International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 23 (2018) pp. 16552-16563

Evaluation of Differential – Linear Cryptanalysis Combined Attack on Cryptographic Security System

B. Srinivasa Rao[1] and P. Premchand[2]

[1] *Department of Computer Science and Engineering*
Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad-500090
Jawaharlal Nehru Technological University Hyderabad, Hyderabad 500038 Telangana, India.

[2] *Department of Computer Science Engineering, University College of Engineering,*
Osmania University, Hyderabad-500007 *India.*

Abstract

In the present research work a novel model has been proposed for evaluation of Differential-Linear cryptanalysis on complex cryptographic security system. The differential and linear methods of whale optimization algorithm have been used as combined attack. A combination of Blowfish and DES algorithm has been used for design of complex cryptographic security system. This proposed work has been implemented in Java programming language with JDK 1.7.0. The comparison of computed key optimization time for several data sets of different sizes for the present proposed cryptosystem and other cryptosystems indicates the significance of combined attacks in cryptanalysis.

Keywords: cryptanalysis, differential-linear cryptanalysis, cryptographic security system, combined attack.

1. INTRODUCTION

Cryptanalysis is a discipline of Cryptology and is converse to another well known discipline Cryptography. Cryptanalysis is a science of breaking the security of various computing systems provided by cryptography, mostly through mathematical understanding of the cipher structure. In general, the main objective of cryptography is to ensure security for information by designing strong cryptosystems. The aim of the cryptanalyst is to identify weaknesses of cryptosystems and defeat the security of the cryptosystem. In the present information age the cryptology is plays a significant role in various fields like commerce, military, governments etc. in providing security. At the same time, due to remarkable advances in cryptanalytic techniques, now-a-days it is also becoming essential to consider including a systematic, qualitative and quantitative analysis of security against newly designed techniques [1-3]. Several cryptanalytic techniques have been devised for various cryptographic security systems and have been reviewed in the literature [4, 5]. But all these attacks are mostly individual attacks or single attacks. These attacks have their role in cryptanalysis. It is quite natural that when new attacks are being designed to counter them strong security measures are devised for cryptographic systems. Hence it is obvious that new attacks are to be designed for enhanced security systems. However, it is a continuous and endless process for designing new attacks and new counter measures. But in each aspect new and creative ideas may improve or provide better and efficient techniques. The present research work is the motivation from the above discussion. In the present research work a novel model has been proposed for evaluation of Differential-Linear cryptanalysis on complex cryptographic security system. The differential and linear methods of whale optimization algorithm have been used as combined attack. A combination of Blowfish and DES algorithm has been used for design of complex cryptographic security system. This proposed work has been implemented in Java programming language with JDK 1.7.0. The comparison of computed key optimization time for several data sets of different sizes for the present proposed cryptosystem and other cryptosystems indicates the significance of combined attacks in cryptanalysis. In this paper, various cryptographic attacks have been briefly reviewed in section-2. The combined attacks have been discussed in section-3. The Proposed Model is developed in section-4.Experimental details have been given in section-5. Results and discussion has been presented in section-6. Finally, section-7 concludes the work done.

2. SECURITY ATTACKS

The cryptanalytic tools should be designed and developed taking into consideration of the complexity involved in the processes being implemented and importance of the security infrastructure. In this aspect to design new cryptanalytic tools two procedures may be followed. (1) Inventing new attacks. (2) Extending, generalising and combining already known cryptanalytic attacks. Research is being done in this direction and several new approaches were reported in the literature. In general it is assumed that Encryption algorithm and Decryption algorithms are available to cryptanalyst and secret

information (also known as Key (K)) is completely unknown. Also Plain Text and Cipher Text copies may be obtained with some skilful efforts. This scenario will make the cryptosystem vulnerable to attacks. The main objective of the attackers is to reveal the secret information (key) to break the cipher for reproducing original Plain Text. In cryptology, an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of data or resources. An attack of a cryptographic system may break the security of system either completely or partially and provides various kinds of information of the system. It has been proposed various levels of attacker's success during cryptanalysis [6]. (i) Total break: deducing and obtaining a secret key. (ii) Global deduction: Discovering an algorithm, that may allow decrypting many messages without knowing the actual secret key. (iii) Local deduction: Discovering an original plaintext of the specific given ciphertext. (iv)Information Deduction: obtaining some information about the secret key or original message. However, the best ciphers should protect against all the cipher's failures levels mentioned above and should not be able to reveal any information related to the secret key and plaintext messages [6]. In spite of all security measure due to flaws in the system, the crypto systems are pruned to various types of attacks. In general the attacks are classified as active and passive attacks. An active attack is a network attack characterized by the attacker attempting to break into the system. During an active attack, the intruder will introduce data into the system as well as potentially change data within the system. A passive attack is a network attack in which the purpose is solely to gain information about the target and no data is changed on the target [6-10]. Thus the process of attempting to discover plain text or key or both is cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst. The categories of cryptanalytic techniques are as follows:1. Cipher text only: A copy of cipher text alone is known to the cryptanalyst. 2. Chosen plaintext: The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key. 3. Chosen cipher text: The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key. 4. Chosen Key attack. 5. Known plaintext: The cryptanalyst has a copy of the cipher text and the corresponding plaintext. 6. Known ciphertext: The cryptanalyst has a copy of the plain text and the corresponding ciphertext. 7. Adaptive chosen plaintext: n-PTs are chosen to obtain n-CTs using EA. 8.Adaptive Chosen ciphertext: n-CTs are chosen to obtain n-PTs using DA [6-10]. A list of cryptanalysis techniques have been listed below:

1. Chosen Plaintext and Cipher text attacks.

1.1 Differential Cryptanalysis

1.2 Truncated cryptanalysis

1.3 Higher order Cryptanalysis

1.4. Impossible differential Cryptanalysis

1.5 Integral cryptanalysis.

1.6. Multiset attack

1.7. Amplified Boomerang cryptanalysis.

1.8. Rectangle attack

2. Adaptive Plaintext /Cipher text attack

2.1 Boomerang attack

3. Chosen Key attack

3.1 Related Key attack

3.2 The Slide attack

3.3 Statistical related key attack

4. Known plaintext/ciphertext attack

4.1 Liner cryptanalysis

4.2 Zero correlation attack

4.3 Bi-linear cryptanalysis

5. Other attacks

5.1 Statistical cryptanalysis

5.2. Brute force attack

5.3. DoS

5.4Attack on Two-Time Pad

5.5Frequency analysis

5.6. Man-in-the-middle attack

5.7. Meet-in-the-middle attack

5.9. Replay attack

5.10. Homograph attack

5.11. Birthday attack

5.12. Rainbow attack

All above mentioned attacks have been implemented on suitable ciphers independently and details are available in literature and also have been reviewed elsewhere [11].

