VOL. 12, NO. 9, MAY 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

INTRODUCING A NEW METHOD IN CRYPTOGRAPHY BY USING DYNAMIC P-BOX AND S-BOX (DPS METHOD) BASED ON MODULAR CALCULATION AND KEY ENCRYPTION

M. Zobeiri and B. Mazloom-Nezhad Maybodi
Faculty of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, Iran
E-Mail: m_zobeiri@sbu.ac.ir

ABSTRACT

Through the passage of time, computer technology has been considered as a pivotal element in human life. Because of this point, it is more evident that information security gained a prominent position. Cryptography is utilized to secure information in a way that information became impenetrable under attack. In this paper, a new method of encryption is introduced according to dynamic P-Box and S-Box based on modular calculation and key encryption. P-Box is a tool that changes the order of the input bits and they appear in the output. In this case, the key is order transmission of input bits in output bits. An S-box is a basic component which performs substitution. In this paper, a new method for the production of encryption method with the help of modular computing is introduced. This method called DPS method which in its P-boxes and S-boxes the order of the input bit transfer in output, are the function of the encryption key.

Keywords: block cipher, dynamic P-box and S-box, modular computation, symmetric key.

1. INTRODUCTION

Successful encryption algorithm is an algorithm that is resistant to breaking attack. The proposed algorithm of the present study is classified as a symmetric encryption algorithm. Each system of symmetric encryption must have two characteristics i.e. "Confusion" and "Diffusion" at the highest possible level. These two characteristics were introduced and used in 1949 by "Claude Shannon"[1]. In theory, encryption system should distribute the statistical indices of the plaintext on the whole of the encrypted text. In other words, the encryption system should never transfer statistical characteristics of the text to the encrypted output in any way. Accordingly, when you analyze the output of an encrypted system, there should not be any correlation among output bits, key and the bits of the text.

A text of any length, including text characters are given to the algorithm as the plaintext. As this method is performed in a block cipher, in each step, some of the characters which have not been encrypted yet, are chosen by the algorithm and they will be returned to one and zero during a process. In this process which will be presented in the section two, a certain permutation algorithm is used to distribute statistical characteristics normally in this section.

In the third part, the suggested algorithm is completed and the cipher text is made. In the fourth part, the procedure of generating symmetric key encryption is introduced. And at the end, in Section fifth, the function of the proposed algorithm and the obtained results of the algorithm will be discussed.

2. CHARACTERS BLOCKING AND CONVERSION OF EACH CHARACTER BLOCK TO ZERO AND ONE WITH DISTRIBUTED STATISTICAL PROPERTIES

One of the common methods of attacking the encrypted text is using letters statistics and their combination in the text[2, 3]. In the operation of code cracking (code cracking is decryption without having the encryption key), the cipher text is analyzed statistically and based on the frequency of the characters, the two-letter and three-letter combinations, some of the characters are specified. Uniform distribution of characters and their combination in the input text, are very important and influential in the resistance of the text against attack. Regarding aforementioned points, in the modern system of cryptography, the data are intertwined in several stages called round. In these stages, besides using powerful performance of Xor, it draws on the numerous constructive elements.

One of the simplest encryption tools, which are used in combination with other components in symmetrical modern encryption methods, is P-BOX. In a short statement, P-BOX is a tool that changes the order the bits and input characters as they appear in the output. Obviously, the P-BOX will not change the number of bits and characters. The other widely used encryption tool is S-BOX is. S-BOX for any n-bit number, as injective function, writes another numerical n-bit. This substitution is done in line with the designer mapping table.

In many encryption methods fixed tables are employed for substitution and permutation. The reason of this is, if the tables are not fixed the permutation and the substitution should be clarified in the encryption key. This work will cause the inappropriate length increase of encrypting key[4-6]. For blocking and uniform distribution the characters of plaintext, the following procedures are followed:

2.1 Blocking of plain text file

The suggested method is classified as block encryption methods. Input file for encryption, is a text file. At each step of algorithm the first 128 characters from among the characters that have been chosen for encryption, is selected as an input block to the algorithm.

As will be explained in the next section, the algorithm can be employed in various versions, depending on which version runs the length of the input block in terms of the number of characters can also accept the other amounts.

