Enhancing Security in Digital Data using various Function of S-box in Data Encryption Standard Method

Leya Elizabeth Sunny
Research Scholar, Department of Information Technology, SOE, CUSAT, Kerala, India.
E-mail: leyabejoy81@gmail.com

Dr. Varghese Paul
Professor, Department of Computer Science and Engineering, Rajagiri School of Engineering and Technology, Kakkanad, Kerala, India. E-mail: vp.itcusat@gmail.com

Received April 23, 2021; Accepted August 18, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18I2/WEB18353

Abstract

Stage of networking is quintessential task in which security comes into play. Securing these networks which contains confidential digital data that needs to secured will be the agenda of cryptography. Many cryptographic algorithms increment their strengths over parameters like key size, increasing the rounds of iteration and finally using confusion box as S-box as it has best robustness. So, this paper mainly focusses over securing digital data with the help of S-box function over Data Encryption Standard (DES) algorithm. For this, a plain text and key will be given to this DES as it extracts 8x8(64) bit characters from the key and converting them into its corresponding ASCII value and are concatenating to form an 8 value by taking mod16. These will give to 8 S-box in order to generate its corresponding output to make even more secure and also shows dynamic DES gives much result than other crypto methods. The evaluation of this integrated s-box and DES shows much fruitful results over factors like non-linearity, Avalanche criterion, Balance, Robustness to linear cryptanalysis, Robustness to differential cryptanalysis.

Keywords

Cryptography, Data Encryption Standard, Digital Data, Substitution-box, Security.

Introduction

Alongside the advancement of the Internet, the utilization of computerized correspondence mechanism for information and data trade is additionally expanding. One of the fundamental issues in advanced correspondence is the security of the information was communicated over the web organization. Information can be taken or gotten to by assailants with the specific methods. Consequently, it is the vital utilization of solid information security methods for information trade through web media. Cryptography and Steganography are two of the most generally used to get computerized information. Cryptography is a procedure for getting information where the first information is randomized so that it is hard to comprehend. Unique information must be opened by a particular individual utilizing predefined custom keys. A portion of the present mainstream cryptographic methods incorporate Advanced Encryption Standard (AES), Data Encryption Standard (DES), RC4 and RSA. Every one of the three are regularly used to get significant information in different applications. Hellman and Martin (1979) execute the DES calculation to create programming that can scramble and unscramble text and records. In the mean-time, Alani and Mohammed (2010) executed the AES and RC4 calculations to get information on the Agricultural Quarantine Agency. Cryptography can likewise be applied to get web-based informing, for example, Yahoo Messenger (Manikandan et al. (2012)).

Cryptography is the secure communication technique derived from set of mathematical calculations, to transfer plain text to cipher text and vice versa. It use public and private key for data encryption and decryption. Symmetric key encryption include Data Encryption Standard (DES), Advance Encryption Standard (AES), Blowfish, Twofish, IDEA, CAST, SEAL and RC4 (Shah and Bhavika (2012); Oukili et al. (2017); Arya et al. (2013)). All the above encryption technique use the same secret key for both encryption and decryption. To encode a message, private key cryptography is used. According to the National Institute of Standards and Technology of the United States, sensible replacement for DES as the new private key encryption estimation. AES is better than DES as it is prudent for large key sizes, 8 cycle chip stages and 32 digit processors (Wong et al. (2001)).

Worked on information encryption standard-DES is a block cypher framework which changes 64-digit information blocks under a 56-cycle secret key, through stage and replacement. It is utilization of 16 round Feistel structure the block size of 64-digit. DES depends on the two essential ascribes of cryptography: Transposition (Diffusion) and Substitution (Confusion). DES calculations comprise of 16 stages every one of which is called as a Round calculation (Figure 1).

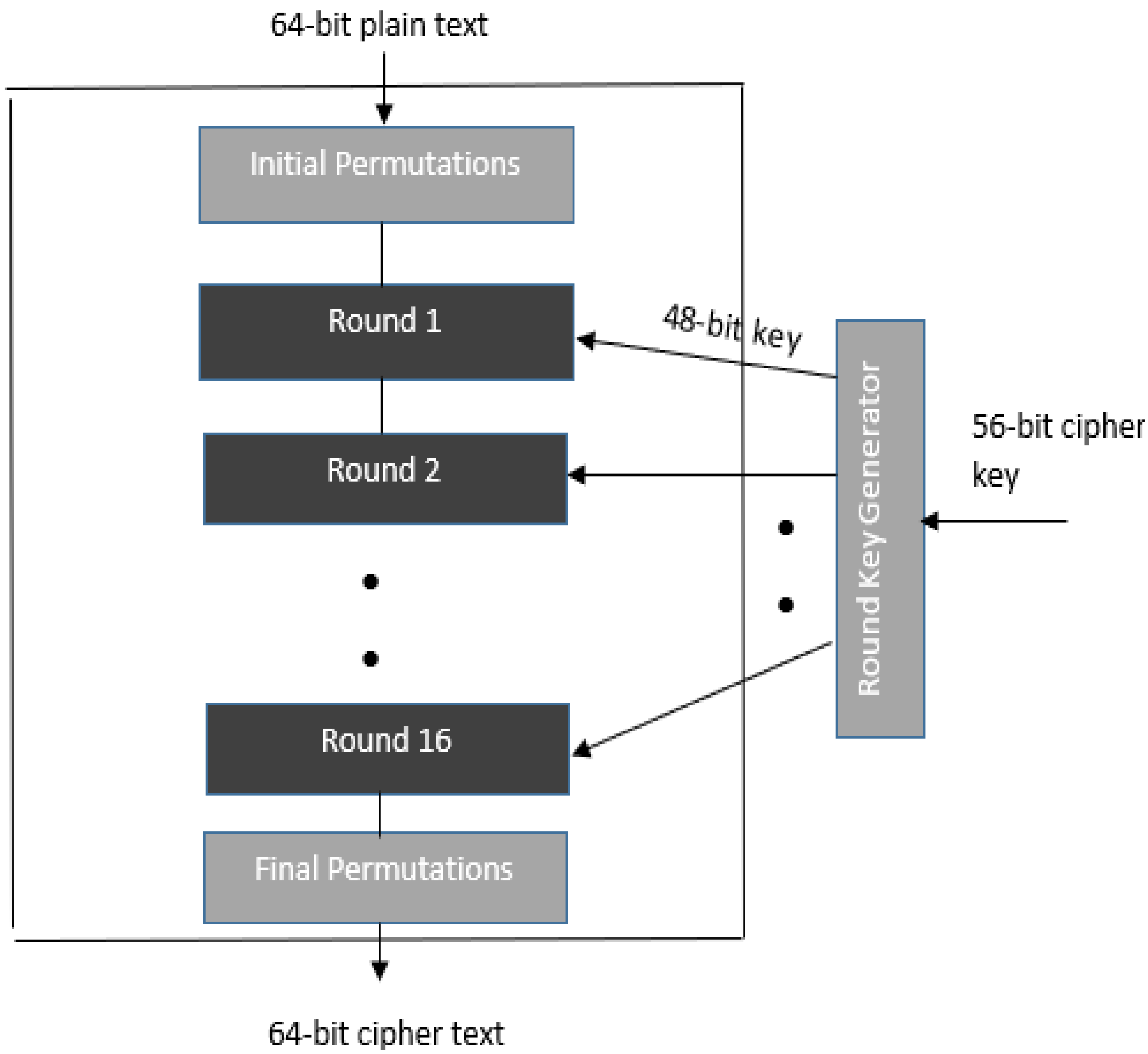


Figure 1 DES basic flow

S-Box is a basic component of symmetric key algorithm to perform substitution (Roslan et al. (2019)). However, two vulnerabilities in the S-Box Render are vulnerable to cryptanalysis. The S-Box is a basic development in any square code system (Rivest et al. (1978)). There are two types of S-boxes, a fixed or a Static S-box, which infers a comparable S-box will be used in each round. A specific S-Box enables attackers to analyze the features of the S-Box and locate its loose spots. The main problem with completing any square code structure is that the S-boxes are part of a fixed plan. A representation of a static S-box is the S-boxes Data Encryption Standard computation (DES) (Nilima et al. (2019)). Figure 2 outlines the current DES that is been utilized for long time by scientists.

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Figure 2 Existing DES design

The dynamic S-box or key-subordinate S-box displayed depends on the key and number of rounds (Zahid et al. (2020); Rahaman et al. (2020)). The configuration of fixed S-boxes licenses them to go against differential and straight cryptanalysis, and dynamic S-boxes are definitely ready to go against these attacks. In addition, a unique S-box differential and straight cryptanalysis is impossible because its development is completely removed from the cryptanalist, so the attacker is incapable of testing anything about the attack on a particular project of S-boxes (Siddiqui et al. (2020)). Additionally, these S-boxes can be built when needed, reducing the need for a range of large data structures within the calculation.

So, in this paper we can see how dynamic S-box act as a boosting function for DES algorithm and together how enhanced version of security is given for protecting digital data (Alabaichi et al. (2015)).

Organization of paper: As we already go through the introductory part, the rest of the section is as follows; Section 2 depict related works that is been put forwarded by various researchers, followed by methodology in Section 3 and implementation and Results in Section 4 and finally conclude over Section 5.

