I.J. Mathematical Sciences and Computing, **2019, 3, 27-36**
Published Online July 2019 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijmsc.2019.03.03

Available online at http://www.mecs-press.net/ijmsc

Randamization Technique for Desiging of Substitution Box in Data Encryption Standard Algorithm

Nilima S.[a*], Alind[b], Nitin Arora[c]

[a,b]*School of Computer Science, Department of Virtualization, University of Petroleum & Energy Studies, Dehradun, India.*
[c]*School of Computer Science, Department of Informatics, University of Petroleum & Energy Studies, Dehradun, India*

Received: 20 January 2019; Accepted: 13 June 2019; Published: 08 July 2019

Abstract
A new approach for the generation of randomized substitution box (S-box) based on the concept of a redesign of S-box with fewer numbers of input bits processed at a time as compared to existing S-box in Data Encryption Standard (DES) Algorithm. The results of experimentation prove that proposed randomized approach also generate promising results, which can be particularly useful for devices with less processing power. Proposed approach retains the diffusion and confusion property of a good cryptosystem algorithm.

Index Terms: Data Encryption Standard Algorithm, Cryptosystem, Substitution boxes, Security, Diffusion, Confusion.

© 2019 Published by MECS Publisher. Selection and/or peer review under responsibility of the Research Association of Modern Education and Computer Science

1. Introduction

The pool of cryptographic algorithms[1] listed in are available which are used for encryption and decryption, these algorithms are divided into different categories which depend on two factors 1. Way of processing the input and 2. How input has prepared for processing. On the basis of the first condition, algorithms are divided into two main categories substitution and transposition. In Substitution technique frequency of occurrence of characters in plaintext may or may not be similar as in cipher-text. While in transposition technique frequency of occurrence of characters in plaintext and cipher-text are always the same. On the basis of the second condition underneath algorithm has to decide about the capacity of bits it can process, handle in single execution round thus algorithms fall into two main categories block cipher and stream cipher. Stream ciphers

* Corresponding author.
E-mail address: nsfulmare@ddn.upes.ac.in

are designed to handle one bit at a time thus entire input has to process in series, whereas block cipher is designed to handle fix number of bits at a time which is known as a block. While dealing with block cipher confusion property which has proposed by Shannon Theory is essential, which seeks to make the relationship as much complicated as can be between encrypted keys and cipher-text. S-box[2][3] is the heart of DES algorithm [4] as its non-linear component which used in block cipher to achieve the desirable confusion property. Besides confusion, diffusion is also a desirable property in block cipher which seeks to make the statistical relationship between the plaintext and encrypted bits as complicated as possible which also known as 'Avalanche Effect'[5]. One single change in plaintext should reflect a maximum change in bits of cipher-text. In an existing DES, S-box process 6 bits at a time thus result into total 8 S-boxes to process 48 bits of plaintext[4]. In this paper, we have proposed a randomized approach[6] for the generation of S-box static and randomized approach with less number of bits 3 bits at a time thus total 16 S-boxes, which can make the attacker[7] difficult to identify which structure has been used for an algorithm.

The rest of this paper is organized as follows. Section 2 introduces the proposed S-box; Section 3 describes the methodology part; Results are discussed in Section 4; paper has been concluded in Section 5 and Section 6 describes the future work.

2. Proposed S-box

S-Box or substitution box is an integral part of any S-P(substitution-permutation)[8][9] network that is aligned with the symmetric key cryptography. Essentially it is used to remove linear relationship[7] between plaintext and cipher-text by implementing the Shannon's property of confusion. S-box can be understood as an encoder which take input and output in bits. Occasionally, an S-box is denoted by M x N, where M represents input bits and N represents output bits where M > N. While assuming an S-Box as a table the N bits of M bits input will be used to select the column and remainder M – N bits are used to select the row number of the table to identify the output cell.