While all the characters of the plaintext aren't submultiple of 128, some random characters will be added the end of plaintext until the length of the final block becomes 128. The number of characters in the final block of plaintext before adding random characters is called$n_{LB(Last\ Block)}$. It is obvious that,$0 \leq n_{LB} \leq 127$, and the amount of n_{LB}in encryption key will be located until the time of the decryption counted accurately.

2.2 Permutingof input block characters

In the suggested encryption method, permutation and substitution table is not fixed; this would have increased the complexity of this algorithm and its ability to resistant to the attacks. In other words, the permutation and substitution will be a function of the encryption key. For having no increase in adverse encryption key, in this algorithm the P-BOX which is based on modular computing is utilized.

In this method [7] the length of the input block is n_1,which its 'houses are set to be permuted. In this method, the permutation of the input houses is based on four fixed numbers i.e. A',B',C',D'. These numbers are located as a code in the encryption key. The houses of input block are numbered from 1 to n_1. One output block with $n_1$house is considered. At each stage, the number of one of the input block house which is not already selected, based on its key is selected and its content in the first empty output block is located. This work will be repeated n_1 times, until the permutation operation of all the input blocks occurred. This function of permutation is indicated by $F_P(Input\ Block, Key_P, n_1)$in which $Key_P$is include four constants as A', B', C', D'. Key_Pwill be used in the encryption key, the length of the input block is n_1.

As mentioned in section 2-1, 128 characters of the plaintext are selected, so n_1= 128. These characters are situates one by one in the input block houses. The input block is called IB_{128ch}. Using the P-Box algorithm, which was introduced in this section, requires four inputs A', B', C' and D' to permute input block houses. Each of these numbers are selected arbitrarily from zero to 8191 and Key will be $Key_P = \acute{A} + \acute{B} + \acute{C} + \acute{D}$. $Key_P$is 52 bits and its amount is placed in symmetric encryption key. Characters permutation in input block are based on the $F_P$function and the result of this permutation is called $IB_{p-128ch}$. This variable consists of 128 input characters which are permuted based on key.

It should be noted that because of numbers A', B', C', D' are identical for all the 128 characters block which are supposed to be encrypted, a fixed permutation table is created for all the blocks. Before using the algorithm through the encryption key, we calculate the 128 characters permutation table, so calculations of permutation table that has a high computational load is done only once, and it won't become an extra load on the suggested encryption algorithm.

$$IB_{p-128ch} = F_P(IB_{128ch}, Key_P, 128) \quad (1)$$

2.3 Substituting input block characters from the previous stage

By permuting characters which was done in the previous section in accordance with encryption key, the place and order of all the characters are completely scrambled. Thus there is no correlation of 2 or 3 characters in the present text, but it can be statistically analyzed with single character. Because of this point, in this section, in accordance with the suggested algorithm, each character in terms of its location will turn to other character.

Input block of this stage is $IB_{p-128ch}$that includes 128 houses that each house is of a character. For each of the houses of this block, a number between zero and 127 is selected. This number is added to ASCII code of character in that house, and it turns characters into other characters. For example, if in the first house character "I" is located and the number which is added to ASCII code is 3, this character will turn into 'L'.

The amount of each number which is added to every home can be considered as both constant number and dependent encryption key. To increase the complexity, characters substitution based on the encryption key is done in accordance with an algorithm that only 12-bit encryption key is allocated to it. The above procedure is as follow.

Number of E' is a 12-bit number and it is selected between 0 and 4095 arbitrarily which is located in the encryption key. E number is equal to E'+31. This ensures that the least amount of E is equal to 31. To substitute the characters of input block based on their position, in K-th step; based on equation2 the level of change is determined for K-th houses.

The amount of change in the character of k =

$$(E - K)^{(E+K)} \text{mod } 127 \quad (2)$$

The change in the k-th character will be a number between zero to 126 and this amount is added to the value of k-th ASCII code of character in house block $IB_{p-128ch}$. If the number was less than or equal to 127, the character is identified, otherwise the rest of the number is divided by 128 which can clarify the intended character.

The reason of computing the rest of number divided by 127 in equation 2 is that 127 is a prime number. Thus, in computation of the rest number, the features of modular computation can be employed, for this reason the amount of computation is reduced obviously.