Related Works

Some of the related works that is been proposed by various researchers over several cryptographic methods for enhancing security of digital data are follows;

Juremi et al. (2012) suggested another new AES key ward with S-Box Rebellion to make S-Box key-subordinate, updating the power of AES accordingly. The built-in key is used to select a value to be used in the curve of the S-box. Each byte of the second key is XORed. The results are then used to engage the disturbance of the S-box, the evaluation of which depends entirely on the round key. Therefore, this code structure reflects the primary AES, but in different approaches is key-subordinate with no change in the S-box value.

Mohammad et al. (2018) suggested an AES with Variable Mapping S-box (VMS-AES). This is a novel AES that combines the basic data for the age of the range used to move the S-box to a better location (remap) based on the data of the base key and subordinate sub keys (Anees et al. (2015); Ullah et al. (2018); Siddiqui et al. (2020)). In VMS-AES, forward replacement byte modification, which limits the operation of AES subbytes, replaces a move with respect to the limit, and resolves and adds the replacement limit to another secret area. Starting from one byte and moving from one specific static region (such as AES) to another space. In addition, the area is secretive because it relies on a secret concept.

Sombir Singh et al. (2013) improved the computation using the Simple Column Transposition Technique (Transposition Cryptography Techniques), which is to plan the substance in the kind of lines inside a square and a short time later redo and read it in an upward direction in an unpredictable way. According to the usage of the substance and the amount it is proposed to be tangled. The eventual outcome of this course of action is the substance that is installed into the DES estimation to scramble it. Accordingly, the resulting encoded text is many-sided, making it difficult to break the computation. The use of this computation requires extra external exercises to execute and deliver different segments self-assertively and a short time later send them over the association impacts network execution (Gupta and Nimmi (2013)).

Payal Patel et al. (2014) has improved the computation by growing the key length and extending the unpredictability of the S-boxes similarly as growing the number of cases used to address the given information. The purpose of extending the key length was not to simplify it for monster power attack. In this assessment, the expert hasn't kept an eye on the key.

Albassali et al. (2004) managed improving the estimation by proposing a procedure for building the sub-keys in the computation using the GA. The sub-keys created by this strategy depends upon the GA that gives an absolutely exceptional plan of semi-self-assertive sub-keys each time where the program is executed. Subkeys are made from one central key, as opposed to the proposed computation.

Sharma et al. (2015) proposed frameworks to improve then DES estimation by using two additional keys despite the 64-digit fundamental key, similarly as an adjustment of a couple inside patterns of DES using S-BOX for the AES computation.

Krishnamurthy and Ramaswamy (2008) suggested that the S-Box AES be changed dynamically from one round to the next. Without a change in the critical institutions of the AES, with one-fourth being subject to the welfare requirement. The primary case uses the last byte from the round keys and subject the S-box to it. The S-box rotates between all bytes of the two case keys depending on the second case being XORED. The third case uses another course of round keys created using a key enhancement calculation, which is similar to the AES key augmentation estimate. The last byte of the round keys is used to riot the S-box. The fourth case is similar to the third case in addition to XORED, and between evaluations of large bytes on the key keys, the S-box rotates depending on the subject.

Mahmoud et al. (2013) made a recommendation for a special AES-128 with key-subordinate S-box subject to the phase of the standard S-box obliged by the AES secret key. The direct input shift register (LFSR) is a pseudorandom generator (PN) that is used to create self-assertive groups. The AES Secret key is used for the age of a hidden territory of LFSR by secluding two areas and XOR the results between them to be used as the fundamental assessment of the LFSR. The yield of the PN generator is XORED with the strange key. The result is changed over to 32 hexadecimal characteristics as s1 and s2. S1 and s2 are used to change the fragments and lines on the standard S-box.

Methodology

Figure 3 depicts the overall workflow of the proposed dynamic DES in which initially the key values that is been arranged will be read and these values are converted into ASCII key values and then passed for whitening process. Here basically a conversion of ASCII values into 8 seeded formats will happens in which if the values of I getting is less than 8 then Si is calculated by increment the i values. Also storing of prime numbers that are in the range of 100 and 1000 in which if the value of i becomes less than 8 then generate the first Sbox. Here we calculate a term called element where it is the mod16 (Seed/Prime) and we again check for the presence of element and if not present then we append this to Sbox1 that is been generated. Then potentially increment the prime value and generate the second Sbox and also store the value of element where here it is calculated as mod16 (Seed +1777/Prime) and check if this is not present. If not then we append this element with Sbox that is generated secondly. Like that we generate every Sbox with different calculation of the "element" value and finally returns 8 Sboxes (Khan et al. (2017)).

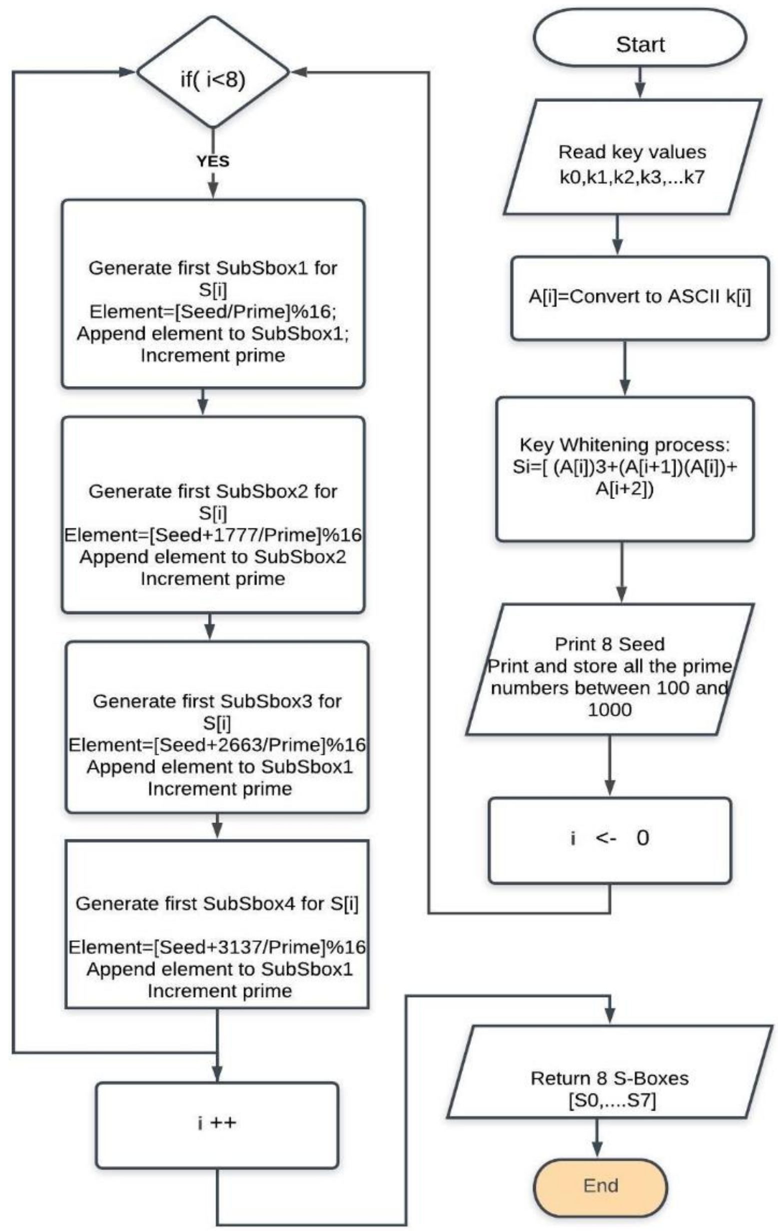


Figure 3 Dynamic DES Flowchart

Table 1. depict the generated 8 Sbox using the Dynamic DES method in which for every Sbox we have different function for enhancing its security even tighter to protect from crypto attacks.

Table 1 8 Sbox generated with various function using Dynamic DES

Dynamic Sbox 1	3	14	6	11	10	1	9	2	8	15	4	7	5	13	12	0
	9	14	15	8	6	5	1	7	2	4	11	0	13	12	10	3
	8	15	13	10	14	1	7	12	5	11	4	9	0	2	6	3
	13	1	2	12	10	9	5	11	6	3	15	4	0	8	14	7
Dynamic Sbox 2	8	3	2	9	11	12	13	10	15	1	6	0	4	5	7	14
	4	10	1	13	14	6	8	5	15	9	3	0	2	11	12	7
	7	8	15	0	3	13	2	10	9	5	4	12	1	11	14	6
	5	11	8	13	12	3	1	4	10	0	6	9	7	15	14	2
Dynamic Sbox3	9	3	12	0	15	7	5	8	14	4	10	13	11	2	1	6
	7	1	10	15	14	5	3	6	12	2	8	11	9	0	13	4
	8	2	11	14	15	6	4	7	13	3	9	12	10	1	0	5
	13	7	2	4	3	11	9	12	1	8	14	0	15	6	5	10
Dynamic Sbox 4	9	3	12	0	15	7	5	8	14	4	10	13	11	2	1	6
	7	1	10	15	14	5	3	6	12	2	8	11	9	0	13	4
	8	2	11	14	15	6	4	7	13	3	9	12	10	1	0	5
	13	7	2	4	3	11	9	12	1	8	14	0	15	6	5	10
Dynamic Sbox 5	9	3	12	0	15	7	5	8	14	4	10	13	11	2	1	6
	7	1	10	15	14	5	3	6	12	2	8	11	9	0	13	4
	8	2	11	14	15	6	4	7	13	3	9	12	10	1	0	5
	13	7	2	4	3	11	9	12	1	8	14	0	15	6	5	10
Dynamic Sbox 6	7	15	11	12	5	10	13	0	8	6	14	1	4	9	2	3
	8	0	12	13	6	11	14	1	9	7	15	2	5	10	3	4
	5	14	9	10	3	8	11	15	6	4	12	13	2	7	0	1
	13	5	0	1	11	4	2	6	14	12	3	7	10	15	8	9
Dynamic Sbox 7	8	15	13	10	14	1	7	12	5	11	4	9	0	2	6	3
	5	12	10	7	11	13	4	9	2	8	1	6	14	15	3	0
	13	3	1	15	2	4	12	0	10	6	9	14	5	7	11	8
	12	2	0	14	1	3	11	5	9	15	8	13	4	6	10	7
Dynamic Sbox 8	5	13	1	0	7	2	14	12	4	6	15	11	8	3	10	9
	13	4	9	8	15	10	7	3	12	14	6	2	5	11	1	0
	12	3	8	7	14	9	6	2	11	13	5	1	15	10	0	4
	6	14	2	1	8	3	0	13	5	7	15	12	9	4	11	10