3. COMBINED ATTACKS

All the attacks that have been discussed in the above section are mostly individual attacks or single attacks. These attacks have their role in cryptanalysis. It is quite natural that when new attacks are being designed to counter them strong security measures are devised for cryptographic systems. Hence it is obvious that new attacks are to be designed for enhanced security systems. However, it is a continuous and endless process for designing new attacks and new counter measures. But in each aspect new and creative ideas may improve or provide better and efficient techniques. The cryptanalytic tools should be designed and developed taking into consideration of the complexity involved in the processes being implemented and importance of the security infrastructure. In this aspect to design new cryptanalytic tools two procedures may be followed. (1) Inventing new attacks. (2) Extending, generalising and combining already known cryptanalytic attacks. Research is being done in this direction and several new approaches were reported in the literature. In this paper some of these related approaches have been reviewed. This section mainly focuses on new approaches for combination of attacks. Various combined attacks have been reported in the literature. In the present survey an attempt has been made do discuss some important combined attacks. The theme behind these combined attacks is an assumption that instead of individual attacks combination of various attacks may defeat the security of the systems quickly and efficiently. At the same time the security level of the systems can be further improved by subjecting them to various efficient combined attacks. Also new attacks may be designed from the existing cryptanalytic attacks with combinations of these attacks. Various attacks and their variations can be classified as mentioned below from which combined attacks may be designed [4,11, 12].

I. Main Cryptanalysis Techniques:

1. Related key crypt Analysis (RKC)
2. Differential Crypt Analysis (DC)
3. Linear Crypt Analysis (LC)

II. Variations in Differential Crypt Analysis (DC)

1. Truncated differential cryptanalysis (TDC)
2. Higher order differential cryptanalysis (HODC)
1. Square cryptanalysis (SC)
2. Impossible Differential Cryptanalysis (IDC)
3. Boomerang Cryptanalysis (BC)
4. Rectangle Cryptanalysis (RC)

III. Variations in Linear cryptanalysis

1. Multiple Linear cryptanalysis (MLC)
2. Non Linear Crypt analysis (NLC)
3. Bilinear cryptanalysis (BLC)

From the above mentioned individual cryptanalytic techniques the possible combinations of attacks have been tabulated in Table-I.

Table I. Possible combinations of attacks

RKC	DC	LC	Combined Attacks so far implemented	Other combinations for future study
	TDC	MLC	D-NLC	D-LC, D-NLC, S-LC, S-NLC, RK-D-LC, RK-D-NLC
	HODC			RK-RC, RK_BC, D-BLC, HOD-LC, D-L-BC,
	SC	NLC	RK-RC	D-BL-BC
	IDC			D-MLC, HOD-MLC, D-NL-BC, D_L_RC, RK-D-MLC
	BC	BLC	RK-BC	RK-D-L-BC, RK-BL-BC, RK-D-NL-BC, RK-D-NL-RC,
	RC			

The objective of these combined attacks should be accurate and reliable evaluation of various cryptographic systems listed Table-II.

Table-II. Cryptographic algorithms

Block Cipher	Hash Functions	MAC Algorithms
SHACAL-1	MD4	HMAC
SHACAL-2	MD5	NMAC
DES	HAVAL	
Triple DES	SHA-0	
AES	SHA-1	
Blowfish		
Variations of Blowfish		
RC6		
CAST		
IDEA		
Others		

From above combinations some of the combined attacks have been considered for review in present work.

3.1. The Differential-Linear Cryptanalytic Attack

Longford and Hellman [13] had proposed a combined attack known as the differential-linear cryptanalysis attack. It is a combination of differential cryptanalysis and linear

cryptanalysis. In this combined attack first differential characteristic of a part of block cipher is determined with probability 1. For the immediately following rounds of the cipher linear approximation is obtained. Thus a differential-linear distinguisher may be constructed to any chosen plain text. The complete description of this attack has been discussed in detail elsewhere [13].

3.2. The Differential-Nonlinear Attack

Kim [11] developed a new combined attack known as Differential-Nonlinear attack. Most of the procedure is same as the differential-linear attack introduced by Longford and Hellman [13] but the difference is in differential calculation. In this attack a non-linear distinguisher is designed and used instead of linear one. The nonlinear approximation is appended to differential characteristic to obtain the distinguisher.

3.3. The Square-(Non) linear Attack

In this section, the square-linear and square-nonlinear attacks that combine the square attack with the linear and nonlinear attacks, respectively will be discussed.. These attacks are similar to the differential-(non)linear techniques. The square attack was introduced when the block cipher SQUARE was pro-posed [14]. After this attack was introduced, it has been extended and generalized to the multiset attack [15] and the integral attack [16]. The basic idea behind this attack is the same as that of the higher-order differential attack [17]. It exploits a square characteristic whose input data consist of a set of plaintexts in which some bits are formed of a saturated set, and whose output data have a property like balancedness in some bits.

3.4. The Related-Key Differential-(Non) linear Attack

As the name suggests, the attack is combination of related key and differential-linear attack which was proposed by Hawkes [18]. Based upon related-key differential probability the attack may be related key and differential-linear attack or related key and differential- non-linear attack. The attack with related key differential probability is 1 and linear approximation bias is ½ , then the attack is related key and differential-linear attack. If bias is less than ½ and differential probability is less than 1 then the attack is related key and differential- non-linear attack. Kim [11].

3.5. Related-Key Rectangle and Boomerang attacks

Kim [11] proposed another combined attack namely Related-Key Rectangle and Boomerang attacks. To implement this attack Kim has devised different distinguishers based upon the type of differentials and number of related keys. Mainly three types of distinguishers were proposed [11].Type-1: Related key Differentials in first sub cipher and regular differential in second sub cipher.Type-2: Regular differential in first sub cipher and related key differential in second sub cipher.Type-3: Related-key differentials in both sub-ciphers.

3.6. Combined algebraic side-channel attacks

Side-channel attacks are powerful cryptanalytic techniques. Generally they target a specific implementation rather than an abstract algorithm. These attacks are implemented for security of embedded devices. Renauld et al proposed a new combined attack of cryptanalysis against block ciphers known as algebraic side-channel attack [19]. In this method a set of lower degree equations are used to express the block cipher and some physical information is provided. Hence, the algebraic cryptanalysis becomes very efficient to break various block ciphers.

3.7. Differential-Bilinear Attack

Biham et al proposed a new attack by combining a bilinear attack with differential attack yielding Differential-Bilinear Attack. The attack enciphers some pairs of plaintexts, and checks whether the computed pair of ciphertexts satisfy some bilinear approximation or not. This attack has been applied to eight round 5DES for a set of using 384 chosen plaintexts [20].