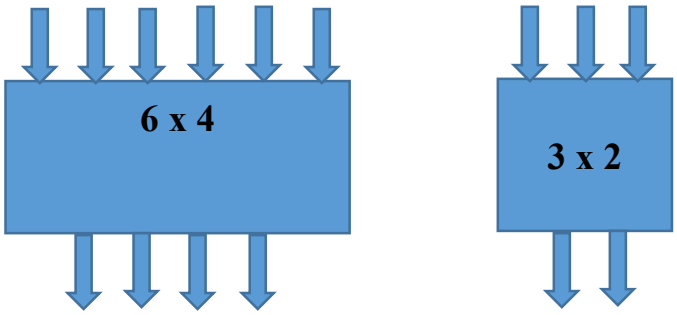

Fig. 1. a) Existing S-box dimension b) Proposed S-box dimension

S-box accepts certain numbers of bits as an input, substitute it with different bits and produce the output. Although a number of input and output bit are not necessarily the same. In exiting S-box number of input bits are 6 and number of output bits are 4, thus total 8 S-boxes are required. In our proposed S-box number of input bits are 3 and output bits 2 thus total 16 S-boxes are required. We have executed the DES algorithm with different sets of inputs and S-box.

3. Methodology

To check strength/limitation of proposed work we have done experimentation by providing 5 different combinations of inputs. We have provided input to DES[10] algorithms in the form of a string as it is the most

convenient way of providing input. Each character is represented by 8 bits thus constitute 64 bits altogether. For analysis purpose first, we have checked with providing 5 different combinations of input lowercase, uppercase, special characters, numbers, and alphanumeric. We have used two categories S-box of dimension 3x2 and 6x4. As DES falls into the category of a block cipher[11][12] to ensure the correctness of the proposed approach we have an emphasis on retention of confusion and diffusion properties. To retain confusion property, which talks about the statistical correlation between generated cipher-text and key which we have used for encryption purpose, we have used a randomized key [13] for complete 16 rounds of DES, thus ensured confusion property of an algorithm should retain. We have experimented with this approach for all 5 sets of input. To retain diffusion property which talks about how cipher-text statistically different from plaintext we have an emphasis on retaining avalanche property which talks about how cipher-text deviates from an earlier version by changing a single bit in plaintext. We have experimented an entire procedure by providing static/dynamic inputs to different dimension and nature of S-boxes.

Table 1. Different set of inputs

Inputs	(3x2)x16	(6x4)x8
Randomized Input includes lowercase, whitespace, uppercase	Dynamic	Dynamic
Lowercase, Uppercase, Special Character, Numeric, Alphanumeric	Static	Static
Lowercase, Uppercase, Special Character, Numeric, Alphanumeric	Dynamic	Dynamic

4. Results & Discussion

To check the strength/limitations of our proposed approach the following results have been fetched: Entropy extracted from DES algorithms by changing the number of input bits to 3 and output bits to 2 and compared over the existing S-box structure of DES input bits 6 and output bits 4. For the first time, we have provided random input and generated random S–box existing and proposed and fetched the results. Results retrieved indicate that for some string entropy retrieved is better in case of randomized 3 x 2 S-box while sometimes it is better in case of randomized 6 x 4 S-box as shown in figure 2. To come to the conclusion which structure provides better results in the form of entropy we have restricted the input as shown in table 1 and restricted the S-box design to static and dynamic nature as shown in figure 3 and figure 4. In both, the cases result retrieved indicate that if we restrict input string to DES algorithm is numbers only and generate either static/dynamic S-box, proposed 3x2 approach provides better results as compared to existing 6x4 static/dynamic generated S-box.