Implementation and Results

Here for evaluating the DES, criterion that is taken for evaluation are non-linearity, Avalanche criterion, Balance, Robustness to linear cryptanalysis, Robustness to differential cryptanalysis. Also, this system is implemented over python in simulation format where there is an ease comparison of Static and Dynamic DES.

Non Linearity

The non-linearity Nf of a Boolean function is the minimum distance to any affine function. It is given through eq (i),

$$N_f = \frac{1}{2}\left(2^N - WHT_{max}(f)\right)N_f = \frac{1}{2}\left(2^N - WHT_{max}(f)\right) \quad \text{(i)}$$

The highest absolute value is taken from the Walsh Hadamard Transform (WHT). It will be defined as

$$WHT_{max}(f) = \left|F_f(\alpha)\right|WHT_{max}(f) = \left|F_f(\alpha)\right| \quad \text{(ii)}$$

The WHT of a Boolean function f is defined by

$$\hat{F}_f(\alpha) = \sum_{x\epsilon B} N \quad \hat{f}(x)\hat{L}_{\alpha(x)}\hat{F}_f(\alpha) = \sum_{x\epsilon B} N \quad \hat{f}(x)\hat{L}_{\alpha(x)} \quad \text{(iii)}$$

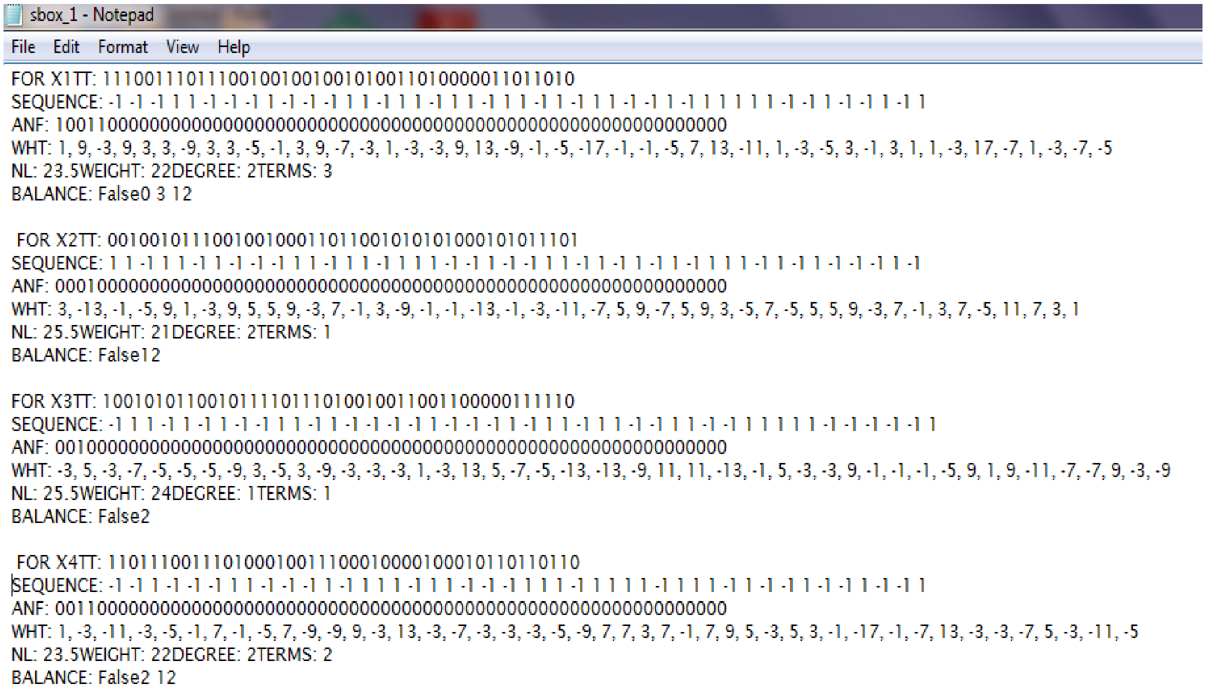
Were,

$$\hat{f}(x) = (-1)^{f(x)}\hat{f}(x) = (-1)^{f(x)} \quad \text{(iv)}$$

The maximum nonlinearity achievable for the S-box in GF(2^8) when N is even is given by

$$N_{max}(N) = 2^N - 2^{\frac{N}{2}-1}N_{max}(N) = 2^N - 2^{\frac{N}{2}-1}$$

For S-boxes in GF (2^8), the optimal value is 120 and for the S-boxes in GF (2^6) the optimal value is 28. Figure 4 (a, b, c, d, e, f, g, h) depict the 8 Sbox output under the factor “Non linearity”.



sbox_1 - Notepad

File Edit Format View Help

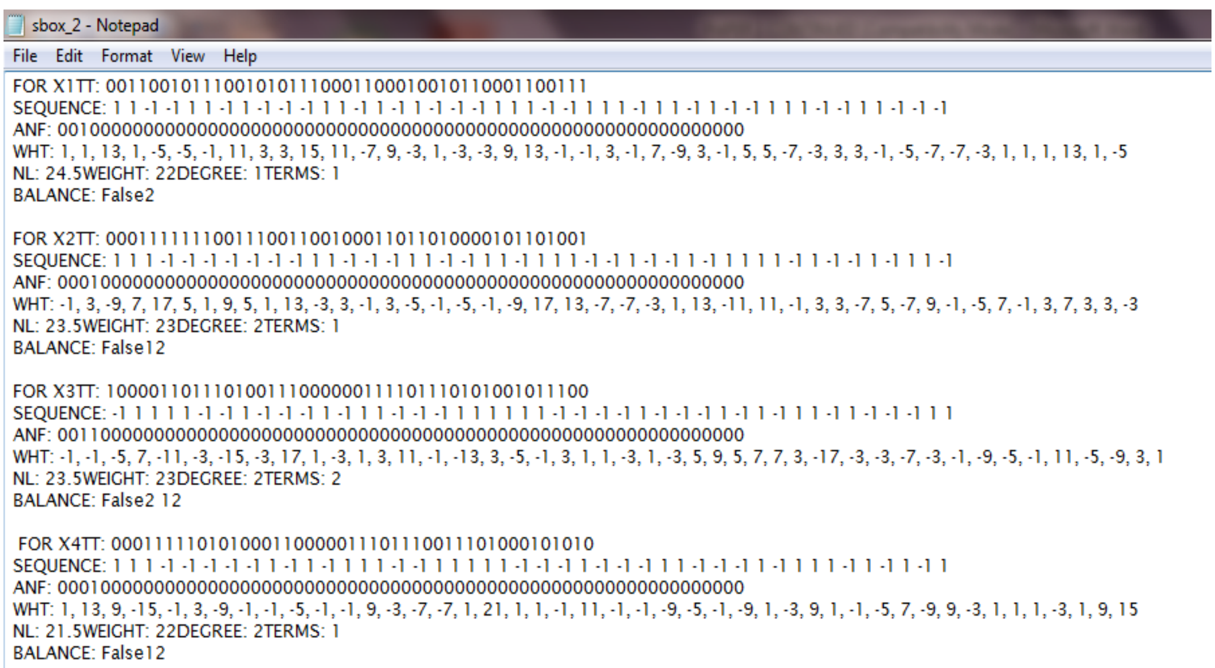
FOR X1TT: 111001110111001001001001010011010000011011010
SEQUENCE: -1 -1 -1 1 1 1 -1 -1 -1 1 -1 -1 -1 1 1 1 -1 1 1 -1 1 1 -1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 -1 1
ANF: 1001100000000000000000000000000000000000000000000000000000000000
WHT: 1, 9, -3, 9, 3, 3, -9, 3, 3, -5, -1, 3, 9, -7, -3, 1, -3, -3, 9, 13, -9, -1, -5, -17, -1, -1, -5, 7, 13, -11, 1, -3, -5, 3, -1, 3, 1, 1, -3, 17, -7, 1, -3, -7, -5
NL: 23.5WEIGHT: 22DEGREE: 2TERMS: 3
BALANCE: False0 3 12

