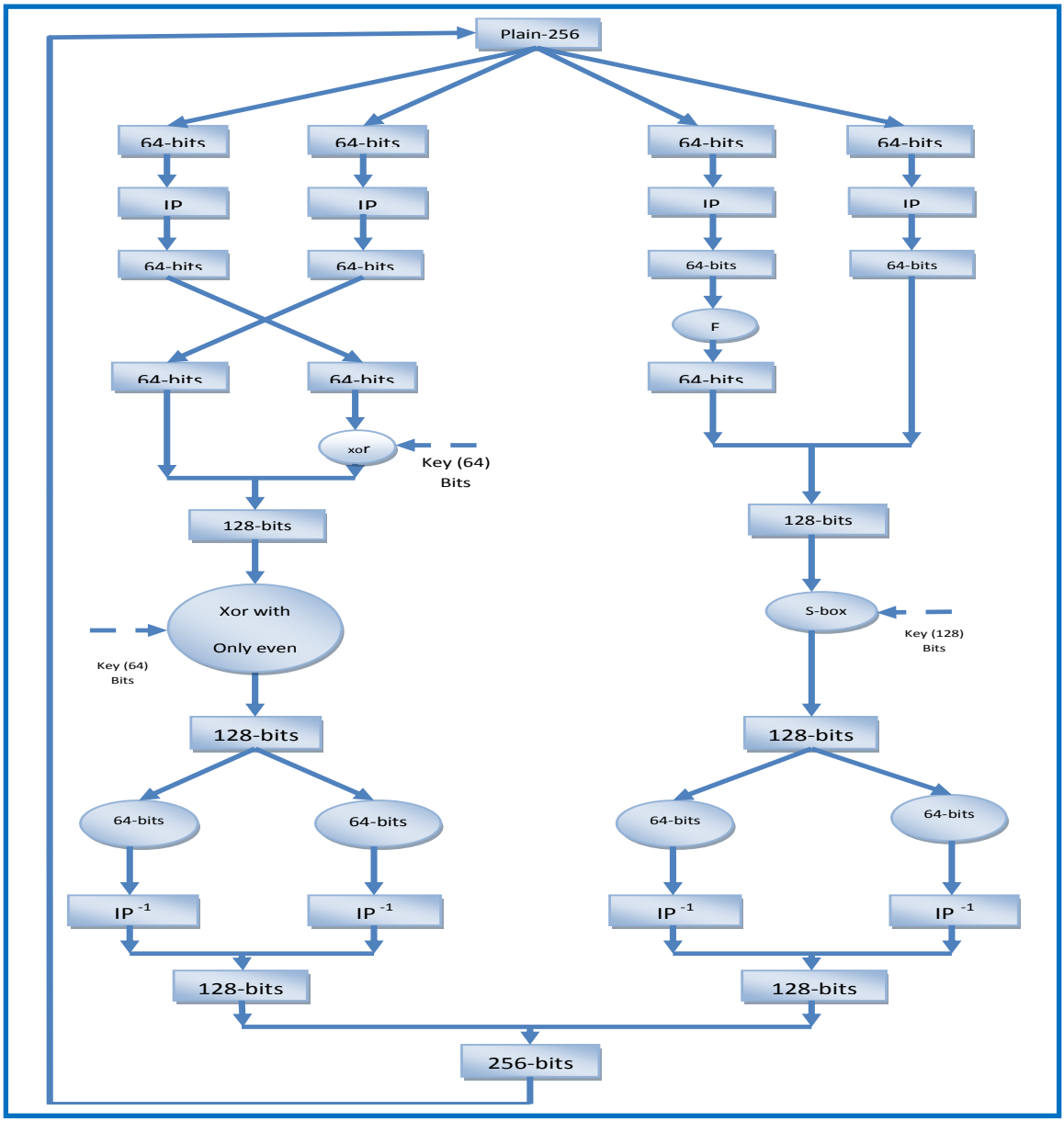


Figure (2): New approach Block Cipher.