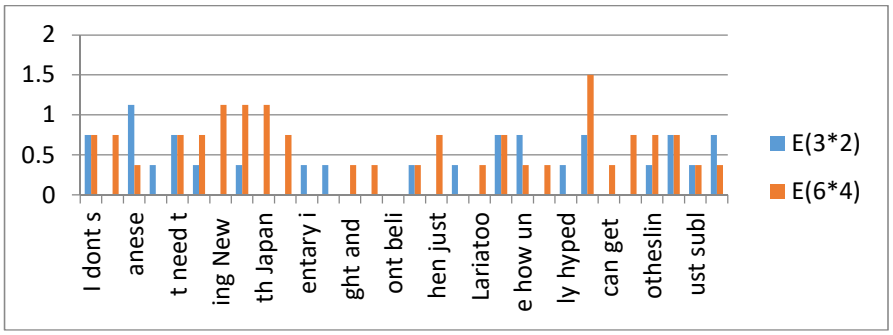

Fig. 2. Entropy retrieved by providing random input and randomly generated S-box

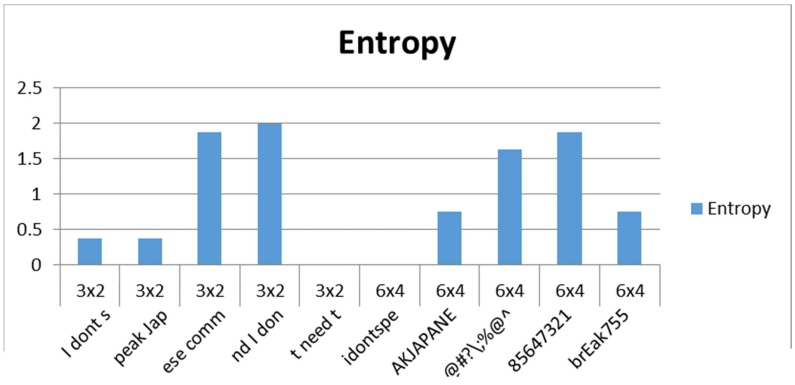

Fig. 3. Entropy retrieved by providing set of inputs and static S-box

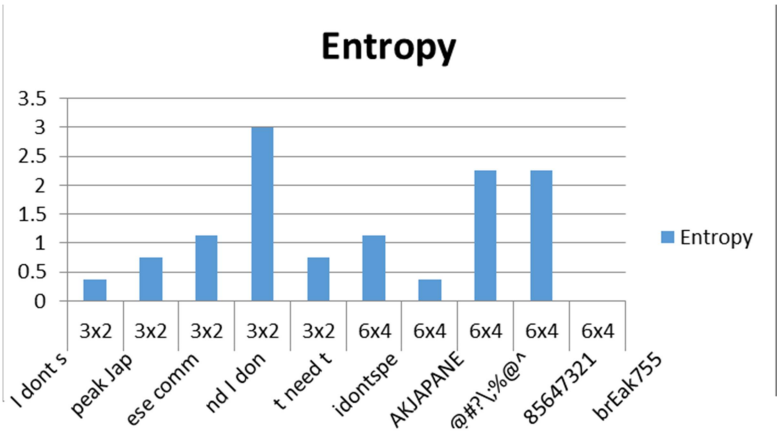

Fig. 4. Entropy retrieved by providing set of inputs and dynamic S-box

To retain the diffusion property we have checked for avalanche effect i.e. how many bits flipped in cipher-text as compared to plaintext as shown in figure 5. Results of avalanche effect has experimented from DES algorithms by changing the number of input bits to 3 and output bits to 2 and compared over the existing S-box structure of DES input bits 6 and output bits 4. For the first time, we have provided random input and generated random s –box existing and proposed and fetched the results. Results retrieved indicate that on an average number of bits flipped are almost same in both the cases 3x2 and 6x4. To come to the conclusion which structure provides better results in the term of avalanche we have restricted the input as shown in table 1 and restricted the S-box design to static and dynamic nature as shown in figure 6 and figure 7. In both, the cases result retrieved indicate that if we restrict input string to DES algorithm other than special characters only and generate either static/dynamic S-box, proposed 3x2 approach provides similar results as compared to existing 6x4 static/dynamic generated S-box.