It should be noted that like 2-2, the number changes in every house block $IB_{p-128ch}$ for all blocks that are supposed to be codified (encrypted) are identical and once this calculation will be done; therefore, overhead computation is not suggested for this algorithm. The new block which is the result of new characters substitution, is a 128 characters block and the name of this block is $IB_{s-p-128ch}$.

2.4 Replacing any character with its ASCII code and permuting generated bits

At the end of stage a 128 characters block names $IB_{s-p-128ch}$is obtained. The characters which are in the house are depending on IB_{128ch} blocks of plaintext and the encryption key (A', B', C', D', E'). Statistically speaking, the obtained results, indicates a uniform distribution among the characters. This point will be discussed in the analysis of the algorithm.

To proceed with the suggested method, we need to convert these characters into binary numbers (base 2). In turn of each character one binary number should be included. The ASCII code is utilized for this conversion. In other words, for each in the house $IB_{s-p-128ch}$ an 8-bit code is replaced. The new block will be 1024 = 8 × 128 bits. This block is called IB_{1024B}.

To increase the complexity of the algorithm once again the P-BOX algorithm introduced in Section 2.2 is employed:

$$IB_{p-1024B} = F_P(IB_{1024B}, Key_{P1}, 1024) \quad (3)$$

Where $Key_{P1}$is a completely arbitrary 52-bit key, includes four 12-bit numbers $(A'_1, B'_1, C'_1, D'_1)$and that derived from the encryption key of cryptographic operations. The steps of section 2 are shown in Figure-1.

Section Two		start	Creation Block after step	Number of Block homes
		↓		
	Plain text →	Blocking of plaintext file	IB_{128ch}	128
		↓		
	$Key_P = f_1(Encription\ Key)$ →	Permutation of Input block	$IB_{p-128ch}$	128
		↓		
	$E = f_2(Encription\ Key)$ →	Substitution of Input block	$IB_{s-p-128ch}$	128
		↓		
		Replacement of any character with its ASCII code	IB_{1024B}	1024
		↓		
	$Key_{P1} = f_3(Encription\ Key)$ →	Permutation of generated bits	$IB_{p-1024B}$	1024

Figure-1. Characters blocking and conversion of each character block to zero and one is competed with distributed statistical properties

3.COMPLETING THE CRYPTOGRAPHY ALGORITHM AND MAKING THE CIPHER TEXT

At the end of section two, a 1024 bits block names $IB_{p-1024B}$is obtained and this block has distributed statistical properties. Encryption methods should be strong against breaking code attacks, so in this section some standard functions like xor and permutation are adding to algorithm. This function leads moreDiffusion and Confusion in proposed method and causes stronger encryption method. At the end of this section, the cipher text will be ready.

3.1 XOR operation of input block bits with the numerical sequence which is function of encryption key

In cryptographic systems Xor function is a tool for increasing both Diffusion and Confusion. "Claude Shannon" in 1949 proved that if you choose a totally random key, after Xor key with the original message, any information or statistical index of encrypted text will not be observed. Because if every bit of the original text (with any probability and any amount of statistical dependence on the rest of the bits) is obtained, which is completely independent and random.

In the following of encryption algorithms, block $IB_{p-1024B}$with a 1024-bit block which is derived from encryption key becomes Xor; this work will increase the

resistance of algorithm against attacks. 1024-bit block that is calculated from code is called Pad_{1024}.

$$IB_{Xor-p-1024B} = (Pad_{1024})\ Xor\ (IB_{p-1024B}) \quad (4)$$

To calculate Pad_{1024} the below procedure is followed:

Step1. Arbitrary number of F with the length of 64 bits is selected. This number will be located in encryption key.

Step 2. Number of G with the length of 12 bits is selected. This number will be located in encryption key.

Step 3. Pad 1024-bit block is defined as follows:

We divide the Pad block to 16 bit blocks called pad (0), pad (1), pad (2), ... (Figure-2).

Pad=	Pad(0)	Pad(1)	…	Pad(15)
	1-64	65-128		961-1024

Figure-2. Forming the bits of Pad block.