Encryption Algorithm:

Input:

M=m1…m256 (plaintext 256-bits)
K=K1…K256 (secret key 64-bits)

Output:

C=c1…c256 (cipher text 256-bits)

Begin

For i =1 to 16 do

Begin

1. Generate new key as 256 bits from the previous key of 64-bits
2. Split the plaintext into four blocks each of 64-bits(LL,LR,RL,RR)
3. IP (LL,LR,RL,RR)
4. Core process
   - 4.1 F(RL) with key 64-bits
   - 4.2 Swap(LL to LR),(RL,LL)
   - 4.3 LR xor key 64-bits to LR
   - 4.4 Merge LL with LR to L, Merge RL with RR to R
   - 4.5 S-box (R) to new R
   - 4.6 Eve n position (L) xor Key 64-bits to new (L)
5. Split R to RR and RL and L to LR,LL
6. IP (LL,LR,RL,RR)
7. Merge (LL,LR,RL,RR)

Approach has multi functions can explain in detail:

Initial permutation (IP)

IP is the important function when design fistel model because in IP can get the diffusion, by the diffusion will difficult analysis from attack and can get special properties in reorder location of bitts.

We design the new IP by reorder of location bits. Can explain the new IP:

The input to the initial permutation is 64 bits and we will full the array of (8X8), this function have two processes:

1-Make the content of array by each row takes 8bits.

2- Exchange (replace) each row to column, to get new array.

In the design we not need the special table of location between sender and receiver can explain in the Figure (3).

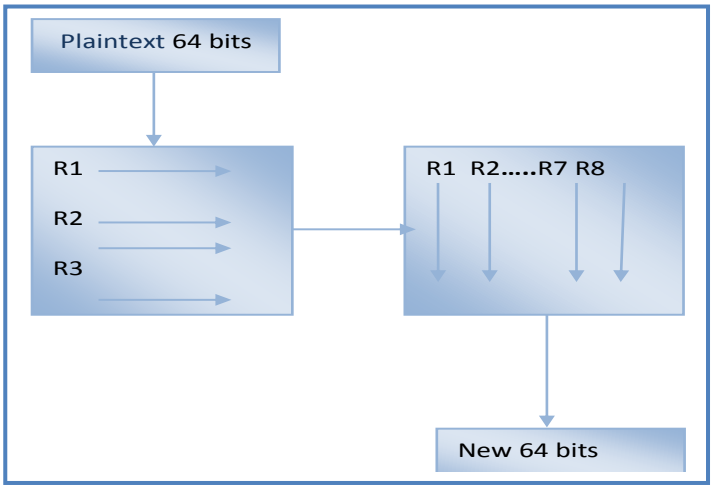


Figure (3): IP Permutation.

Inverse of initial permutation (IP^{-1})

IP^{-1} is the inverse of IP and the input to the inverse permutation is 64 bits and we will full the array of (8X8), this function also have two processes:
1-Make the content of array by each Colum takes 8-bits
2-Rotate the array by replace each Colum to row.
The figure(4) display the **IP^{-1}** to get the original location for bits:

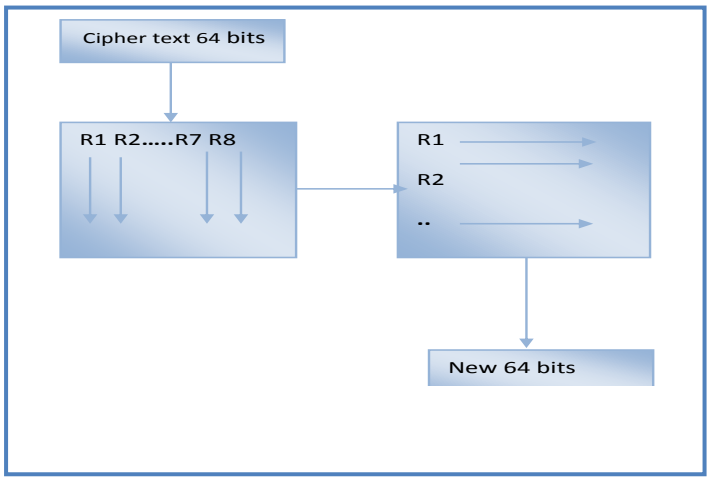


Figure (4): IP^{-1} Permutation.