3.8. Higher-Order Differential and Linear combined Attack

It is combination of higher-order differentials with linear approximations. The XOR values of various sets of masked bits of elements of the cipher are compared with value with the XOR of the masked ciphertext bits in all of the encryptions. The attack uses the higher order differential to predict the XOR value of the sets of masked bits. The square-nonlinear attack was used to attack reduced round version of SHACAL-2 [20]

3.9. Combining the Boomerang Attack with Linear and Bilinear Techniques

A new attack was proposed by Kim [11] to exploit the β difference between the intermediate decryption values X3 and X4 of the encryptions whose ciphertexts are C3 and C4. If there is a differential-bilinear approximation for $E^{-1}_{0,}$ then the pair (X3, X4) has the required input difference, and thus, there is some bilinear relation between X3 and X4 whose probability not equal zero [20].

4. PROPOSED MODEL

In the present work a model was proposed for evaluation of a combined cryptanalysis attack on a cryptographic security system. The proposed system mainly consists of two modules: 1.Cryptographic Security System 2.Cryptanalysis attack. The cryptographic security system is designed to provide security to data through a complex double encryption

method. The cryptanalysis attack is a combination of individual attacks that has been used to defeat the designed cryptographic security system. The design of the proposed model is shown in fig.1.

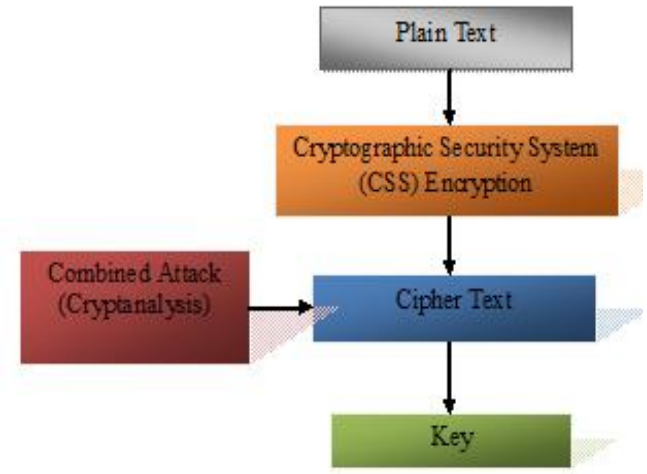

Fig.1 Model for Combined attack on a Security System

In the present model, as a first step a complex security system is designed in which the security of the system is improved by a double encryption scheme. In the next step, a Differential-Linear Cryptanalysis combined attack is designed based upon the features of the Whale Optimization Algorithm [21]. For the evaluation of the designed combined attack, it has been implemented on the proposed cryptographic security system. The outcome of the implementation shows the influence of combined attack over individual attacks.

4.1 Design of a Cryptographic Security System

In the present work, a novel duel encryption security system has been proposed by designing a double encryption algorithm in which two ciphers are combined together for encryption process that increases the security of an encryption system. The dual encryption algorithm is a combination of blowfish and DES algorithm. The encryption algorithms convert original plain text into ciphertext. Here, initial phase of blowfish encryption method is exploited after the second phase procedure of the encrypted data over again operates to DES encryption method. This duel encryption security system is subjected to a combined cryptanalysis attack using Differential-Linear cryptanalysis to find the keys. Thus in the present work the Differential-Linear cryptanalysis attack has been evaluated for a complex security system. The detailed procedure is described below. The proposed model is shown in fig.2.

4.1.1. Cryptographic Security System: The cryptographic security system components are Plain Text, Secret Keys, Blowfish cipher, DES cipher and Cipher Text. The design of the present cryptographic security system is shown in fig.2.The design components are described below.

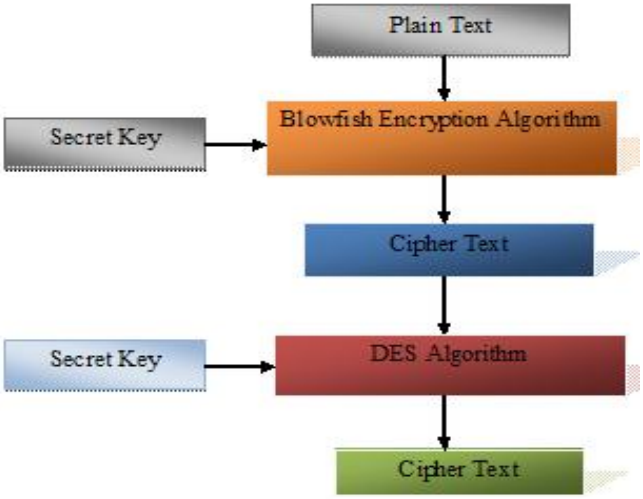

Fig.2 Model for Double Encryption Cryptographic Security System.

a) Blowfish algorithm

i.Blowfish Encryption method: The Blowfish algorithm has been adequately and extensively engaged in the rule of accomplishing the symmetric key cryptography. In the progressive technique, the Blow Fish strategy is sophisticatedly engaged for both the encoding and decoding. It separates a message up into constant length obstructs amid encryption and decryption. Blowfish incorporates 64-bit block measurement and length of the key from 32 bit to 448 bits. It comprises of P-array and four 32 bit S-boxes. This algorithm includes two subkeys arrays, for example, 18 of 32-bit P-array and four 256-section S-boxes. The S-boxes acknowledge 8-bit input and deliver 32-bit output. The encryption of data takes up the 16 round Feistel framework, among each enclosing endowed by a key dependent blend and a key dependent changeover. Every last one of the task means those of the XOR and the embellishments on 32-bit words in the blowfish technique. [22]

ii.Subkeys of BlowFish algorithm: An extremely large number of subkeys are deployed in the Blowfish technique, and they have to be invariably pre-computed before carrying out the encryption and decryption processes. A) P-array consists of 18 of 32-bit subkeys b)four 32 bit S-box contains 256 entries

iii. Encryption: The encryption signifies the assignment of renovating fundamental text into the difficult ciphertext. In the epoch-making method, the input employ is the 64-bit data, which, in the preliminary encircling, is separated into two 32

bit bisect, which is marked as the left halves (LH) and right halves (RH). In the original blowfish algorithm, the primary 32 bit left halves and the P-array carry out the XOR task and the result is delivered to the function (F) revealed in figure 3. Afterward, carry out the XOR task for equally left halves and the subsequently 32 bit right halves gracefully. This is chase by the transaction of both the result. Subsequently, the remaining of the encircling prolong until the accomplishment of the 16 round. The obtained result of this section is first level encryption output.