Pad "i" is equal to "i" load a 64-bit shift to the right F number. Therefore, Pad (0) = F and the other Pad (i) are calculated in terms of rotation to the right of the F.

Step 4. Random number G is calculated based on 10 and number m is defined as follow: m = G + 0.9. The number m is a full non-square rational number. The number m' is equal to $\sqrt{m}$. Number m' is an irrational number; therefore the number of its decimals is unending. Remove the correct part of m' and the rest number is called m''$(m'' = m' - [m])$.The number m'' is turned to be the basis for 2. Since the number of decimal m " are unending, thus the number of decimals m " in the basis of 2 will be numerous. We should select 1024 first digit after the decimal m " in basis of 2 and call Pad'.

$$m'' = (0.a_1a_2a_3 \cdots a_{1024}a_{1025} \cdots)_2 \quad (5)$$

$$Pad' = a_1a_2a_3 \cdots a_{1024} \quad (6)$$

Proof: $\sqrt{m}$ is an irrational number

Reduction ad absurdum: $\sqrt{m}$ is a rational number

$$c = \sqrt{m} \in Q \rightarrow c = \frac{a}{b};\ (a,b) = 1;\ a,b \in N$$

$$\left.\begin{matrix} m = c^2 \\ m = G + 0.9,\ G \in N \end{matrix}\right\} \rightarrow G + \frac{9}{10} = \frac{a^2}{b^2} \rightarrow \begin{cases} 10G + 9 = \frac{10a^2}{b^2} \\ 10G + 9 \in N \end{cases}$$

$$\rightarrow \left.\begin{matrix} \frac{10a^2}{b^2} \in N \\ (a,b) = 1 \end{matrix}\right\} \rightarrow b^2 | 10 \rightarrow b = 1 \rightarrow 10G + 9 = 10a^2$$

$$9 = 10(a^2 - G) \rightarrow 10|9 \text{Paradox} \rightarrow \sqrt{m} \in Q'$$

Step 5. Pad_{1024} is obtained as follow:

$$Pad_{1024} = (Pad) Xor\ (Pad') \quad (7)$$

It should be noted that Pad_{1024} is obtained only one time in this algorithm and it is fixed in the code of the other blocks. Thus, the calculations are not an extra load on the algorithm. Also, Pad_{1024} is completely dependent on encryption key, so changing the related encryption key creates critical changes of Pad_{1024}.

At the end of the 3-1 $IB_{Xor-p-1024B}$ block is obtained. This block contains 1024 bits, which is a quite complex and nonlinear functioning of the 128 characters of the plaintext and the encryption key.

3.2. The final permutation of $IB_{Xor-p-1024B}$

The last step in completing the process of encryption is that the bits of $IB_{Xor-p-1024B}$ bits are permutated. In section 2-2, 1024 bits of input block IB_{1024B} are permuted based on F_P function and the encryption key. We use this function again.

A text file called cipher(out).txt is created. The obtained results of new permutation located in OB_{1024} .

$$OB_{1024} = F_P(IB_{Xor-p-1024B}, Key_{P2}, 1024) \quad (8)$$

Where Key_{P2} is a completely arbitrary 52-bit key, includes four 13-bit numbers (A'_2, B'_2, C'_2, D'_2) and that derived from the encryption key of cryptographic operations.

The results of section 3-2 is OB_{1024}. A text file called cipher(final).txt is created. The results of encryption of each 128 characters block from the plaintext after section 3-2 is located in OB_{1024} block. We put OB_{1024} block in the file of Cipher(final) in the following of previous block. In other words, until the code of the whole plaintext are not located in the cipher(final).txt, section two and three will be repeated. The steps of section 2 are shown in Figure-3.Cipher(final) includes encrypted text or the final text of the suggested algorithm. If all the blocks of the plaintext is n_{pt}, the number of bits of cipher(final).txt is equal to $n_{pt} \times 1024$bits(Figure-4).

		Continue	Creation Block after step	Number of Block homes
Section Three		↓		
	Pad_{1024}=$f_4(Encription\ Key)$ →	**Xor operation of input block**	$IB_{Xor-p-1024B}$	1024
		↓		
	$Key_{P2} = f_5(Encription\ Key)$ →	**The final permutation**	OB_{1024}	1024
		↓		
		Cipher Text		

Figure-3. Xor operation of input block and final permutation

Plain Text	→	**Proposed method cryptography**	→	**cipher(final)**

Figure-4. Making cipher text is the goal of proposed method.