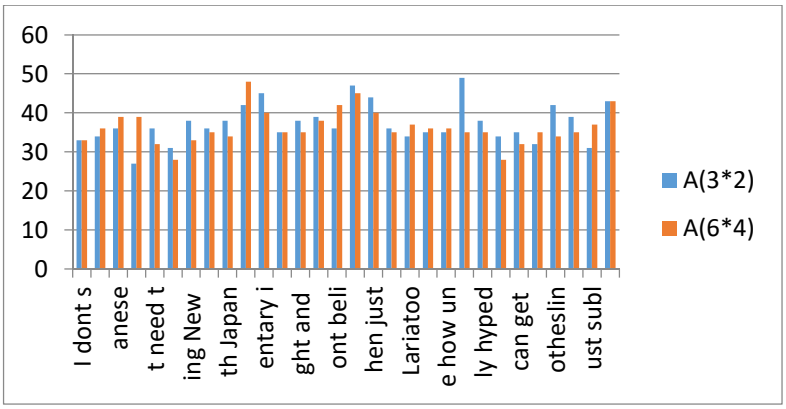

Fig. 5. Avalanche effect by providing random input and randomly generated S-box of dimension 3x2 and 6x4

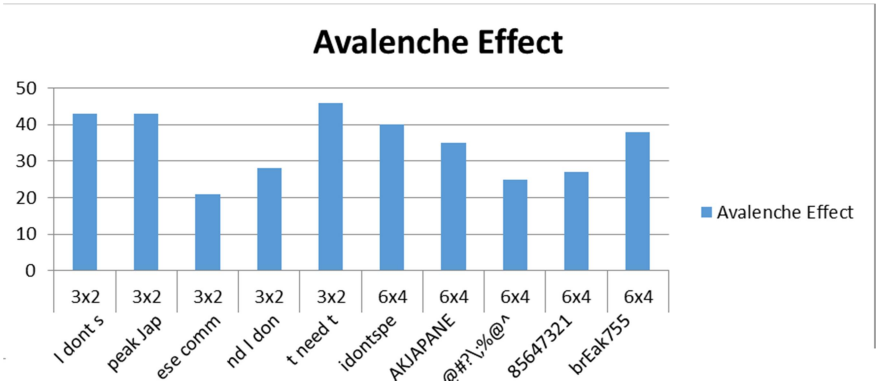

Fig. 6. : Avalanche effect by providing different combinations of input to static S-box of dimension 3x2 and 6x4 static S-box

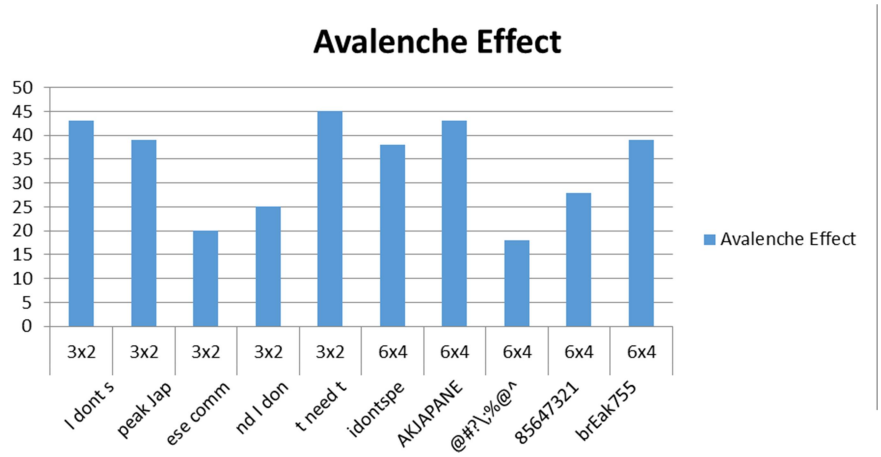

Fig. 7. Avalanche Effect by providing different combinations of input to dynamic S-box of dimension 3x2 and 6x4

4.1 Compressive Results

We have experimented with 9 different combinations in plaintext and retrieved the results. We have achieved results number of bits flipped ≥ 50% to retain the property of diffusion in 7 cases whereas we have not achieved the results which satisfy diffusion property only in the combination of only numeric and only special case characters where number of bits flipped in the cipher text is less than < 50%.