S-box Function

One of important of design fistel model S-box function, by the s-box can get the confusion, the confusion is reducing the statistical properties of plain text, and we need design S-box for special idea and has the confusion.
This function consists of two stages:-
1-The first stage is shift to left of the plaintext but this shift will be depend on the number of round in the first round the shift to left by one and if the round two the shift to left by two and so on.

2- The second stage is (XOR) operation the plaintext that results from the first stage with the key but only 128 bits of the key.(the key 128bits take from key generator for each round),Can explain in the figure()5.

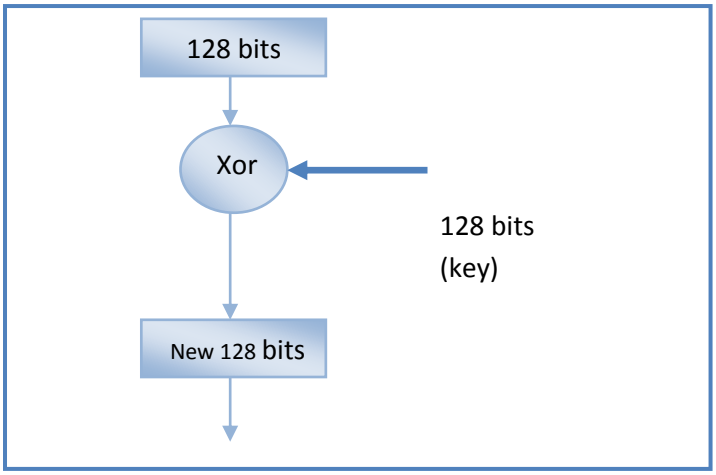


Figure (5): S-box.

S-box^{-1} Function

Is the inverse of S-box function consisting of two stages:-

1-The first stage is (Xor) operation the cipher text with key of 128 bits and this key is the same as the key that is used in S-box.

2-The second stage is shift to right the result of cipher text at the first stage by number of round as we explained earlier in the S-box ,can explain detail in figure(6).

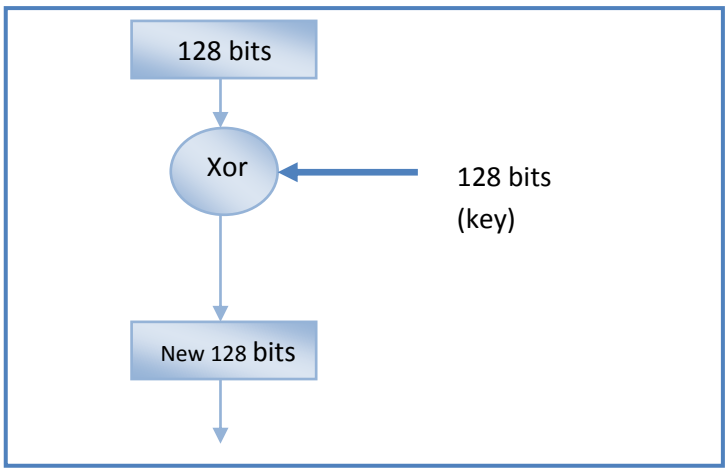


Figure (6): S-box^{-1} .