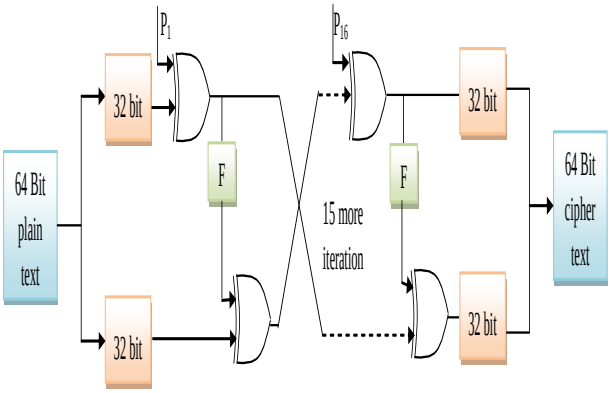

Figure 3: Blowfish algorithm process

iv.The process of F function:

The F function deploys four 32 bit S-boxes, with each one encompassing 256 entries. In the novel blowfish technique, the initial 32 bit left halves are subdivided into four 8 bit blocks such as m, n, o, and p.

The formula employing the F_t function is elegantly exhibited in the ensuing Equation 1.

$$F(L_H) = ((S_{b1,m} + S_{b2,n} \bmod 2^{32}) \oplus S_{b3,o}) + S_{b4,p} \bmod 2^{32} \quad (1)$$

The detailed working process of F function is shown below Figure 4.

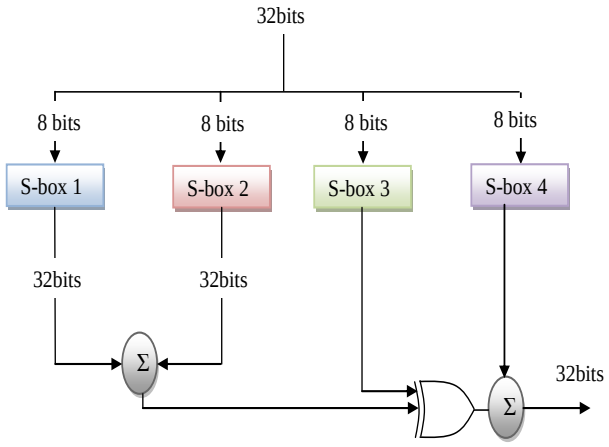

Figure 4: Working process of F function

v. Decryption: The decryption system of the blowfish method is alike to that of the encryption, even if in the earlier, the P-array is engaged in the repeal. The productivity of the blowfish method accumulates the folder which is arranged as the input of the second segment. By the support of the communal and personal keys, the folder experiences the task of encryption.

Blowfish Algorithm

Step 1: Read the 64bit input data X

Step 2: Input data X divided into two equal parts x_1 *and* x_2

Step 3: for $i = 0$ *to* 15

$x_1 = x_1\ XOR\ x_2$

$x2 = f(x_1)\ XOR\ x_2$

Step 4: Exchange x_1 *and* x_2

Step 4: Again Exchange x_1 *and* x_2 (go to step 4)

$x_1 = x_1\ XOR\ P_{18}$

$x_1 = x_1\ XOR\ P17$

Step 5: Combine x_1 *and* x_2

The S-boxes and P-boxes are initiated by standards from hex digits of pi. The variable length user-input key is afterward XOR by P-entries. Subsequently, a mass of zeros is encrypted, and this outcome is utilized for P1 and P2 access. This double encryption procedure oriented encrypted the confidence data to the protection principle. In experiment procedure, the third party offers the demand for encrypted data way the demand will be established or discarded and also the specified data in the cluster also recognized.

b) DES algorithm

After the blowfish based encryption process completed, again the encrypted data is given to the DES algorithm for encryption. DES is a type of symmetric key encryption algorithm [23]. This algorithm encrypts data in the blocks and the size of each block is 64 bits. That is the DES algorithm takes the input of 64 bits plain text and converts that input into 64 bits ciphertext. The key length of this algorithm is 56 bits. DES is based on two fundamental attributes of cryptography: Substitution (confusion) and transposition (Diffusion). In the initial step of encryption, the information in the block of 64 bit goes through initial permutation stage. After that, 16 rounds of permutation and substitution is performed [24]. The DES consists of 16 round. The last round of 16, the DES gives the outcome of 64-bit ciphertext. The steps involved in DES algorithm is explained below:

DES Procedure

Step-1: Consider a 64-bit plaintext block to the initial permutation (IP) function.

Step-2: After the permutation, the block is divided into two halves namely Left Plain Text (LPT) and Right Plain Test (RPT).

Step-3: Then, each LPT and RPT is given to the 16 round encryption process. Consider an independent key of 56 bit size each time.

Step-4: Then, use a 48-bit sub-key during each round which is generated from the 56-bit key.

Step-5: Extend RPT from 32 bits to 48 bits using expansion permutation

Step-6: Then, XOR the 48-bit key with 48-bit RBT and pass the value to the next step.

Step-7: Compress the 48-bit value obtained from the Step-6 to 32-bit using the S-box substitution.

Step-8: Permute the 32 bits block using P-Box Permutation

Step-9: Then, XOR the output of P-Box with the 32-bit LPT.

Step-10: Then, swap the 32-bit LPT and 32-bit RBT output quantities to create a pre-output which is the inverse of the initial permutation

Step-11: The output of the final permutation is the 64-bit ciphertext.

4.1.2 Combined Cryptanalysis attack

The Differential-Linear cryptanalysis attack is the combined cryptanalysis attack that has been used to defeat the above designed complex security system. The details of the Differential-Linear cryptanalysis have been described elsewhere [11, 13]. The technique has been briefly explained in this section.

i. Differential Cryptanalysis:

It is a Chosen Plaintext and Cipher text attack applied on block ciphers introduced by Biham and Shamir in 1990 [25] to exploit the high probability of certain occurrences of plaintext differences and cipher text differences into the last round of the cipher. Its initial design was extensively applied for block ciphers in particular for DES and its advancements. The basic and conceptual ideas of the algorithm with respect to DES are shown fig.5.