Table 2. Random and Static Inputs

String	Text	Random		Static		Random		Static	
		E(3*2)	E(6*4)	E(3*2)	E(6*4)	A(3*2)	A(6*4)	A(3*2)	A(6*4)
Randomly Generated Inputs	I dont s	0.75	0.75	0.38	0.375	33	33	36	38
	peak Jap	0	0.75	0	0.375	34	36	35	39
	ese comm	0.75	0.75	0.38	0.375	41	45	39	45
	nd I don	0.375	0	0	0.75	27	39	32	36
	t need t	0.75	0.75	0.38	0.375	36	32	37	35
	idontspe	0	1.125	0.38	0	43	38	43	40
Fixed Inputs	AKJAPANE	0.375	0.375	0.38	0.75	39	43	43	35
	@#?\;%@^	0.75	2.25	1.88	1.625	20	18	21	25
	85647321	1.125	2.25	2	1.875	25	28	28	27
	brEak755	3	0	0	0.75	45	39	46	38

As per figure 8.a proposed approach of reducing the number of bits at a time generate promising result as compare to existing approach in case of entropy retrieval.

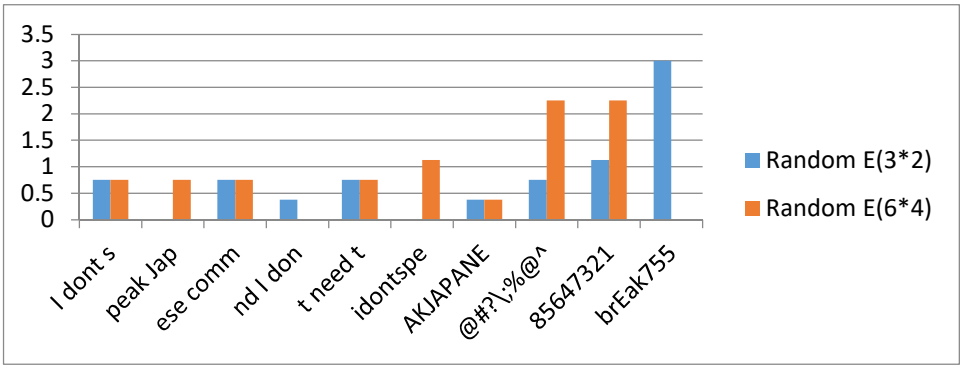

Fig. 8. (a) Dynamic Input and Entropy

As per figure 8.b proposed approach of reducing the number of bits at a time generate promising result as compare to existing approach in case of entropy retrieval and provided static S-box. Figure 8.c and 8.d supports the result of diffusion retention by proposed approach.