3.3 Chaining encrypted blocks

In symmetric encryption methods such as AES, 3DES, RC6 and the like, cryptographic operations are performed on the block. If the input blocks to the encryption system are similar, the same result is achieved. This operation causes the transfer of similarity in the input file to the encrypted file.

Even if the analyst cannot obtain the original file, it can identify similar parts of the original file. Although the analyst is unable to break the encryption key, but can change the fields with each other. So without anybody realizing it, he could interfere in the process of operation and a "passive attack" against the encrypted system occurred. To compensate this defect in the cipher block system, the chains of the cipher block is used. So base on version of algorithm, the user can use a method for chaining like ECB, CBC, CFB and OFB.[8-10]

4. CREATION OF THE ENCRYPTION KEY

The suggested method of encryption is included in symmetrical key method. All the necessary information for encoding, encryption operation and decryption should be located in the encryption key, until the operation of two sections is done correctly.

The encryption key of this algorithm has 256 bits and these bits define as follow (Table-1):

a) Five bits are utilized for identifying the version of the algorithm. As explained in previous sections, the potential of changing in some parts like the number of characters in one section.
b) Seven bits for n_{LB} variable in section 2-1.
c) 52 desired bits for four 13 bits variable A',B',C',D' which were utilized in section 2-2.
d) 12 completely desired bits for E' variable which was utilized in section 2-3.
e) 52 completely desired bits for four 13 bits A'_1, B'_1, C'_1, D'_1variables which were utilized in section 2-4.
f) 64 completely desired bits for F variable which were utilized in sections 2-5.
g) 12 completely desired bits for G variable in section 2-5.
h) 52 completely desired bits for four 13 bits A'_2, B'_2, C'_2, D'_2variables which were utilized in section 2-6.

Table-1. The Parameters of suggested encryption key.

Title	Version	n_{lb}	Key_p	E'	Key_{p1}	F	G	Key_{p2}
Number of bits	5	7	52	12	52	64	12	52
Address in key	K_{0-4}	K_{5-11}	K_{12-63}	K_{64-75}	K_{76-127}	$K_{128-191}$	$K_{192-203}$	$K_{204-255}$
Use in section		2-1	2-2	2-3	2-4	3-1	3-1	3-2

In the present study, the encryption key has 256 bits and also 5 of these bits are for identifying algorithm and 7 bits of n_{LB}variable are the function of the number of the plaintext characters. Thus, 244 other bits are completely random and desired. These bits are utilized for quantifying the variables of some sections of encryption algorithm. The amount of these variables does not have any effects on the power of the algorithm. In other words, there is no strong or weak key in the obtained algorithm.

5. RESULTS AND CONCLUSIONS

Successful encryption is a method which is strong (resistant) against breaking code attacks. Because of this point to investigate the efficiency of the suggested algorithm, its resistance is evaluated against common attacks.

Linear cryptanalysis

Linear cryptanalysis is done through a great volume of encrypted blocks and unencrypted blocks equivalents. Code cracking tries to find linear relationship among bits of input text, encrypted content and the main key. The base of this method which was suggested by M. Matsui[11], is the linear estimation of the fixed tables of p-box and s-box. S-boxes are the most non-linear elements of the encrypting algorithm.

Code cracking should investigate various combination of input and output of those s-boxes and through statistical analysis the linear estimation is presented. To do this estimation, code cracking should start from the input of encryption system. And it should identify all the parts which can have effects on them. Then for the P-boxes and S-boxes, this path is considered through linear estimation. Through the help of encrypted blocks and decrypted blocks, the estimation will come closer to reality and the key or the part of the key is discovered.

To keep the linear attacks away, S-boxes should be selected in a way that the estimated relationships have the lowest bias. In the suggested algorithm, P-box tables are a function of the encryption key. Also, the substitutions of the input text characters with new characters are a function of the encryption key (such as the previous operation). For this reason, the non-linear estimation is impossible and the linear attack of the code is nullified.