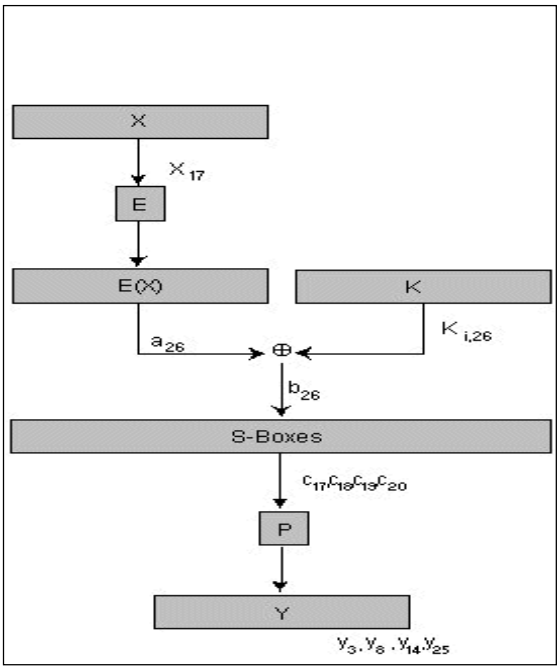

Fig.5 Differential cryptanalysis round function

In this technique the attacker has the choice to choose inputs and test the outputs to obtain the key. Let P and P' are two plain-texts and C and C' are corresponding ciphertexts of given block cipher. Let $\Delta P = P \oplus P'$ and $\Delta C = C \oplus C'$ be some fixed plaintext difference, and certain ciphertext differences respectively that may occur with high probability. This high probability is used to find the secret key using differential cryptanalysis. In differential cryptanalysis high probability differential are calculated for S-BOX of the block cipher. For this the concept of Substitution Permutation Net-work (SPN) is considered. Further to compute plaintext difference $\Delta P = P \oplus P'$ to the ciphertext difference $\Delta C = C \oplus C'$ products of high probabilities of differential of S-boxes used [25, 26]. The probability of a particular pair (ΔP ΔC) (known as differential) is $1/2^n$ where n is the number of bits of P. In such a system let $X = [X_1 X_2 ... Xn]$ be the input and $Y = [Y_1 Y_2 ... Y_n]$ be the output .Let Y′ and Y″ be the outputs for any two inputs X′ and X″ respectively. The input and output differences $\Delta X = [\Delta X_1 \Delta X_2 .....\Delta X_n]$ and $\Delta Y = [\Delta Y_1 \Delta Y_2 ..... \Delta Y_n]$ are computed by using bit-wise exclusive-OR for the pairs(X′ and X″) and Y′ and Y″ respectively. As discussed earlier to compute the differential characteristics, for each S-Box and for each input difference ΔX and output difference ΔY Difference distribution tables are computed. The high probabilities of (ΔX; ΔY) can be identified due to the weakness of the S-Box. By considering each S-Box is independent, all pairs of (ΔX; ΔY) of each S-Box the high probabilities are traversed and combined from first round to second last round. Hence, It is possible to find some bits of last round sub key by obtaining the second last round with sufficient high probability p_D. Hence we obtain Target Partial Subkeys (TPS).The mechanism of the Differential cryptanalysis is implemented in two steps as follows [4, 25-27].

ii. Differential cryptanalysis procedure

(i) Computation of Distinguisher

(ii) Key Recovery.

(i) Computation of Distinguisher:

1. Construct Difference distribution table for each S-Box for pairs of (ΔX; ΔY).
2. Compute probability of the each for pairs of (ΔX, ΔY).
3. Traverse the S-Boxes from first round till second last round of the cipher to obtain the differential probability p_D.
4. Now, the differential probability p_D is the distinguisher.

(ii)Key Recovery:

1. Using ΔP obtain plaintext/ciphertext pairs (N).
2. For each TPS the following steps are followed:

   i Set COUNT =0

   ii Perform the partial decryption for each Ciphertext (CT) (for i =1to N).

   (a) CT (i) ⊕ TPS*

   (b) Traverse through S-boxes backward to get bits into the last Round

   (c) Verify the equality of value of the computed partial decryption and the differential characteristic.

   (d) In case of equality COUNT is incremented. Also the partial sub key value with largest COUNT is considered for each TPS.

3. Construct a table for partial sub key values and corresponding probability P = (COUNT / N).
4. If P = p_D, Exact TPS is obtained.

ii. Linear Cryptanalysis

Linear cryptanalysis is known plaintext attack which is implemented successfully on various block ciphers like DES, FEAL, Serpent etc [28-30]. This attack obtains highly probable linear expressions that relate plaintext, ciphertext and sub key bits. The details of the linear crypt analysis are available in the literature [26-30]. Let u be bits of input and v be bits of output with high and low probabilities and form a linear expression. If P_L is probability to hold the expression, then bias probability is defined as $\varepsilon = |p_L - 1/2|$. If $P_L > 1/2$, then the expression $X_{i1} \oplus X_{i2} \oplus X_{i3} \ldots \oplus X_{iu} \oplus Yi_1 \oplus Y_{i2} \oplus Y_{i3} \ldots \oplus Y_{Yv} = 0$ is said to be linear approximation otherwise it is known as affine approximation. When ε is large, the system will be weak and may be vulnerable to attack. To attack the cipher a linear approximation table (T) is constructed. The general principle for linear crypt analysis is shown in fig.35.

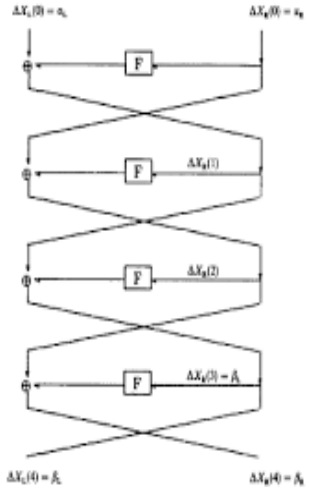

Fig.35 Linear cryptanalysis principle

iii. Linear cryptanalysis Procedure

1. Compute T for each S-Box of size nxm.
   i. Consider the linear relations $a.x = a_1x_1 \oplus a_2x_2 \oplus \ldots\ldots \oplus a_nx_n$ and $b.y = b_1y_1 \oplus b_2y_2 \oplus \ldots\ldots \oplus b_my_m$ for input and output. Here a, b represents n and m bit numbers respectively for $0 \le a \le 2^{n-1}$ and $0 \le b \le 2^{m-1}$.
   ii. Obtain p_L from the Table T by dividing the elements of linear approximation table by 2^n.
   iii. Compute p_L of each S-Box for each round with the expression $\varepsilon = |p_L - 1/2|$.
2. Store the linear trail for the elements with highest bias probability ε in each round till second last round.
3. Compute the expected bias probability p_D on calculating ε_i for each round and at last probability of $p_D(x_1 \oplus x_2 \oplus \ldots\ldots \oplus x_n = 0) = 1/2 + 2^{k-1} \pi_{i=1tok} \varepsilon_i$ where $\varepsilon_{1.2\ldots.k} = 2^{k-1} \pi_{i=1tok} \varepsilon$.