F-function

The main processes in this function is (XOR) between the plain or cipher text with new sub key (64)bits, andthis sub key can get from the selector function.
In this function design selector to choose some of bits from the key and these bits will share between the sender and receiver to make sure that nobody can know which bits that selected and this function will use in both encryption and decryption and after make the selection it will be enter into a liner feedback shift register and repeated these operation 64 times to obtain 64 bits and these 64 bits will be xored with the plaintext if the operation is cipher and with key but if the decryption we use then the 64 bits that result from liner feedback shift register will XOR with cipher text and the key. Can explain in the Figure (7).

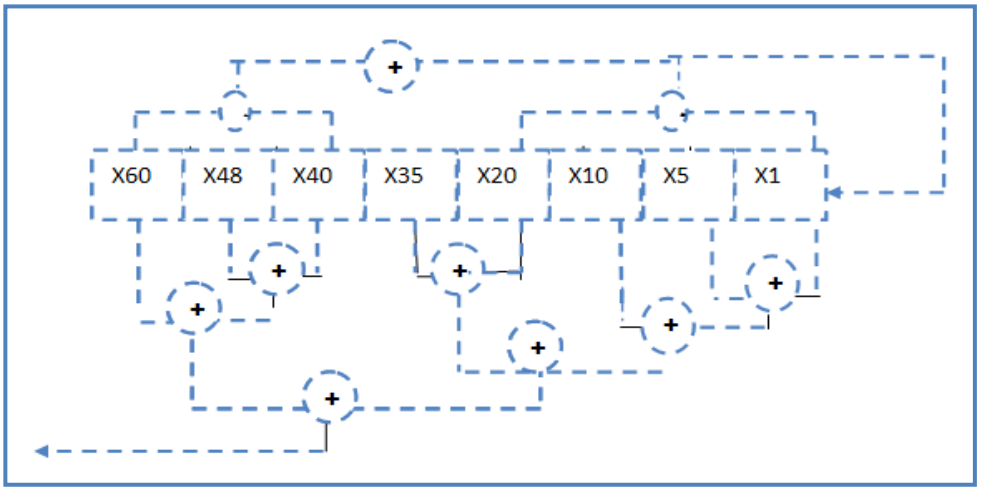


Figure (7): F-function.

Key Generator

Weneedmultiplekey in this new approach because each block need 256-bits and each block has 16 round 16*256 key for each round and the massage has multi block ,so we design the generator to generate all keys we need to process all block ,the generate have two stage, the figure(8) explain the key generator for one iteration:

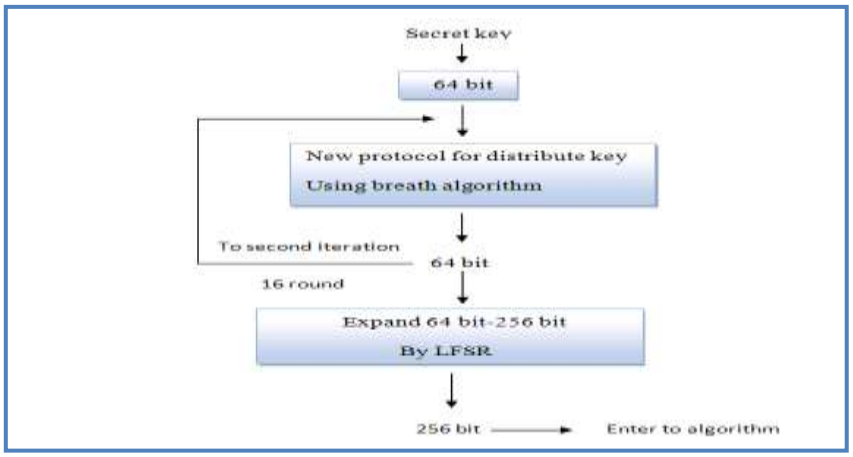


Figure (8): **flow chart for key generator for (1 iteration)Tree**.