Differential cryptanalysis

This method is based on the principle that, how changes between two blocks of the main text (plain text) (even just a bit) affect the output of encrypted text (cipher text) and how the encrypted result of these two blocks are differentiated from each other[12]. This relationship can, in certain circumstances, reveal some key bits [13-16]. Normally the difference, Hamming distance criterion is considered as a two-bit pattern. Operations such as permutations, under constant table, and the operation of Xor do not have any resistance to differential cryptanalysis.

In this method, all changes may be applied to the table and changes of the output are recorded. Through statistical analysis of these results and forming difference distribution Table, the main indices of attacking to the whole closed system are extracted. In the following through the use of enough encrypted text and equal amount of unencrypted text, the main key is calculated through different steps. The main strength of the suggested algorithm which can cause resistance to the above attack is that the permutation and substitution tables are not fixed. These changes cause the differential distribution table and the effective parameters not to correctly form to attack. So the differential cryptanalysis would be negating too.
Investigating the changes of the cipher text based on the plaintextand encryption key differences

Changing some bits of the key and considering its result

One of the studies in the area of encryption method is creating change in the encryption key bits and investigating the level of changes on the cipher text. [17]
As each part of the key is related to a part of encrypted algorithm various parts of the key is changed individually. And, the results of this change are evaluated based on the performance.

a) Changing the $key_p(A', B', C', D')$ and $key_{p1}(A'_1, B'_1, C'_1, D'_1)andkey_{p2}(A'_2, B'_2, C'_2, D'_2)$

These three keys with length of 52 bits are used in the permutation F_P. To investigate the effects of key_p change in this section, initially, a block called $Test_{128}$ is created.$Test_{128}$has 128 houses and each house contains its number house (According Figure-5).

Home number	0	1	2	3	…	127
Contain of Home	0	1	2	3		127

Figure-5. The Schematic presentation of an input block.

According to the one 52 bits random key called Key1, the permutation of the blockhouses $Test_{128}$ is calculated and they are located in 128 bits block called$Outtest1_{128}$.

Four times, a bit from Key1 is selected randomly and changed. Based on the new key, the permutation of the $Test_{128}$ block houses is calculated and they are located in order as $Outtest2_{128}$,……, $Outtest5_{128}$. The similarities of the pairwise results are calculated. The main purpose of similarities is the number of houses which have the same contents with the same number. As the results of the experience indicate, the most similar output blocks consist of 22 identical houses and the least similar were with 8 identical houses (Table-2). This result is indicator of this point that, great change is based on the related key. The results of key_{p1} and key_{p2}which are related to permutation of 1024 houses, are created same results.

Table-2. Changing bits of Key_p and its effects on output of permutation function.

	$Outtest1_{128}$	$Outtest2_{128}$	$Outtest3_{128}$	$Outtest4_{128}$	$Outtest5_{128}$
$Outtest1_{128}$		12	15	21	19
$Outtest2_{128}$	12		8	13	17
$Outtest3_{128}$	15	8		19	16
$Outtest4_{128}$	21	13	19		22
$Outtest5_{128}$	19	17	16	22	

b) Key change in bits of E'

The E' key in the permutation section of characters is applicable in section 2.2. To investigate the effects of E' key change in this section, initially, the 12 bits E' is selected randomly. (E=E'+31) the level of character change in K-house is calculated based on chapter 1and its amount is located in K-house128 bits block called$Outtestch1_{128}$. Three times, a bit from E' is selected randomly and changed.

Accordingly, $Outtestch2_{128}$,…., $Outtestch4_{128}$ are calculated again. The level of pairwise similarities is obtained. In most similar phase, just 8 houses have same content among output blocks.

c) Key change in bits of F

This part of key is utilized for Xor operation. In the conducted experiments, it is proved that the level of change in this section, based on percentage, is transferred to the output similarly. Of course this result was completely predictable.

Comprehensive test of the space of the key

As mentioned before, the proposed method is resistant against two popular methods of attacks against symmetric cipher systems, the linear cryptanalysis and differential cryptanalysis. Thus no part of the key can be extracted by these two methods. Inevitably, the analyst should all the status of key to break the encryption key. As mentioned in section of forming encryption key, 244 bits of the encryption key bits, are randomly selected. There is no difference among encryption key concerning strengths and weaknesses. There are 2^{244}possible unique encryption keys. Now with the current technology, the keys which have more than 2^{90} independent state are resistant against the comprehensive test of the space of the key.