ii) Obtaining the secret key

1. Produce M pairs of plaintext (PT) and ciphertext (CT)
2. For each TPS from 2^n possibilities n-bit TPS, do the following:

   i Set COUNT=0

   ii For each CT(i) for i = 1 to M do the partial decryption

   (a) CT (i) ⊕ TPS

   (b) Run S-boxes backward to get bits into the last round

   (c) XOR the bits of PT (i) with XOR of the last round bits of S-boxes obtained in step (b)

   (d) If the result of step (c) is 0, then increments COUNT

   iii |Bias| = |COUNT- M/2 |

3. Construct a table for all sub keys corresponding to. |Bias|

4. From the table, if |Bias| = 0 then TPS is not a correct one. If |Bias| = Expected value, then the TPS is correct.

iv. Combined Differential-Linear cryptanalysis attack

In the present work the differential-linear cryptanalysis attack has been considered for combined attack incorporating the features of the whale optimization algorithm. The used attack is a combination of linear and differential cryptanalysis attacks. The whale optimization algorithm [21] is a newly proposed meta-heuristic that is inspired by the bubble-net hunting technique of humpback whales and is mainly used for the key evaluation process. First the optimal key is obtained using proposed method. Then a particular key and corresponding encrypted data are given as input of the attack that decrypts the information. This procedure is implemented in the following steps.

Step 1: Initialization: Initialization is an important process for the entire optimization algorithm. The aim of this step is to break the system with out any key information. For that n number of keys of size of 64 bit are randomly generated which are the combinations of 0's and 1's as shown in figure 4.

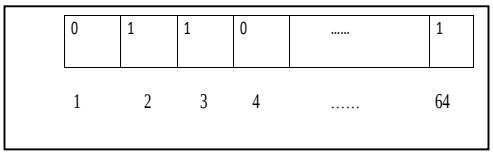

Figure 4: Representation of solution

Step 2: Fitness calculation: Now it is required to compute the optimal key by calculating the fitness of the input solution obtained in the previous step using a fitness function. The selected key and the encrypted documents are given to the double attack. The Differential-Linear cryptanalysis is for breaking the system. The fitness function checks, how much meaningful information obtained using each key. The maximum amount of meaningful information key is considered as the best key.

Step 3: Encircling the prey strategy: In encircling prey, at first, the whales have monitored the location of the prey (fishes). Then, the whales are encircling the prey. The prey, very close to the whales is considered as the best candidate solution. Once the best hunting agent is identified, the other whales are updating their position towards the best hunting agent. The encircling process is given in equation (2).

$$D = \left| U.Y^*(k) - Y(k) \right| \quad (2)$$

$$Y(k+1) = Y^*(k) - V.D \quad (3)$$

Where $_{U,V}$ are coefficient, k denotes the current iterations, $Y^*(t)$ is a position vector of the best solution, Y(t) represents the current position vector and $|.|$ represents an absolute value. The coefficient vectors $_{U,V}$ are calculated as follows:

$$V = 2.v.r - v \quad (4)$$

$$\vec{U} = 2.r \quad (5)$$

Where, v is a variable linearly decrease from 2 to 0 over the course of iteration and r is a random number [0, 1].

Step 4: Bubble-net attacking strategy (exploitation phase): In order to model the bubble-net behaviour of humpback whales mathematically, two improved approaches are designed.

1. Shrinking encircling mechanism: This behaviour is achieved by decreasing the value of an in the equation (4). Note that the fluctuation range of $_V$ is also decreased by v. In other words $_V$ is a random value in the interval [−v, v] where v is decreased from 2 to 0 over the course of iterations. Setting random values for V in [−1, 1] the new position of a search agent can be defined anywhere in between the original position of the agent and the position of the current best agent.

2. Spiral updating position

Here, at first, the humpback whales search the prey and then calculate the distance from themselves to the prey. Then, the humpback whales move with a conical logarithmic spiral motion to prey on the fish herds. Each humpback whale is proposed to update its position according to the spiral flight path. This behaviour is mathematically expressed as follows

$$Y(k+1) = D'.e^{bt} * \cos(2\pi k) + Y^*(k) \quad (6)$$

$$D' = \left| Y^*(k) - Y(k) \right| \quad (7)$$

Where; b is a constant for defining the shape of the logarithmic spiral, t is a random number in [−1, 1], and "*" is an element-by-element multiplication. Note that humpback whales swim around the prey within a shrinking circle and along a spiral-shaped path simultaneously. To model this simultaneous behaviour, we assume that there is a probability of 50% to choose between either the shrinking encircling mechanism or the spiral model to update the position of whales during optimization. The mathematical model is as follows:

$$\vec{X}(t+1) = \begin{cases} X^*(i) - \vec{V}..\vec{D} & if\ R < 0.5 \\ \vec{D}'.e^{bk}.\cos(2\prod k) + \vec{X}^*(t) & if\ R \geq 0.5 \end{cases} \quad (8)$$

Where, R is a random number in [0, 1]. In addition to the bubble-net method, the humpback whales search for prey randomly.

Step 5: Search for prey (Exploration period): To get the global optimum values updating has done with randomly chosen search agent rather than the best agent

$$\vec{D} = \left| \vec{C}.X_{rand} - \vec{X} \right| \quad (9)$$

$$\vec{X}(t+1) = X_{rand} - \vec{V}.\vec{D} \quad (10)$$

Where, X_{rand} , is a random whales current population.

Step 6: Termination: The algorithm discontinues its execution only if a maximum number of iterations are achieved and the solution which is holding the best fitness value is selected. Once the best fitness is attained by means of algorithm, selected key is given to the decryption process.

5. EXPERIMENT

The experiment is performed by implementing algorithm for the proposed model as shown in the diagram.

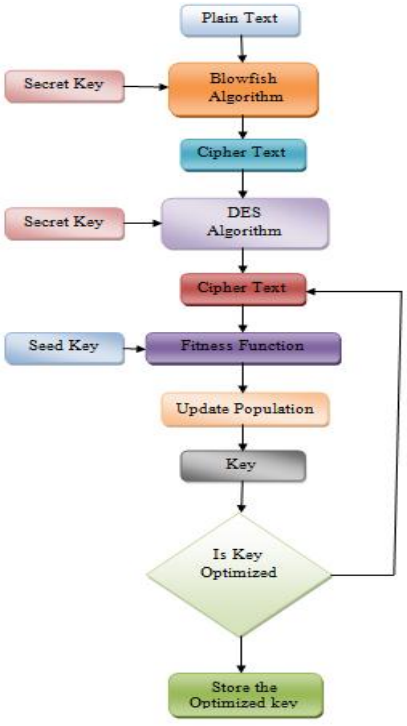

Fig.5 Algorithm for the proposed model

Step-1: Input secret key and plaintext to first encryption process of the cryptographic security system (Blowfish).