FOR X2TT: 001001011100100100011011001010101000101011101
SEQUENCE: 1 1 -1 1 1 1 -1 1 -1 -1 -1 1 1 1 -1 1 1 1 -1 1 1 1 1 -1 -1 1 -1 -1 1 1 1 -1 1 -1 1 -1 1 1 -1 1 1 1 1 -1 1 -1 1 -1 -1 -1 1 1 -1
ANF: 0001000000000000000000000000000000000000000000000000000000000000
WHT: 3, -13, -1, -5, 9, 1, -3, 9, 5, 5, 9, -3, 7, -1, 3, -9, -1, -1, -13, -1, -3, -11, -7, 5, 9, -7, 5, 9, 3, -5, 7, -5, 5, 5, 9, -3, 7, -1, 3, 7, -5, 11, 7, 3, 1
NL: 25.5WEIGHT: 21DEGREE: 2TERMS: 1
BALANCE: False12

FOR X3TT: 100101011001011110111010010011001100000111110
SEQUENCE: -1 1 1 -1 1 -1 1 -1 -1 1 1 1 -1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 1 -1 1 1 1 -1 -1 1 1 1 -1 -1 1 1 1 1 1 1 -1 -1 -1 -1 -1 1 1
ANF: 0010000000000000000000000000000000000000000000000000000000000000
WHT: -3, 5, -3, -7, -5, -5, -5, -9, 3, -5, 3, -9, -3, -3, -3, 1, -3, 13, 5, -7, -5, -13, -13, -9, 11, 11, -13, -1, 5, -3, -3, 9, -1, -1, -1, -5, 9, 1, 9, -11, -7, -7, 9, -3, -9
NL: 25.5WEIGHT: 24DEGREE: 1TERMS: 1
BALANCE: False2

FOR X4TT: 110111001110100010011100010000100010110110110
SEQUENCE: -1 -1 1 -1 -1 -1 1 1 1 -1 -1 -1 1 -1 1 1 1 1 -1 1 1 1 -1 -1 -1 1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 1 1 -1 -1 1 1 -1 -1 1 1 -1 -1 1 1
ANF: 0011000000000000000000000000000000000000000000000000000000000000
WHT: 1, -3, -11, -3, -5, -1, 7, -1, -5, 7, -9, -9, 9, -3, 13, -3, -7, -3, -3, -3, -5, -9, 7, 7, 3, 7, -1, 7, 9, 5, -3, 5, 3, -1, -17, -1, -7, 13, -3, -3, -7, 5, -3, -11, -5
NL: 23.5WEIGHT: 22DEGREE: 2TERMS: 2
BALANCE: False2 12

a



sbox_2 - Notepad

File Edit Format View Help

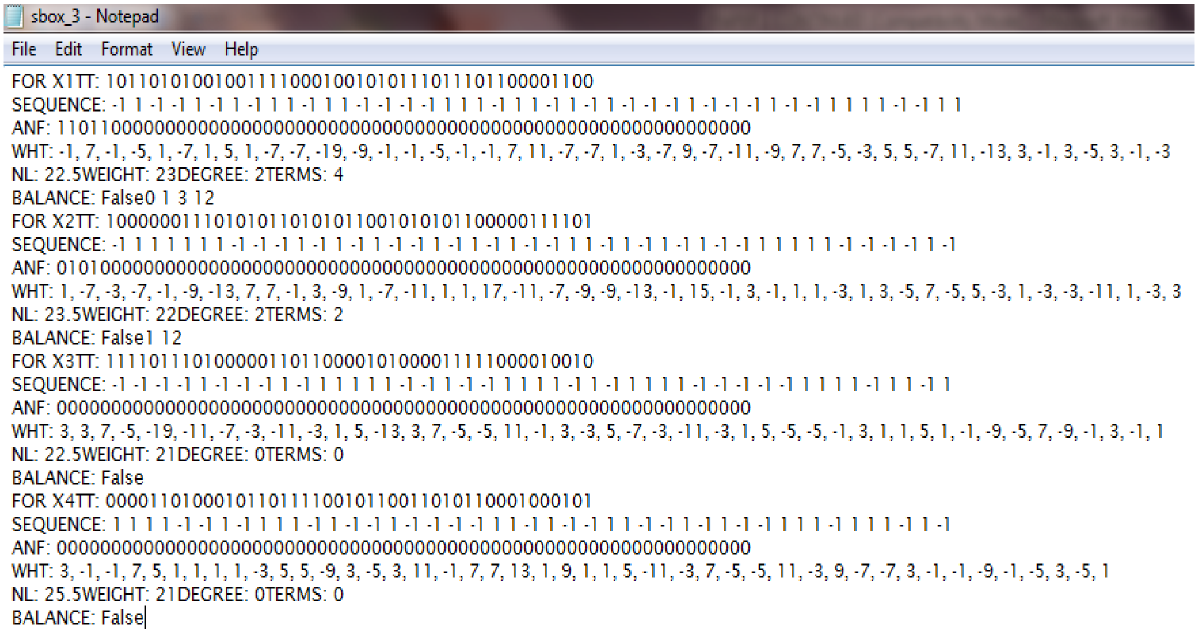
FOR X1TT: 001100101110010101110001100010010110001100111
SEQUENCE: 1 1 -1 -1 1 1 1 -1 1 -1 -1 -1 1 1 1 -1 1 -1 1 -1 -1 -1 1 1 1 1 -1 -1 1 1 1 1 -1 1 1 -1 1 -1 -1 1 1 1 1 -1 -1 1 1 1 -1 -1 -1
ANF: 0010000000000000000000000000000000000000000000000000000000000000
WHT: 1, 1, 13, 1, -5, -5, -1, 11, 3, 3, 15, 11, -7, 9, -3, 1, -3, -3, 9, 13, -1, -1, 3, -1, 7, -9, 3, -1, 5, 5, -7, -3, 3, 3, -1, -5, -7, -7, -3, 1, 1, 1, 13, 1, -5
NL: 24.5WEIGHT: 22DEGREE: 1TERMS: 1
BALANCE: False2

FOR X2TT: 000111111100111001100100011011010000101101001
SEQUENCE: 1 1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 1 1 1 -1 -1 1 1 1 -1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 1 1 1 1 -1 1 1 -1 -1 1 1 -1 1 1 1 -1
ANF: 0001000000000000000000000000000000000000000000000000000000000000
WHT: -1, 3, -9, 7, 17, 5, 1, 9, 5, 1, 13, -3, 3, -1, 3, -5, -1, -5, -1, -9, 17, 13, -7, -7, -3, 1, 13, -11, 11, -1, 3, 3, -7, 5, -7, 9, -1, -5, 7, -1, 3, 7, 3, 3, -3
NL: 23.5WEIGHT: 23DEGREE: 2TERMS: 1
BALANCE: False12

FOR X3TT: 100001101110100111000000111101110101001011100
SEQUENCE: -1 1 1 1 1 1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 1 1 -1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 1 -1 1 1 1 -1 1 1 -1 -1 -1 1 1 1
ANF: 0011000000000000000000000000000000000000000000000000000000000000
WHT: -1, -1, -5, 7, -11, -3, -15, -3, 17, 1, -3, 1, 3, 11, -1, -13, 3, -5, -1, 3, 1, 1, -3, 1, -3, 5, 9, 5, 7, 7, 3, -17, -3, -3, -7, -3, -1, -9, -5, -1, 11, -5, -9, 3, 1
NL: 23.5WEIGHT: 23DEGREE: 2TERMS: 2
BALANCE: False2 12

FOR X4TT: 000111110101000110000011101110011101000101010
SEQUENCE: 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 1 1 1 1 -1 -1 1 1 1 1 1 1 -1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 -1 -1 1 1 -1 1 1 1 1 -1 1 1 -1 1 1 -1 1 1
ANF: 0001000000000000000000000000000000000000000000000000000000000000
WHT: 1, 13, 9, -15, -1, 3, -9, -1, -1, -5, -1, -1, 9, -3, -7, -7, 1, 21, 1, 1, -1, 11, -1, -1, -9, -5, -1, -9, 1, -3, 9, 1, -1, -5, 7, -9, 9, -3, 1, 1, 1, -3, 1, 9, 15
NL: 21.5WEIGHT: 22DEGREE: 2TERMS: 1
BALANCE: False12