Applications

Cryptography is devoted to keeping data and communications secure[18]. It is a field at the core of information and communication technologies and combines mathematics, physics, computer science, and engineering. Individuals and organizations around the world depend on the ability to ensure data and communications systems are secure and reliable. Information security allows users to access services, verify the identities of other users and organizations, and authenticate the origin and integrity of software and other data.

Encryption is the process of converting data to an unrecognizable or encrypted form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet[19, 20].

REFERENCES

[1] Shannon C. 1990. Communication theory of secrecy system. Bell Syst.Tech. J. 28: 656-715.

[2] Meier W., S.O. 1989. Fast Correlations Attacks on Certain Stream Ciphers. Journal of Cryptology, Springer. pp. 159-176.

[3] T. Xusick, W. Wood. 1990. The REDOCcryptosystem, advances incryptology. Proc. of CRYPTO'SO, Lecture Notes inComputer Science. 526: 545-563.

[4] N., K. G. and V. Ramanswarm. 2008. Making AES Stronger: AES with Key Dependent S-Box. IJCSNS International Journal of Computer Science and Network Security. 8: 388-398.

[5] Zhao, G., H. Yan and F. Lu. 2007. Research of Changeable S-Box in Block Cryptosystem Based on Chaos. International Conference on Communications, Circuits and Systems.pp. 436-441.

[6] Zaibi, G., A. Kachouri, F. Peyrard and D. Fournier-Prunaret. 2010. A New Design of Dynamic S-box based on Two Chaotic Maps. International Conference on Computer Systems and Applications (AICCSA).pp. 1-6.

[7] Zobeiri.M and Mazloom-NezhadMaybodi.B. 2017. Introducing Dynamic P-Box and S-Box based on Modular Calculation and Key encryption for Adding to Current Cryptographic Systems against the Linear and Differential Cryptanalysis. ARPN Journal of Engineering and Applied Sciences. 12(3).

[8] Huang. K, Chiu. J and Shen. S. 2013. A Novel Structure with Dynamic Operation Mode for Symmetric-Key Block Ciphers. International Journal of Network Security & its Applications. 5(1): 17-36.

[9] Kamara. S and Katz. J. 2008. How to encrypt with a malicious random number generator. FSE Springer.

[10] Lamacchia. B, Lauter. K and Mityagin. A. 2007. Stronger security of authenticated key exchange. provSec Springer. pp. 1-16.

[11] M.Matsui. 1994. Linear Cryptanalysis Method for DES Cipher advances in Cryptology EUROCRYPT. Springer-Verlag.

[12] T.R.N. Rao and K.H. Nam. 1987. Private -Key Algebraic-Code Encryption. IEEE Transactions. 35(4): 829-833.

[13] Coppersmith D. 1994. The data Encryption standard (DES) and its strength against attacks. IBM journalof research and development. 38(3).

[14] Biham and Shamir. 1990. Differential Cryptanalysis of DES-like Cryptosystems. Technical Report CS90-16 (Weizmann Institute of Science).

[15] Kim, C.H. 2012. Differential Fault Analysis of AES: Toward Reducing Number of Faults. Journal of Information Sciences. 199: 43-57.

[16] Kim C.H. 2012. Improved Differential Fault Analysis on AES Key Schedule. IEEE Transactions on Information Forensics and Security. 7: 41-50.

[17] Jawahar Thakur, D., Aesand Blowfish. 2011. Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering. 1(2).

[18] T. Mo, J. Wang and W. Mo. 2011. Design of secure communications network system based on data encryption and digital signature. International Conferance on High Performance Computing & Simulation.pp. 626-630.

[19] I.Hussain, N. A.Azam and T. Shah. 2014. Stego optical encryption based on chaotic S-box transformation. Optics & Laser Technology. 61: 50-56.

[20] Rudolf M., StanićLoknar N. and Žiljak Stanimirović I. 2015. Infrared steganography with individual screening shapes applied to postage stamps with security features. Technical Gazette. 22(4): 939-945.