Step-2: Input another secret key and obtained cipher text from Blowfish algorithm to the second encryption process (DES).

Step-3: Input the seed key randomly and cipher text obtained from second encryption process to the Fitness Function to obtain the new key.

Step-4: Check whether the new key is optimal. If it is optimal that is real-key for breaking the cryptographic system. Else go to Step-5

Step-5: Input new key and cipher text to the Fitness function to repeat the steps from Step-3 to Step-4.

This proposed algorithm has been implemented in Java programming language with JDK 1.7.0 in a windows machine containing configurations Intel (R) Core i5 processor, 1.6 GHz, 4 GB RAM. The operating system platform is Microsoft Wnidow7 Professional. The experimental result and the performance of the proposed method have been discussed in the next section.

6. RESULTS AND DISCUSSION

In order to evaluate the Differential-Linear cryptanalysis attack on the proposed cryptographic system **key optimization time** is taken as a parameter. It denotes the time taken to compute the optimal key to break the cryptographic system for a fixed size of data. In the present work, four sets of data with several sizes have been considered for three cryptographic systems for evaluation and comparison. The three cryptographic systems are: 1.Present Model 2.Blowfish 3.DES. For the Present model Differential-Linear cryptanalysis with the features of whale optimization algorithm has been used. For the other two models the general Differential-Linear cryptanalysis proposed by Longford and Hellman [13] has been implemented. The computed optimization times for 16th round of all the three systems have been presented in Table-III.

Table-III: Key optimization time (In power of 2)

Key optimization time (In power of 2)			
File size	Proposed	Blowfish	DES
5kb	$2^{12.01}$	$2^{12.42}$	$2^{12.89}$
10 kb	$2^{12.21}$	$2^{12.84}$	$2^{13.00}$
15kb	$2^{12.51}$	$2^{13.73}$	$2^{13.94}$
20 kb	$2^{13.12}$	$2^{13.80}$	$2^{14.10}$

From the Table-III the following can be observed.

1. The Key optimization time is ranging from 2^{12} to 2^{14}.
2. In all three cryptographic security systems the Key optimization time is increasing with respect to file size.
3. Similarly for a particular file size the Key optimization time is increasing from the proposed model to DES through Blowfish. This is true for all four files ranging from 5kb to 20kb.
4. It is quite evident from the table that in terms of key optimization time the present model is showing better performance when compared with the other two cryptographic systems. The explicit key optimization times have been presented for all sets of files and cryptographic in Table-IV.

Table IV: Explicit key optimization times

Key optimization time			
File size	Proposed	Blowfish	DES
5kb	4564	8485	9645
10 kb	6235	9264	9645
15kb	8954	12487	13878
20 kb	10446	13544	14553

The key optimization time is acquired for various file sizes. They are then compared to the proposed method, Blowfish algorithm, and DES algorithm. 5kb, 10kb, 15kb, and 20kb are the sizes of the files considered for the comparison. The key optimization time acquired by utilizing the proposed method is 4564, it is 8485 when utilizing the Blowfish algorithm and 9645 when utilizing DES algorithm when the file size is set to 5kb. Moreover, the key optimization time acquired by utilizing the proposed method is 6235, it is 9264 when utilizing the Blowfish algorithm and 9645 utilizing DES algorithm when the file size is set to 10kb. When the file size is set as 15kb, the key optimization time acquired by utilizing the proposed method is 8954, it is 12487 when utilizing the Blowfish algorithm and 13878 utilizing DES algorithm. At the point when the file size is set as 20kb, the key optimization time acquired by utilizing the proposed method is 10446, it is 13544 when utilizing the Blowfish algorithm and 14553 when utilizing DES algorithm. In general, for all the file sizes, the proposed method performed better when compared with Blowfish algorithm and DES algorithm. The graphical representation of the performance analysis based on key optimization time by varying file size is shown in the following figure 7.

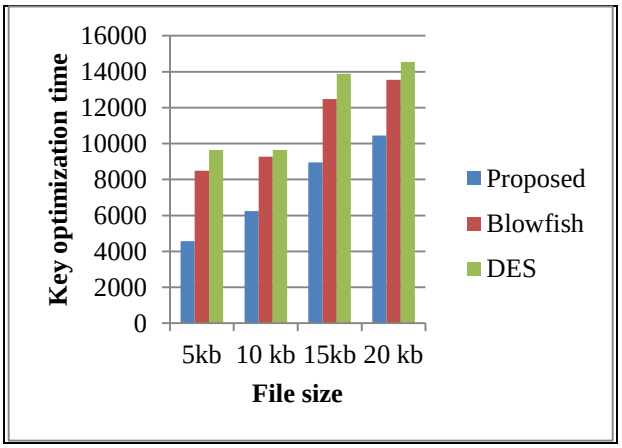

Figure 7: Performance comparison based on key optimization time

Logarithmic key optimization time variation for each file size has been shown in fig.8. Similarly, Logarithmic key optimization time variation for each model with file size has been shown in fig.9. From fig.7 to fig.9 it is very clear that the present model has better performance when compared with other models. The reasons for the better performance of the present model are (i) Differential-Linear Cryptanalytic Combined attack. (ii) Incorporation of Whale optimization algorithm features in Differential-Linear cryptanalysis.