The input is a string of eight characters and will be converting to binary form and result 64 bit this 64 bit will enter to fixed table that will be shared between sender and receiver can explain in table(1):

Table (1): Initial key table

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

And table(1) will used to spread the tree the first 32 bit will be spread into left tree and the second 32 will be to the right of tree and then will be used breadth algorithm to generate new 64 bit, can visible in Figure(2) .

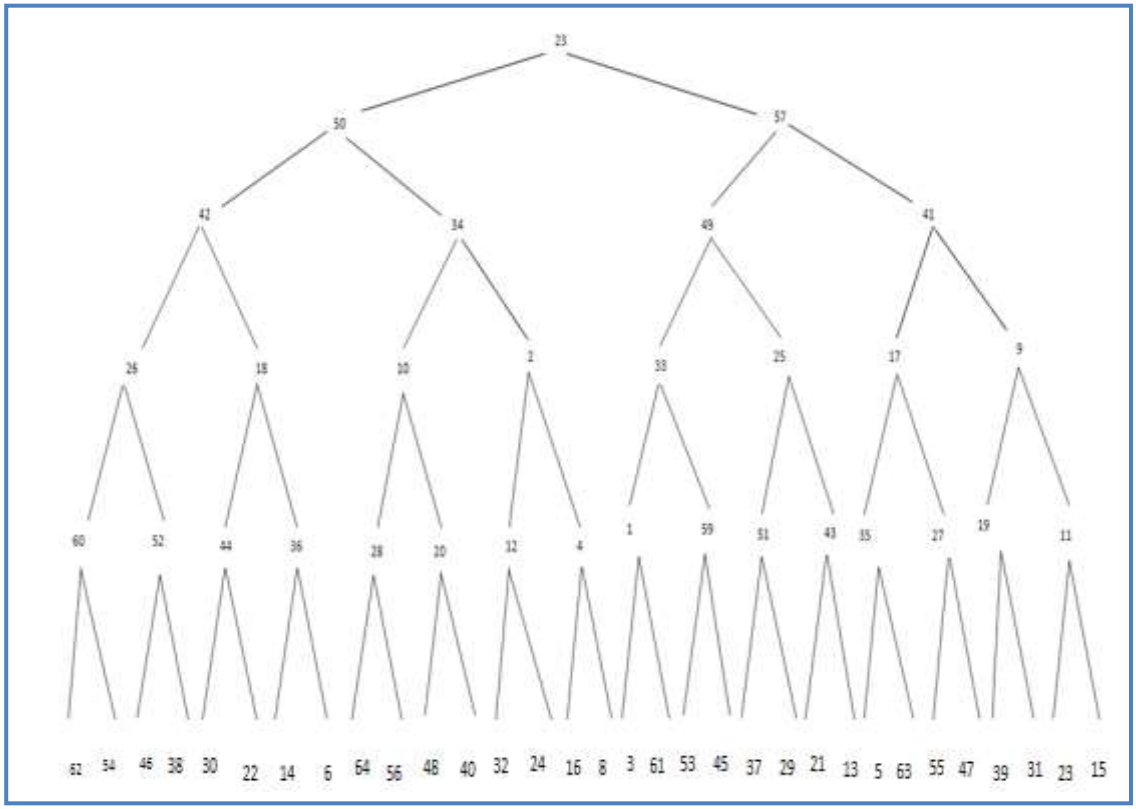


Figure (9):-**Distribute in Tree .**

When the breath algorithm runs in the tree can get new sub key, explain in Table(2):