b

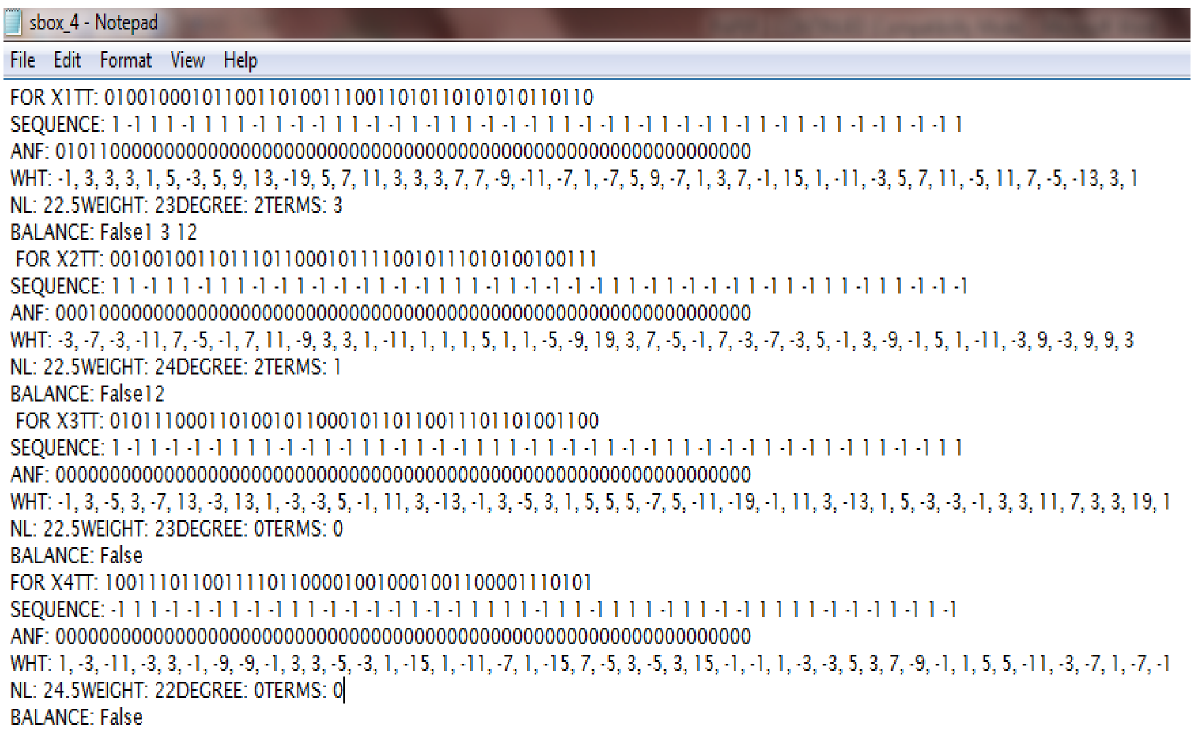


sbox_3 - Notepad

File Edit Format View Help

FOR X1TT: 101101010010011110001001010111011101100001100
SEQUENCE: -1 1 -1 -1 1 -1 1 -1 1 1 -1 1 1 -1 -1 -1 -1 1 1 1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 -1 -1 1 -1 -1 1 1 1 1 1 -1 -1 1 1
ANF: 110110000000000000000000000000000000000000000000000000000000000000
WHT: -1, 7, -1, -5, 1, -7, 1, 5, 1, -7, -7, -19, -9, -1, -1, -5, -1, -1, 7, 11, -7, -7, 1, -3, -7, 9, -7, -11, -9, 7, 7, -5, -3, 5, 5, -7, 11, -13, 3, -1, 3, -5, 3, -1, -3
NL: 22.5WEIGHT: 23DEGREE: 2TERMS: 4
BALANCE: False0 1 3 12
FOR X2TT: 100000011101010110101011001010101100000111101
SEQUENCE: -1 1 1 1 1 1 1 1 -1 -1 -1 1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 1 1 1 1 -1 -1 -1 -1 1 1 -1
ANF: 010100000000000000000000000000000000000000000000000000000000000000
WHT: 1, -7, -3, -7, -1, -9, -13, 7, 7, -1, 3, -9, 1, -7, -11, 1, 1, 17, -11, -7, -9, -9, -13, -1, 15, -1, 3, -1, 1, 1, -3, 1, 3, -5, 7, -5, 5, -3, 1, -3, -3, -11, 1, -3, 3
NL: 23.5WEIGHT: 22DEGREE: 2TERMS: 2
BALANCE: False1 12
FOR X3TT: 111101110100000110110000101000011111000010010
SEQUENCE: -1 -1 -1 -1 1 -1 -1 -1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 1 1 1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 -1 1
ANF: 000000000000000000000000000000000000000000000000000000000000000000
WHT: 3, 3, 7, -5, -19, -11, -7, -3, -11, -3, 1, 5, -13, 3, 7, -5, -5, 11, -1, 3, -3, 5, -7, -3, -11, -3, 1, 5, -5, -5, -1, 3, 1, 1, 5, 1, -1, -9, -5, 7, -9, -1, 3, -1, 1
NL: 22.5WEIGHT: 21DEGREE: 0TERMS: 0
BALANCE: False
FOR X4TT: 000011010001011011110010110011010110001000101
SEQUENCE: 1 1 1 1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 -1 -1 -1 1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 -1 1 1 1 -1 1 1 1 1 -1 1 -1
ANF: 000000000000000000000000000000000000000000000000000000000000000000
WHT: 3, -1, -1, 7, 5, 1, 1, 1, 1, -3, 5, 5, -9, 3, -5, 3, 11, -1, 7, 7, 13, 1, 9, 1, 1, 5, -11, -3, 7, -5, -5, 11, -3, 9, -7, -7, 3, -1, -1, -9, -1, -5, 3, -5, 1
NL: 25.5WEIGHT: 21DEGREE: 0TERMS: 0
BALANCE: False

c



sbox_4 - Notepad

File Edit Format View Help

FOR X1TT: 010010001011001101001110011010110101010110110
SEQUENCE: 1 -1 1 1 -1 1 1 1 1 -1 1 -1 -1 1 1 1 -1 -1 1 -1 1 1 1 -1 -1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 -1 -1 1 1
ANF: 010110000000000000000000000000000000000000000000000000000000000000
WHT: -1, 3, 3, 3, 1, 5, -3, 5, 9, 13, -19, 5, 7, 11, 3, 3, 3, 7, 7, -9, -11, -7, 1, -7, 5, 9, -7, 1, 3, 7, -1, 15, 1, -11, -3, 5, 7, 11, -5, 11, 7, -5, -13, 3, 1
NL: 22.5WEIGHT: 23DEGREE: 2TERMS: 3
BALANCE: False1 3 12
FOR X2TT: 001001001101110110001011110010111010100100111
SEQUENCE: 1 1 -1 1 1 1 -1 1 1 1 -1 -1 1 -1 -1 -1 1 -1 -1 1 1 1 1 -1 1 -1 -1 -1 -1 1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 1 1 1 -1 1 1 1 -1 -1 -1
ANF: 000100000000000000000000000000000000000000000000000000000000000000
WHT: -3, -7, -3, -11, 7, -5, -1, 7, 11, -9, 3, 3, 1, -11, 1, 1, 1, 5, 1, 1, -5, -9, 19, 3, 7, -5, -1, 7, -3, -7, -3, 5, -1, 3, -9, -1, 5, 1, -11, -3, 9, -3, 9, 9, 3
NL: 22.5WEIGHT: 24DEGREE: 2TERMS: 1
BALANCE: False12
FOR X3TT: 010111000110100101100010110110011101101001100
SEQUENCE: 1 -1 1 -1 -1 -1 1 1 1 1 -1 -1 1 -1 1 1 1 -1 1 -1 -1 1 1 1 1 -1 1 -1 -1 1 -1 -1 1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 1 1 -1 -1 1 1 1
ANF: 000000000000000000000000000000000000000000000000000000000000000000
WHT: -1, 3, -5, 3, -7, 13, -3, 13, 1, -3, -3, 5, -1, 11, 3, -13, -1, 3, -5, 3, 1, 5, 5, 5, -7, 5, -11, -19, -1, 11, 3, -13, 1, 5, -3, -3, -1, 3, 3, 11, 7, 3, 3, 19, 1
NL: 22.5WEIGHT: 23DEGREE: 0TERMS: 0
BALANCE: False
FOR X4TT: 100111011001111011000010010001001100001110101
SEQUENCE: -1 1 1 -1 -1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 1 1 1 -1 1 1 1 -1 1 1 1 1 -1 1 1 1 -1 -1 1 1 1 1 1 -1 -1 -1 1 1 -1 1 -1
ANF: 000000000000000000000000000000000000000000000000000000000000000000
WHT: 1, -3, -11, -3, 3, -1, -9, -9, -1, 3, 3, -5, -3, 1, -15, 1, -11, -7, 1, -15, 7, -5, 3, -5, 3, 15, -1, -1, 1, -3, -3, 5, 3, 7, -9, -1, 1, 5, 5, -11, -3, -7, 1, -7, -1
NL: 24.5WEIGHT: 22DEGREE: 0TERMS: 0
BALANCE: False