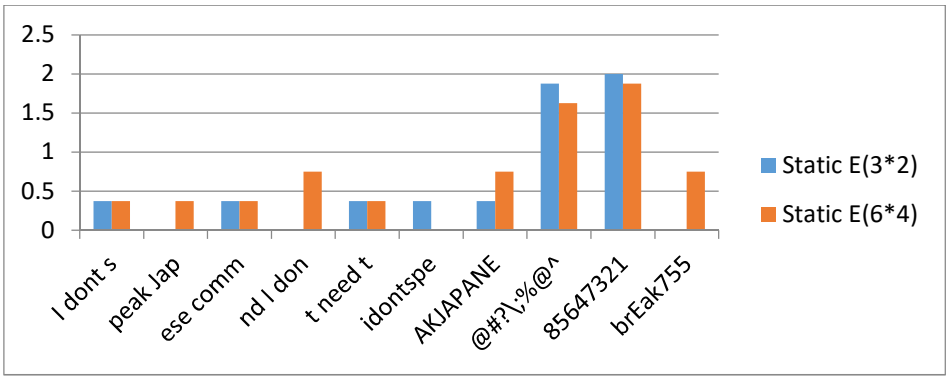

Fig. 8. (b) Static Input and Entropy

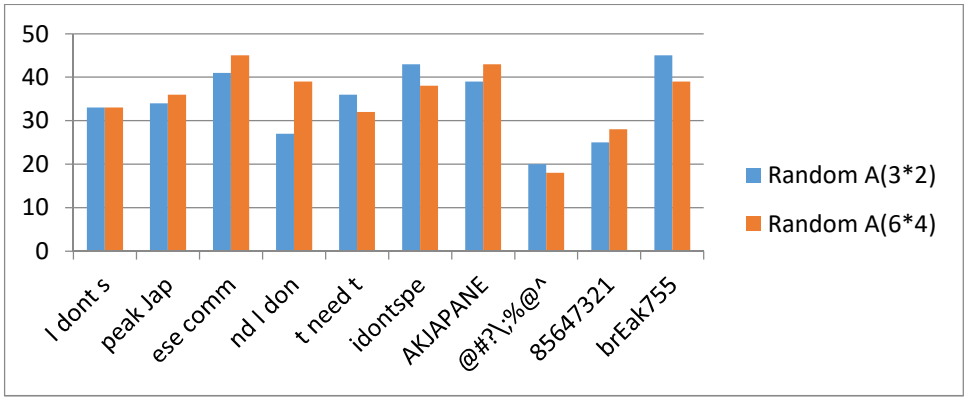

Fig. 8.(c) Dynamic Input and Avalanche

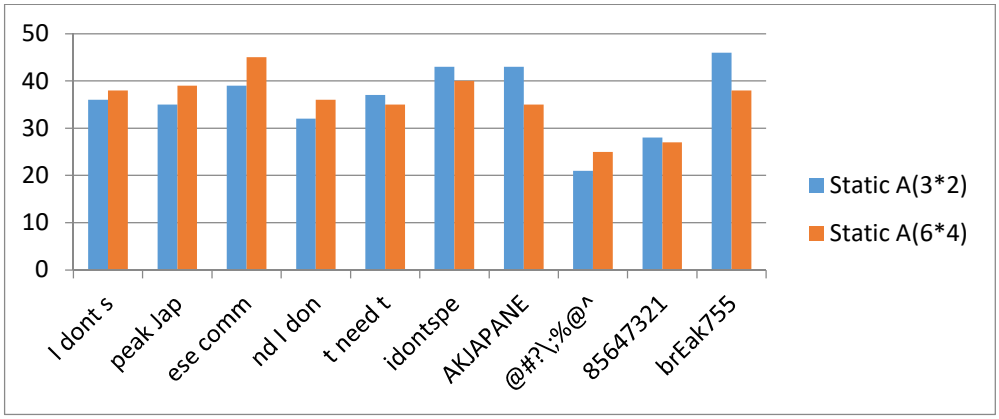

Fig. 8. (d) Static Input and Avalanche

Table 3. Percentage deviation of Avalanche Effect of Random and Static generated S-box for proposed and existing approach

Sr. No.	Plaintext	Random 3 x 2	%	Random 6 x 4	%	Static 3 x 2	%	Static 6 x 4	%
1	Lowercase with 2 white spaces	33	51.56	33	51.6	36	56.25	38	59.38
2	Combination of lower and upper case with 1 whitespace	34	53.13	36	56.3	35	54.69	39	60.94
3	Lowercase with 1 white space	41	64.06	45	70.3	39	60.94	45	70.31
4	Lowercase with 2 white spaces	36	56.25	32	50	37	57.81	35	54.69
5	Lowercase	43	67.19	38	59.4	43	67.19	40	62.5
6	Uppercase	39	60.94	43	67.2	43	67.19	35	54.69
7	Special Characters	20	31.25	18	28.1	21	32.81	25	39.06
8	Numeric	25	39.06	28	43.8	28	43.75	27	42.19
9	Alphanumeric	45	70.31	39	60.9	46	71.88	38	59.38

Table 4. Entropy retrieved of Random and static generated S-box for proposed and existing approach

Text	Random		Static		Comments
	E(3*2)	E(6*4)	E(3*2)	E(6*4)	
I dont s	0.75	0.75	0.375	0.375	
peak Jap	0	0.75	0	0.375	
ese comm	0.75	0.75	0.375	0.375	We have retrieved random results neither comment on the basis of dynamic and static nature of S-box nor on the basis of dimension used. As sometimes we have achieved a better result in static S-box case whereas other time we have achieved better results in the dynamic case. So retrieval of information is not dependent on the nature and dimension of S-box.
nd I don	0.375	0	0	0.75	
t need t	0.75	0.75	0.375	0.375	
idontspe	0	1.125	0.375	0	
AKJAPANE	0.375	0.375	0.375	0.75	
@#?\;%@^	0.75	2.25	1.875	1.625	
85647321	1.125	2.25	2	1.875	
brEak755	3	0	0	0.75	

5. Conclusion

We have done experimentation with static and dynamic inputs and S-box.We have generated very promising results thus dynamic input and changed configuration of S-box can be used for the encoding and decoding purpose**.**

6. Future work

We will do experimentation with different combinations of S-box and identify the parameters which are responsible for information retrieval from the plaintext. We will check for comparison of diffusion property for single DES and triple DES.