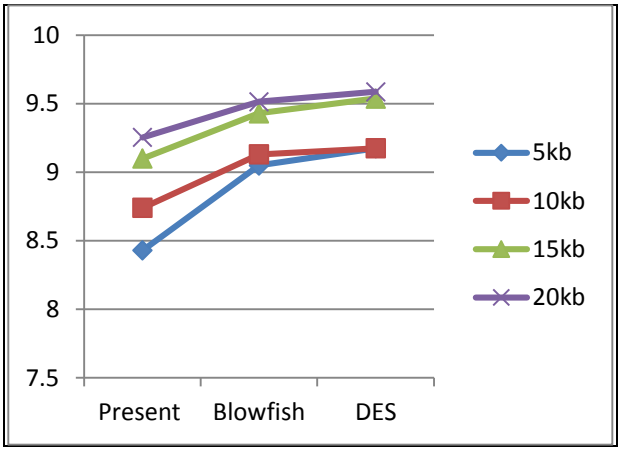

Fig.8. Variation of Key optimization time for each file size

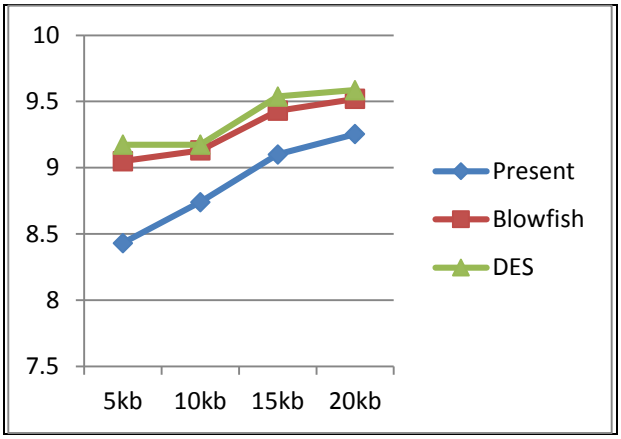

Fig.9 Variation of Key optimization time for all models with file size

7. CONCLUSION

The cryptography security system and cryptanalysis approaches have been implemented in the platform of JAVA. The proposed system was developed based on three modules such as cryptography security system, security blocking system and optimal security system. Here, the dual encryption algorithm was designed and performances are analyzed. Moreover, whale optimization algorithm with cryptanalysis attacks was used to generate key and choice the correct key (secret key) to break the ciphertext and recover the plain text.

Acknowledgements

Dr. B. Srinivasa Rao is very much thankful to Dr. L. Pratap Reddy, Professor, Department of Electronics and

Communication Engineering, JNTUH, Hyderabad for his supervision of my research work and valuable suggestions. He is also thankful to the management of Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad for encouragement and cooperation.

REFERENCES

[1] Rescorla E.**,** SSL and TLS: Design and Building Secure System, Addison Wesley Professional, U.S.A. 2001

[2] Ooi S.K. and. Vito C.B., Cryptanalysis of S-DES, University of Sheffield Centre, Taylor's College, 1st April 2002

[3] Noorman, J., Van Bulck, J., Muehlberg, T.J., Piessens, F., Maene, P., Preneel, B., Verbauwhede, I., Goetzfried, J., Mueller, T., and Freiling, F., "Sancus 2.0: A Low-Cost Security Architecture for IoT Devices," ACM Transactions on Privacy and Security PP (99), 32 pages, 2017.

[4] Khurana M. and Kumari M., Variants of Differential and Linear Cryptanalysis, International Journal of Computer Applications, 131, 18, pp20-28, 2015

[5] 5.Goyal R. and Khurana M., Cryptographic Security using Various Encryption and Decryption Method I.J. Mathematical Sciences and Computing, 3, 1-11 2017

[6] http://www.crypto-it.net/eng/attacks/index.html

[7] Stallings W., Cryptography and Network Security, Ed.4, Pearson prentice Hall, 2006

[8] Forouzan B. A., Cryptography and Network Security, Tata Mc Graw-Hill, Special Edition, 2007.

[9] Schneier B., Applied Cryptography, Ed.2, John Wiley & Sons, 1996

[10] https://www.tutorialspoint.com

[11] Kim, J., Combined differential, linear and related-key attacks on block ciphers and MAC algorithms. PhD Thesis, Katholieke Universiteit Leuven, 2006.

[12] Rao B.S., A Review on Combined Attacks on Security Systems, IJAER (RIP) 2018(Under Production).

[13] Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis, in Desmedt, Y. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 17–25. Springer, Heidelberg (1994)

[14] J. Daemen, L.R. Knudsen and V. Rijmen, The Block Cipher Square, Proceedings of FSE 1997, LNCS 1267, pp. 149-165, Springer-Verlag, 1997

[15] Liu Y., Gu D., Liu Z., and Li W., Impossible Differential Attacks on Reduced Round LBlock, in ISPEC 2012, LNCS 7232, pp. 97-108, 2012(Springer-Verlag Berlin Heidelberg)

[16] Knudsen L.R. and. Wagner D, Integral Cryptanalysis, Proceedings of FSE 2002, LNCS 2365, pp. 112-127, Springer-Verlag, 2002.

[17] Wagner D., The Boomerang Attack., in Knudsen R.L., editor, Fast Software Encryption – FSE'99, volume 1636 of Lecture Notes in Computer Science, pages 156–170. Springer Verlag, 1999.

[18] https://pdfs.semanticscholar.org

[19] Biham E., Dunkelman O. and Keller N.: New Combined Attacks on Block Ciphers in Gilbert H. and Handschuh H.(Eds.): FSE 2005, LNCS 3557, pp. 126–144, 2005

[20] Mirjalili S. and Lewis A., The Whale Optimization algorithm, Advances in Engineering software, 95, pp51-67 2016

[21] Schneier B, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings. Springer-Verlag: 191–204. Archived from the original on 2014-01-26 (1993)

[22] Walter Tuchman, A brief history of the data encryption standard, Internet besieged: countering cyberspace scofflaws. ACM Press/Addison-Wesley Publishing Co. New York, NY, USA. pp. 275–280 1997

[23] Amazon Web Services, AWS. Online at: http://aws. amazon.com.

[24] Biham E. and Shamir A., Differential Cryptanalysis of DES-like Cryptosystems, Advances in Cryptology, LNCS 537, pp. 2-21, Springer-Verlag, 1990.

[25] Heys M. H., A Tutorial on Linear and Differential Cryptanalysis. http://www.cs.bc.edu

[26] Tardy-Corfdir A. and Gilbert H., A Known Plaintext Attack of FEAL-4 and FEAL-6. In Feigenbaum J. (Eds), Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings, volume 576 of Lecture Notes in Computer Science, pages 172–181. Springer, 1991

[27] Matsui M., Linear Cryptanalysis Method for DES Cipher, in Helleseth T., (Eds.), Advances in Cryptology - EUROCRYPT '93, Lecture Notes in Computer Science, 765, pp 386–397, Springer, 1993

[28] Cho J.N, Hamelin M. and Nyberg K.., A New Technique for Multidimensional Linear Cryptanalysis with Applications on Reduced Round Serpent, in Lee P.J. and Cheon J.H.,(Eds.), Information Security and Cryptology - ICISC 2008, 5461, Lecture Notes in Computer Science, pp383–398.,Springer, 2008.

[29] Hakala R.M. and Nyberg K., Linear Distinguishing Attack on Shannon, in Mu Y., Susilo W., and Seberry J. (Eds.), information Security and Privacy, Lecture Notes in Computer Science, 5107, pp 297–305, Springer, 2008

[30] Nakahara Jr. J., Preneel B., and Vandewalle J., Linear cryptanalysis of reduced-round versions of the SAFER block cipher family, in Schneier B.(Eds.), Lecture Notes in Computer Science, 1978, pp 244–261, Springer, 2000