d

```
sbox_5 - Notepad
File Edit Format View Help
FOR X1TT: 1010110100110000011001111100111010001110010110
SEQUENCE: -1 1 -1 1 -1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 1 -1 -1 1 1 -1 -1 -1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 1 -1 -1 1 1 -1 1 -1 -1 1 1
ANF: 1100000000000000000000000000000000000000000000000000000000000000
WHT: -1, -5, -5, 3, 1, -11, 5, -3, -3, 1, -7, 1, 11, -9, -1, 7, 7, -5, 3, -13, -7, -11, 13, -3, -3, -7, -23, -7, 11, -1, -1, -1, -3, 1, 1, 9, 3, -1, -1, 7, -9, 3, 11, 3, 1
NL: 20.5WEIGHT: 23DEGREE: 1TERMS: 2
BALANCE: False0 1

 FOR X2TT: 0111110110011111011010000000110101001001001111
SEQUENCE: 1 -1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 1 -1 -1 1 -1 1 1 1 1 1 1 1 1 -1 -1 1 -1 1 -1 1 1 -1 1 1 -1 1 1 1 -1 -1 -1
ANF: 0111000000000000000000000000000000000000000000000000000000000000
WHT: -3, 5, -3, -7, 11, 3, 11, 15, 3, 3, -5, 7, -11, 5, -3, 17, -11, 5, 5, -7, 3, 3, 3, -1, 3, 11, -5, -1, 5, -3, -3, 9, -5, 3, -5, -1, 5, -3, 5, 1, -3, -3, 5, 9, -13
NL: 23.5WEIGHT: 24DEGREE: 2TERMS: 3
BALANCE: False1 2 12

FOR X3TT: 0110000101100011111011001011011100010101011100
SEQUENCE: 1 -1 -1 1 1 1 1 -1 1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 -1 1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1
ANF: 0010000000000000000000000000000000000000000000000000000000000000
WHT: -1, 7, 7, 11, -3, -11, -3, 9, 5, 5, -11, -7, -1, -1, 7, 3, 11, 11, 11, 7, 1, 1, -7, 13, 1, 9, 9, -11, 3, -5, 3, -9, -7, -7, 1, 5, -5, -5, -5, 7, 3, -5, -13, 7, -7
NL: 25.5WEIGHT: 23DEGREE: 1TERMS: 1
BALANCE: False2

FOR X4TT: 1100000110110110001001010011110001011101110000
SEQUENCE: -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 1 -1 -1 1 1 1 -1 1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 -1 1 1 1 1 1
ANF: 0010000000000000000000000000000000000000000000000000000000000000
WHT: 3, 3, 3, -1, 1, -7, 1, -3, 1, 9, 1, -3, 3, 3, -13, 15, -1, -1, -1, -5, -3, 5, -19, -7, -3, 5, -3, -7, -1, 15, -1, 11, 1, 1, 1, 5, -5, -13, 11, -1, 11, 3, -5, -1, 1
NL: 22.5WEIGHT: 21DEGREE: 1TERMS: 1
BALANCE: False2
```

e

```
sbox_6 - Notepad
File Edit Format View Help
FOR X1TT: 0100101101100110100100011010101001010010111101
SEQUENCE: 1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 1 -1 1 1 1 -1 -1 1 -1 1 -1 1 -1 1 1 -1 1 -1 1 1 -1 1 -1 -1 -1 1 1 -1
ANF: 0101100000000000000000000000000000000000000000000000000000000000
WHT: 1, -7, 1, 5, -1, 7, -9, 3, 7, 15, 7, -13, 1, 9, -7, -3, -3, 5, -3, 17, 3, 11, -5, 7, 3, -5, 3, -1, 5, 13, -3, 1, 3, -5, 3, -1, 5, -3, -3, 1, -3, 5, -3, -15, 3
NL: 23.5WEIGHT: 22DEGREE: 2TERMS: 3
BALANCE: False1 3 12

FOR X2TT: 1000011100001000111100001111001110011010010100
SEQUENCE: -1 1 1 1 1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 -1 -1 -1 -1 1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 -1 1 -1 1 1 -1 1 -1 1 1
ANF: 0101000000000000000000000000000000000000000000000000000000000000
WHT: 3, -1, 3, -5, -7, 5, -7, -7, -3, -7, -3, -3, -1, -5, -1, -9, 11, -1, -5, -5, 17, 5, 1, -7, -11, -7, 5, -3, 7, -5, -9, -9, 1, -3, 1, 1, -5, -9, -5, 3, -1, 11, -1, 7, -3
NL: 23.5WEIGHT: 21DEGREE: 2TERMS: 2
BALANCE: False1 12

 FOR X3TT: 1000000011111110010011001011011000001100011111
SEQUENCE: -1 1 1 1 1 1 1 1 1 -1 -1 -1 -1 -1 -1 -1 1 1 -1 1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 1 1 1 1 -1 -1 1 1 1 1 -1 -1 -1 -1
ANF: 0011000000000000000000000000000000000000000000000000000000000000
WHT: 1, -3, -11, 5, -1, 3, 11, -5, 23, 3, -13, -5, 9, -3, -3, 5, 1, -3, -3, -3, -1, 3, 3, 3, 15, -5, 3, -5, 1, -11, -3, -11, -1, -5, -5, 3, -7, -3, -3, -11, 9, 5, -3, -3, -1
NL: 20.5WEIGHT: 22DEGREE: 2TERMS: 2
BALANCE: False2 12

FOR X4TT: 1111100010100100110101000110010010010001110111
SEQUENCE: -1 -1 -1 -1 -1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 -1 1 1 -1 1 1 -1 1 1 -1 1 1 1 -1 -1 -1 1 1 -1 -1
ANF: 0010000000000000000000000000000000000000000000000000000000000000
WHT: 1, 5, -11, -3, -17, -5, 3, -5, -1, 3, 3, -13, -7, 5, -3, -3, -3, -7, 1, -15, -5, -1, -1, -1, 3, -1, 7, -1, -3, 1, 1, 9, 3, -1, -9, 15, -11, -7, 9, 1, -11, 1, -7, -7, -5
NL: 23.5WEIGHT: 22DEGREE: 1TERMS: 1
BALANCE: False2
```

f

Figure 4 (a, b, c, d, e, f, g, h) Shows Simulation results of 8 S-box for the analysis of Dynamic S-box

A comparative analysis of Dynamic DES and Static DES based on factor "non-linearity" is showed in figure 5 in which it is evident that the non-linearity values of Dynamic S-boxes are 24.5, 23.25, 23.5, 23, 23, 22.75, 24 and 24.5, while that of Static S-boxes is 23.5, 21, 23.5, 22.5, 20.5, 19, 21.5 and 23 respectively. Thus, we can see that in all the cases, the non-linearity of Dynamic DES outperforms the non-linearity of static DES in almost all the cases.

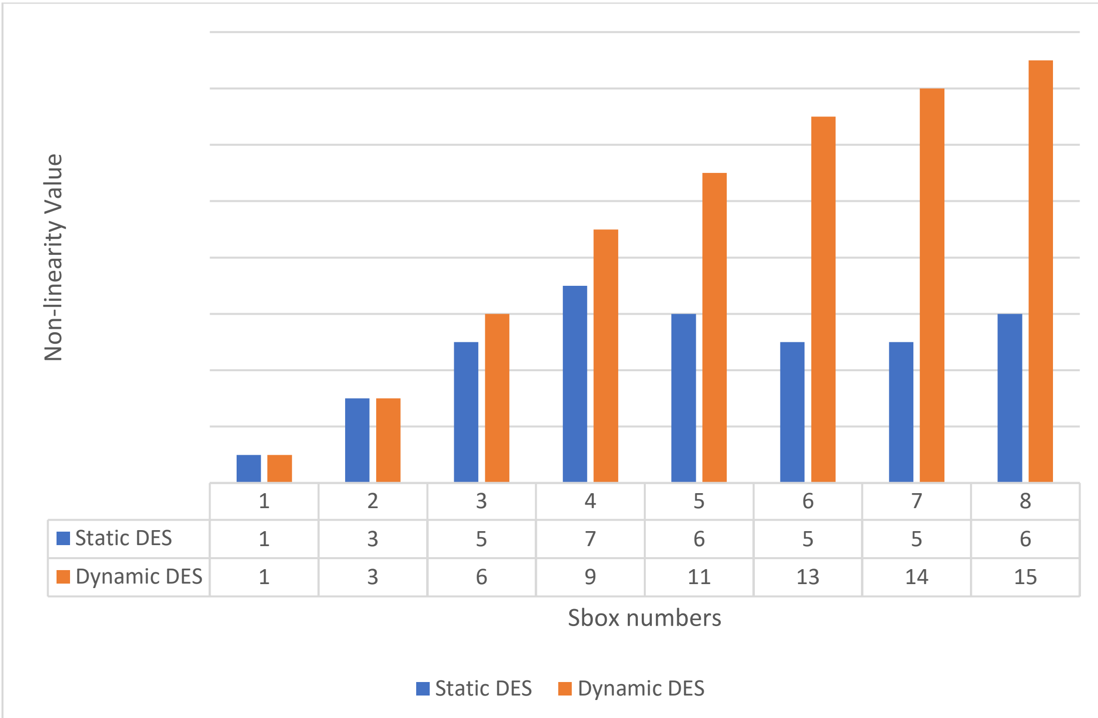


Figure 5 Comparative analysis of static and Dynamic DES over non-linearity

Balance

A Boolean function is said to be balanced its truth table has equal number of 0s and 1s. In our S-box equations are balanced, i.e., 0 and 1 have an equal probability of occurrence. Since our 8 Dynamic S-boxes gives the values 0-15 in each of the four rows and are unique, we can say that our S-box is balanced.

Avalanche Criterion

Strict Avalanche Criterion (SAC) says that if any input bit is flipped then exactly half of output bits should change. For a cipher to exhibit the cryptographic property, the output bits should change by at least half, whenever an input bit changes. Table 2 depict the avalanche criterion values of static and dynamic DES. Figure 6 shows the graphical representation and Figure 7 depict the snapshots while evaluating dynamic and static DES.