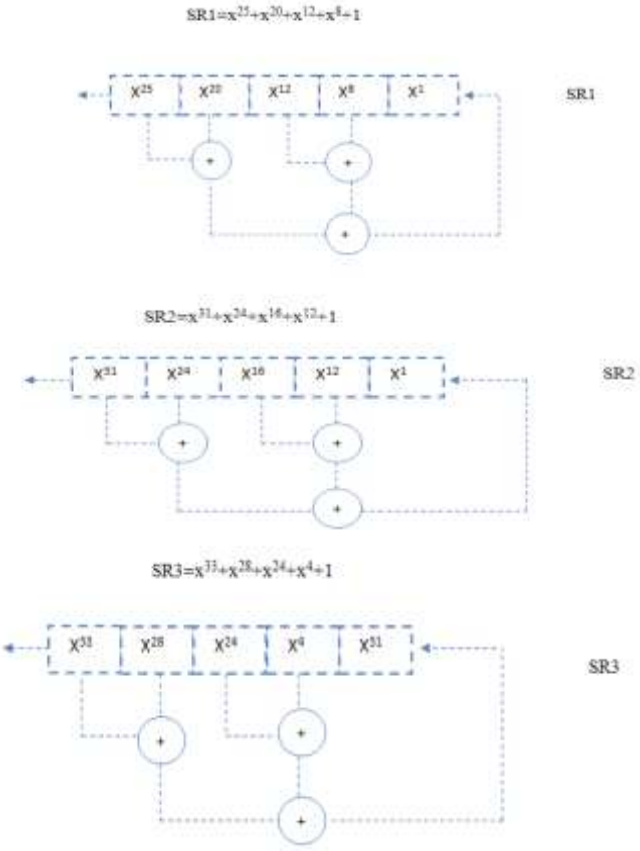
Table (2): Output table key.

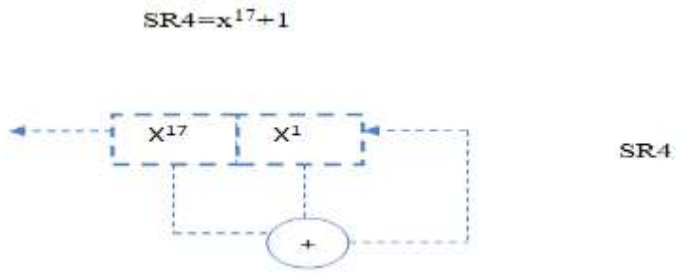
58	50	57	42	39	49	41	26
28	10	2	33	25	17	9	60
52	44	36	24	20	12	4	1
59	51	43	35	27	29	11	62
54	46	38	30	22	14	6	64
56	48	40	32	24	16	8	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

The new sub key is copy in two, one send to expand to get 256- bits and the two copy reset to stage one (tree).

- **Expanding Function**

In this function, the main process expand the 64-bits to 256-bits by using multi of register each register is choose by special properties ,in this function we have 4 SR and correct in special design to get maximum period **[9]**.
This 64-bit will expand in 256-bit by using liner feedback shift register using this registers in figure (10):





Figure(10): Registers System .

And this register will take bits form the key and the result form every register will be take it as anumber and enter into sum to find the resat in a binary array that will be enter as 3*3 for example if the resat from SR1 is 1 and SR2=0 and SR3=1 the sum of these will be101=5 so we take the position 5 in the array and find what in position 5 and take it and then will exored with the output of SR4 and find the first bit in 256 bits and the repeat this process 256 time to generate 256 bits and result of every register will enter to first position and so on we use 64 bit that resat and enter for second iteration and for every time we find bit we will shift these registers to left .can explain in Figure(11) :