References

[1] F. Özkaynak and A. B. Özer, "A method for designing strong S-Boxes based on chaotic Lorenz system," Phys. Lett. Sect. A Gen. At. Solid State Phys., vol. 374, no. 36, pp. 3733–3738, 2010.
[2] D. Lambić, "A new discrete chaotic map based on the composition of permutations," Chaos, Solitons and Fractals, vol. 78, pp. 245–248, 2015.
[3] D. Lambić, "A novel method of S-box design based on discrete chaotic map," Nonlinear Dyn., vol. 87, no. 4, pp. 2407–2413, 2017.
[4] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," J. Cryptol., vol. 4, no. 1, pp. 3–72, 1991.
[5] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," Nonlinear Dyn., vol. 87, no. 1, pp. 337–361, 2017.
[6] D. Lambić and M. Živković, "Comparison of random S-Box generation methods," Publ. l'Institut Math., vol. 93, no. 107, pp. 109–115, 2013.
[7] A. Biryukov, "The Boomerang Attack on 5 and 6-Round Reduced AES Conference Paper in Lecture Notes in Computer Science • May 2004," no. May 2004, pp. 2–7, 2016.
[8] L. Keliher, "Substitution-Permutation Network Cryptosystems Using Key-Dependent S-Boxes," no. September, 1997.
[9] Q. Wang et al., "Theoretical Design and FPGA-Based Implementation of Higher-Dimensional Digital Chaotic Systems," IEEE Trans. Circuits Syst. I Regul. Pap., vol. 63, no. 3, pp. 401–412, 2016.
[10] Kamesh and N. Sakthi Priya, "Gbaam," Int. J. Appl. Eng. Res., vol. 9, no. 22, pp. 5968–5974, 2014.
[11] G. Liu, W. Yang, W. Liu, and Y. Dai, "Designing S-boxes based on 3-D four-wing autonomous chaotic system," Nonlinear Dyn., vol. 82, no. 4, pp. 1867–1877, 2015.
[12] Y. Wang, K. W. Wong, X. Liao, and T. Xiang, "A block cipher with dynamic S-boxes based on tent map," Commun. Nonlinear Sci. Numer. Simul., vol. 14, no. 7, pp. 3089–3099, 2009.
[13] Ü. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar, "A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system," Nonlinear Dyn., vol. 87, no. 2, pp. 1081–1094, 2017.

Authors' Profiles

Dr. Nilima S. working as Assistant Professor (Selection Grade) at University of Petroleum & Energy Studies, Dehradun. She has 14 years of teaching experience. Her research interest areas are signal processing, EEG, cryptography and statistical analysis.

Alind received his M. Tech degree in 2015 from Indian Institute of Technology Delhi and B. Tech degree in 2012 from Uttar Pradesh Technical University, Lucknow. Presently he is working as Assistant Professor-Senior Scale in Department of Virtualization, School of Computer Science, University of Petroleum and Energy Studies, Dehradun. His research interest lies in Optimization, Image Processing and Machine Learning. He has also served as TPC member of International Conferences.

Nitin Arora received his M. Tech degree in 2012 from G. B. Pant Engineering College, Pauri and B. Tech degree in 2008 from NIT, Allahabad. Presently he is working as Assistant Professor-Senior Scale in the Department of Informatics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun. His research interest lies in Optimization, Image Processing and Machine Learning.

How to cite this paper: Nilima S, Alind, Nitin Arora,"Randamization Technique for Desiging of Substitution Box in Data Encryption Standard Algorithm", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.5, No.3, pp.27-36, 2019. DOI: 10.5815/ijmsc.2019.03.03