Table 2 Avalanche criterion for static and dynamic DES

	No of bits changed in the cipher when PT is 12345678 and key is 12345678	No. of bits changed in the cipher when there is 1 bit change in plaintext	No. of bits changed in the cipher when there is 1 bit change in key
Static DES	27	26	27
Dynamic DES	31	30	31

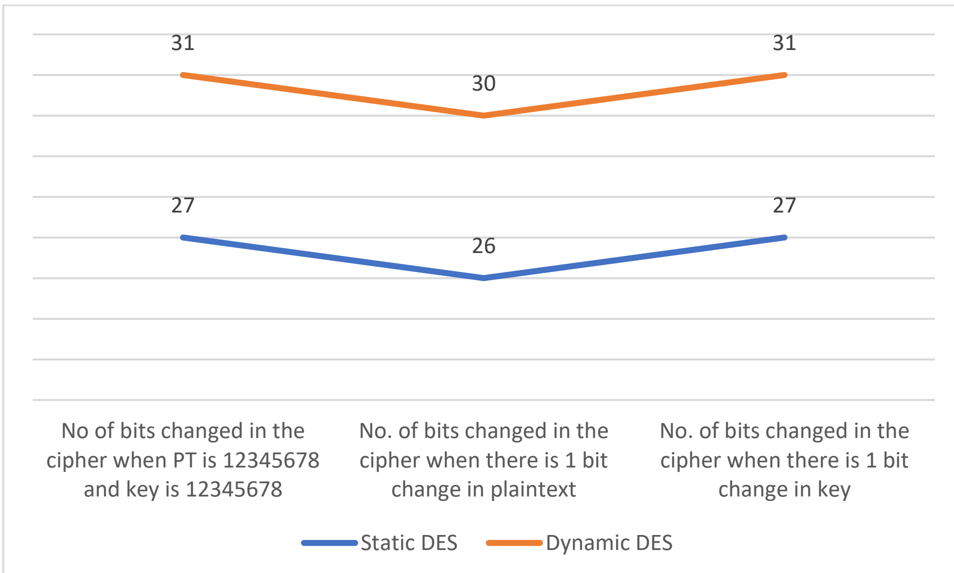
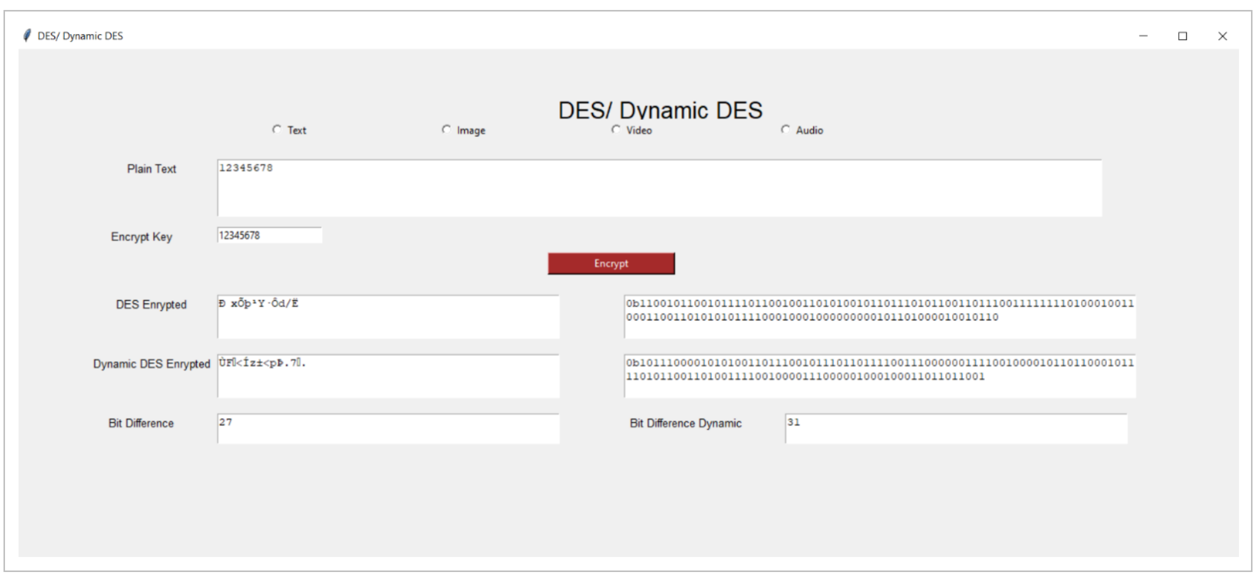


Figure 6 Avalanche effect of static and dynamic DES



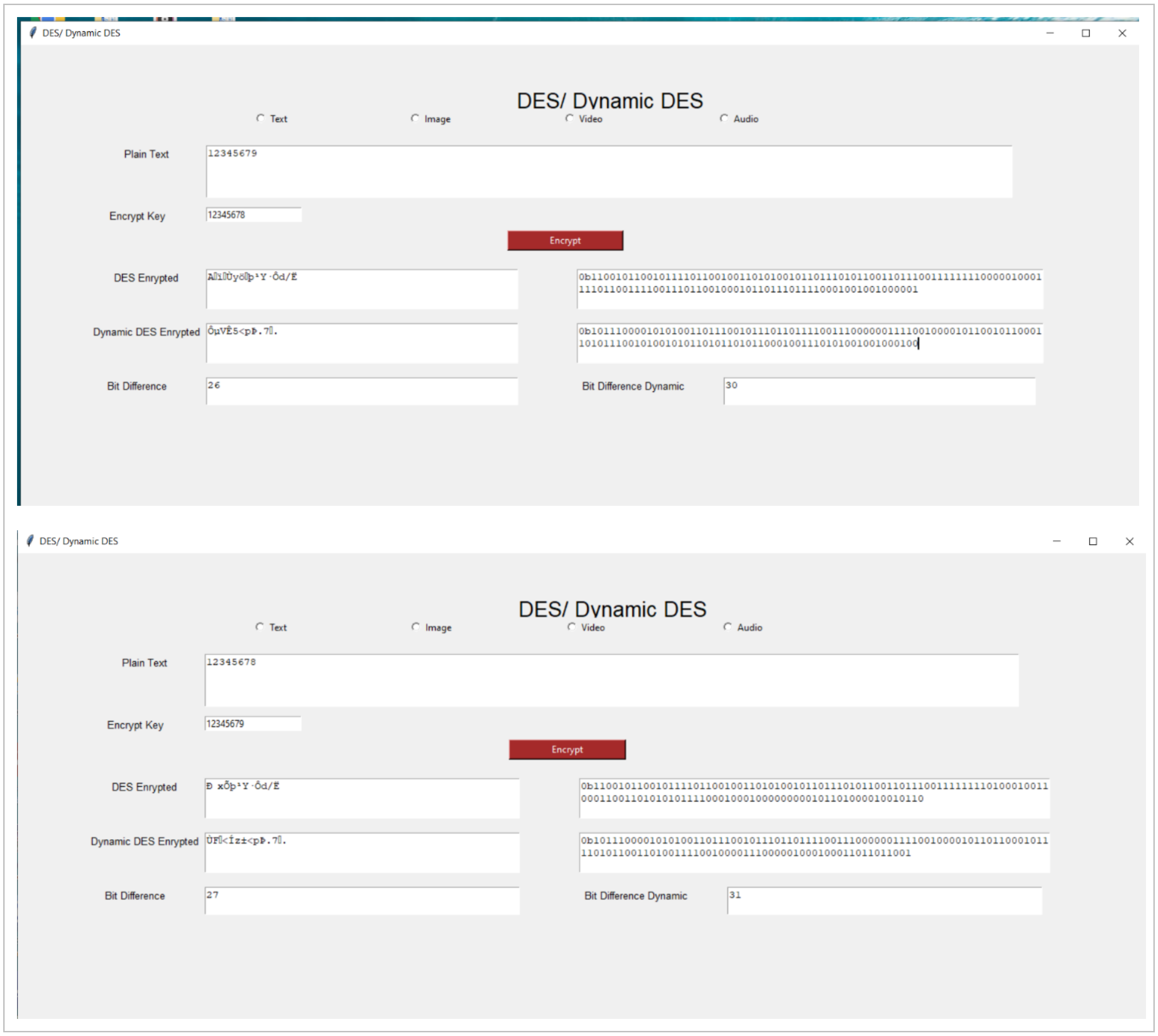


Figure 7 Snapshots while evaluating Avalanche criterion

Robustness of Linear Cryptanalysis

Differential and Linear Cryptanalysis are powerful cryptanalytic attacks on private-key block ciphers (Altaleb et al. (2017)). The complexity of linear cryptanalysis depends on the size of the largest entry in the Linear Approximation Table. Larger the value, the greater the cipher is prone to cryptanalytic attacks. Robustness to Linear Cryptanalysis has been explained with the help of Linear Approximation Table. The complexity of linear cryptanalysis depends on the size of the largest entry in the LAT. High value in a row of Linear Approximation Table specifies that the S-box is prone to linear cryptanalysis. Table 3 depict LAT of static and Table 4 depict LAT of dynamic DES.

Table 3 LAT-static DES

a	b															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	8	6	6	8	8	6	14	10	10	8	8	10	10	8	8
2	8	8	6	6	8	8	6	6	8	8	10	10	8	8	2	10
3	8	8	8	8	8	8	8	8	10	2	6	6	10	10	6	6
4	8	10	8	6	4	4	6	8	8	6	10	10	10	4	10	8
5	8	6	6	8	8	8	12	10	6	8	10	10	8	6	6	8
6	8	10	6	12	8	8	8	10	8	6	12	12	6	8	8	6
7	8	6	8	10	4	4	10	8	6	8	8	8	12	10	8	10
8	8	8	8	8	8	8	8	8	6	10	6	6	10	6	6	2
9	8	8	6	6	8	8	6	6	4	8	10	10	8	12	10	6
BA	8	12	6	10	8	8	10	6	10	10	8	8	10	10	8	8
B	8	12	8	4	8	8	12	8	8	8	8	8	8	8	8	8
C	8	6	12	6	8	8	10	8	10	8	12	12	8	10	8	6
D	8	10	10	8	12	12	8	10	4	6	8	8	10	8	8	10
E	8	10	10	8	4	4	8	10	6	8	6	6	4	10	6	8
F	8	6	4	6	8	8	10	8	8	6	6	6	6	8	10	8

By checking the Dynamic S-box and the static S-box, we can see that the highest value in static S-box is 14 and the highest value in Dynamic S-box is 12. Complexity of linear cryptanalysis is low in our Dynamic S-box as our largest entry is 12 compared to 14 in LAT of static DES.