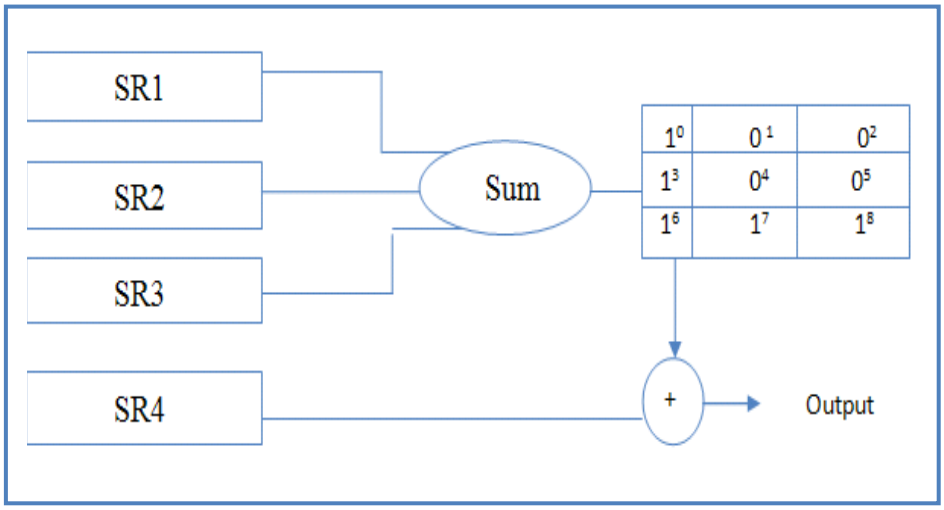


Figure (11): Replaced.

NEW APPROACH VERSUS DES ALGORITHM (TIME AND COMPLEXITY)

In this part we will try to find out some aspects of evaluation concerning speed, complexity and resistance against kwon attack as a comparative study with DES block cipher system. The speed of the new approach and DES is non equivalent. The S-box Function of DES is an 8 tick time consuming function because there are 8 S-box which work serially. In New approach the S-box takes 1 tick time consuming function because the new approach have one S-box,the work of the S-box independent from other processes.The new algorithm is programmed in visual basic.net on personal computer(P4) with hardware CPU (2GB) and Ram (1GB).Then they applied to messages that have different sizes we take 1MB, 2MB, 3MB and both encryption process and decryption process in minutes and the test

the messages five times to make sure that results is clear because the CPU might be busy with another process. In table (30 explain the running time in minutes:

Table (3): Time Measure .

Message Size	Operation	DES In Min	New approach In Min
1 MB	Encryption	6	6
	Decryption	6	6
2 MB	Encryption	25	15
	Decryption	25	15
3 MB	Encryption	46	25
	Decryption	46	25

Curves are used to explain the difference in time. They have been illustrated in Figures(12) and (13):

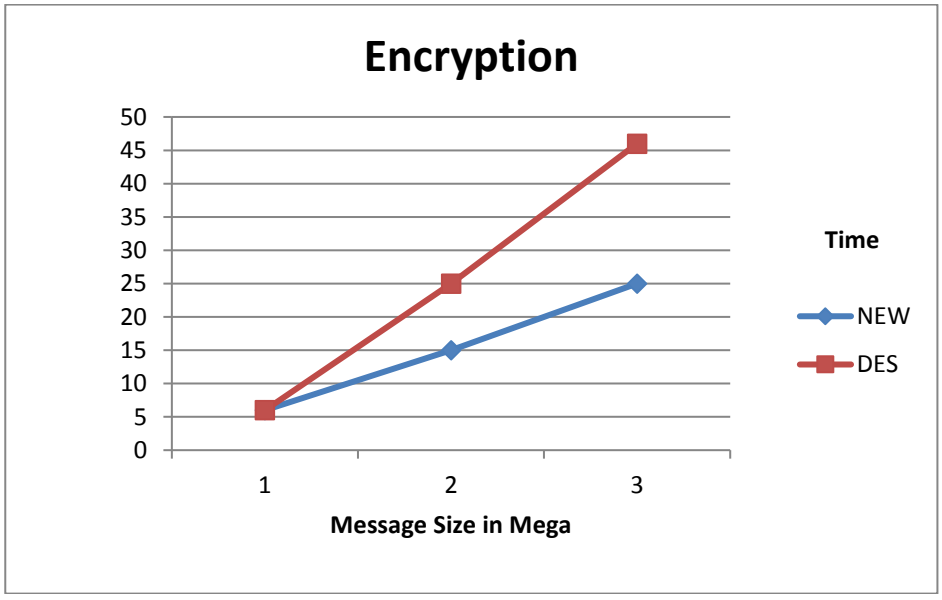


Figure (12): **(Encryption processes).**

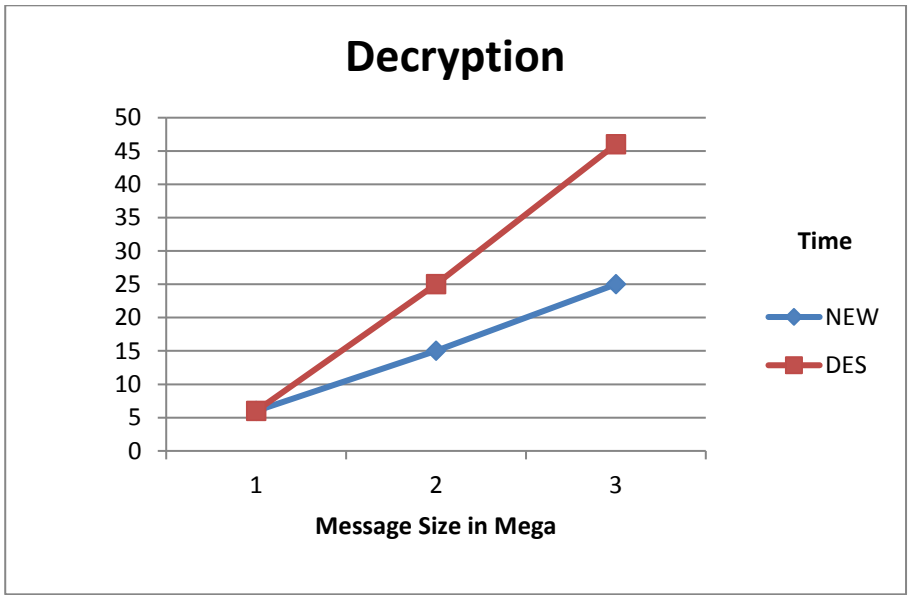


Figure (13) :(Decryption processes).

CONCLUSIONS

1-The new approach of block cipher algorithm enhances two criteria of standard block cipher, which are confusion and diffusion in multistage.

2-The new approach of block cipher algorithm is developed to increase the complexity degree against the attacker task by consuming more time to achieve the analytical process depend on numbers of keys used.

3- The new approach of block cipher algorithm increase the randomness of the used secret key by expanding the original key through the stream generator and breadth search algorithm which gives higher randomness as a new long secret key with higher randomness property.

REFERENCES

[1].Ali M.,"Design public key cryptography base on new discretelogarithm problem", PhD, thesis, Baghdad,university of technology, 2007.

[2].Information security. Retrieved from Wikipedia the free Encyclopedia: http://en.wikipedia.org/wiki/Information _seaurity,2005.

[3].Schneider, B.,"Applied cryptography: protocols, Algorithms, and source code in C.", second edition .New York: John Wiley & sons, 1996.

[4]. Walter T.,"A Brief History of the Data Encryption Standard." In Internet Besieged: Countering Cyberspace Scofflaws, New York, NY, USA: ACM press/Addison –Wesley publishing Co., 275-280.1007.

[5].Beker, H. and Piper, F."Cipher Systems", Wiley, 1982.

[6].William Stallings, "CryptographyandNetworkSecurityPrincipleand Practice", Pearson Education, Inc., publishing as Prentice Hall,2011.

[7].Stuart J.Russell and peter Noving ," Artificial Intelligence modernapproach second edition",publishing as Prentice Hall.

[8].Amit K.,"Artificial Intelligence and Software Computing: behavioral and cognitive modeling of human brain",John Wiley &sons ,1999.

[9].Alaa K.," Security Protocol for Mobile Data", PhD, thesis, Baghdad,university of technology, 2009.