Table 4 LAT-dynamic DES

a	b															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	10	10	8	8	6	8	8	8	6	6	8	10	6	6	12
2	8	6	8	6	8	10	8	10	6	4	10	8	8	4	6	8
3	8	8	6	10	12	12	6	10	10	6	8	8	10	4	4	4
4	8	8	4	6	8	10	10	8	8	6	10	10	10	6	6	4
5	8	10	10	8	8	8	8	6	4	10	10	12	8	4	4	4
6	8	8	10	10	8	8	8	10	8	6	6	10	6	8	12	8
7	8	8	6	4	10	8	10	4	6	10	8	10	12	6	6	8
8	8	6	4	4	4	12	10	10	6	6	8	8	10	8	10	10
9	8	12	6	6	2	8	6	6	4	8	8	6	8	8	10	10
A	8	4	6	4	6	8	6	12	10	8	10	8	10	8	2	10
B	8	10	6	8	10	6	8	10	8	10	8	10	8	8	10	8
C	8	4	4	8	6	10	12	12	10	4	8	8	8	10	10	6
D	8	6	10	6	6	6	8	6	4	6	8	6	10	10	6	6
E	8	8	12	8	8	10	6	6	6	10	8	8	4	8	10	10
F	8	2	8	6	6	8	8	8	8	8	8	10	6	6	6	12

Robustness to Differential Cryptanalysis

Differential Cryptanalysis are powerful cryptanalytic attacks on private-key block ciphers. The complexity of differential cryptanalysis depends on the size of the largest entry in the XOR table and the total no of zeros in the XOR table. It uses a Differential Distribution Table that contains the differentials. Table 5 depict the DDT of static DES and Table 6 depict DDT of dynamic DES.

Table 5 DDT of static DES

a’	b'															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Table 6 DDT of Dynamic DES

a’	b'															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	2	2	0	0	4	2	4	0	0
2	0	0	0	4	0	4	0	0	2	2	0	0	2	2	0	0
3	0	2	0	0	0	2	0	0	8	0	0	2	0	0	0	2
4	0	0	2	0	0	0	0	2	2	4	0	0	0	2	0	4
5	2	0	4	0	4	2	0	0	2	0	0	2	0	0	0	0
6	0	2	0	0	2	0	0	0	0	0	6	0	2	0	2	2
7	0	4	2	2	0	0	0	4	2	2	0	0	0	0	0	0
8	0	2	4	0	0	2	0	0	0	0	0	2	4	0	0	2
9	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2	2
A	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2	2
B	0	0	0	2	4	0	0	2	0	2	4	0	0	2	0	0
C	0	0	2	2	0	4	2	0	0	0	2	2	0	0	2	0
D	2	0	0	0	0	2	2	0	0	2	2	2	0	0	4	0
E	0	2	0	2	0	0	4	0	0	0	0	0	0	2	4	2
F	0	2	2	0	0	2	2	0	0	0	2	2	0	2	2	0

For a robust S-box, the number of non-zero entries should be higher. In the DDT OF Dynamic S-box, it contains a greater number of non-zero entries corresponding to static S-box. Higher the number of non-zero entries, larger is the robustness against differential cryptanalysis. Our dynamic S-box has low propagation criteria and it maintains good XOR profile, as it maintains small variations across the rows.

Table 7 and 8 depict the overall performance measures of original and dynamic DES in which above analysis, we can see that our Dynamic S-box outperforms static S-box in terms of linearity, SAC, Balance, Robustness to Linear and Differential Cryptanalysis.

Table 7 Performance value of original Sbox DES

Sbox	Index	Nonlinearity	Balance	XOR Table	LAT
DES Sbox1	1	18	True	16	14
	2	22	True		
	3	20	True		
	4	18	True		
DES Sbox2	1	18	True	16	10
	2	18	True		
	3	20	True		
	4	22	True		
DES Sbox3	1	18	True	16	16
	2	20	True		
	3	22	True		
	4	18	True		
DES Sbox4	1	22	True	16	16
	2	22	True		
	3	22	True		
	4	22	True		
DES Sbox5	1	20	True	16	14
	2	18	True		
	3	20	True		
	4	22	True		
DES Sbox6	1	20	True	16	14
	2	20	True		
	3	20	True		
	4	20	True		
DES Sbox7	1	20	True	16	14
	2	14	True		
	3	22	True		
	4	18	True		
DES Sbox8	1	22	True	16	16
	2	20	True		
	3	20	True		
	4	22	True		

Table 8 Performance value of dynamic Sbox DES

Sbox	Index	Nonlinearity	Balance	XOR Table	LAT
DES Sbox1	1	23.5	True	16	12
	2	25.5	True		
	3	25.5	True		
	4	23.5	True		
DES Sbox2	1	24.5	True	16	10
	2	23.5	True		
	3	23.5	True		
	4	21.5	True		
DES Sbox3	1	22.5	True	14	12
	2	23.5	True		
	3	22.5	True		
	4	25.5	True		
DES Sbox4	1	22.5	True	16	14
	2	22.5	True		
	3	22.5	True		
	4	24.5	True		
DES Sbox5	1	20.5	True	18	14
	2	23.5	True		
	3	25.5	True		
	4	22.5	True		
DES Sbox6	1	23.5	True	14	14
	2	23.5	True		
	3	20.5	True		
	4	23.5	True		
DES Sbox7	1	25.5	True	18	14
	2	21.5	True		
	3	23.5	True		
	4	25.5	True		
DES Sbox8	1	22.5	True	16	16
	2	24.5	True		
	3	25.5	True		
	4	25.5	True		

Conclusion

As stated earlier that, in today's world security is a key thing for every aspect and the main objective of today's digital data sharing is to protect data from various attacks, thereby increasing the mode of security to next level. So here in this paper we depicted an efficient multi-function Sbox generation using dynamic DES for securing digital data from various attacks. With the help of various function generating throughout 8 Sbox, attackers can't even guess the possibility as the level of security increased up to certain level. Also, this paper depicts 5 main criterions for evaluating dynamic and static DES under factors non-linearity, Avalanche criterion, Balance, Robustness to linear cryptanalysis, Robustness to differential cryptanalysis in which dynamic DES outperforms better than static DES in all criteria's and also shows better performance than AES and Triple AES (Adhie et al. (2018)).

Table 9 Abbreviations

AES	Advance Encryption Standard
DES	Data Encryption Standard
DDT	Differential Distribution Table
LAT	Linear Approximation Table
RSA	Rivest–Shamir–Adleman
SCTT	Simple Column Transposition Technique
VMS	Variable Mapping S-box
GA	Genetic Algorithm
LFSR	Linear Feedback Shift Register
PN	Pseudorandom Generator
SAC	Strict Avalanche Criterion
SNR	Signal to Noise Ratio
DPA	Differential Power Analysis

References

Hellman, M.E. (1979). I.des will be totally insecure within ten years'. *IEEE spectrum, 16*(7), 32-40.

Alani, M.M. (2010). DES96-improved DES security. *In 7th International Multi-Conference on Systems, Signals and Devices*, 1-4.

Manikandan, G., Rajendiran, P., Chakarapani, K., Krishnan, G., & Sundar Ganesh, G. (2012). A modified crypto scheme for enhancing data security. *Journal of Theoretical and applied information Technology, 35*(2), 149-154.

Shah Kruti, R., & Gambhava. B (2012). New approach of data encryption standard algorithm. *International Journal of Soft Computing and Engineering (IJSCE), 2*(1), 322-325.

Arya, G.P., Nautiyal, A., Pant, A., Singh, S., & Handa, T. (2013). A cipher design with automatic key generation using the combination of substitution and transposition techniques and basic arithmetic and logic operations. *The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), 1*(1), 21-24.

Wong, D.S., Fuentes, H.H., & Chan, A.H. (2001). The performance measurement of cryptographic primitives on palm devices. *In Seventeenth Annual Computer Security Applications Conference,* 92-101.

Rivest, R.L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120-126.

Juremi, J., Mahmod, R., & Sulaiman, S. (2012). A proposal for improving AES S-box with rotation and key-dependent. *In Proceedings Title: International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec),* 38-42.

Al-Muhammed, M.J. (2018). Light but Effective Encryption Technique based on Dynamic Substitution and Effective Masking. *International Journal of Advanced Computer Science and Applications, 9*(9), 614-628.

Singh, S., Maakar, S.K., & Kumar, D.S. (2013). Enhancing the security of DES algorithm using transposition cryptography techniques. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(6), 464-471.

Gupta, N. (2012). Implementation of optimized des encryption algorithm upto 4 round on spartan 3. *International Journal of Computer Technology and Electronics Engineering (IJCTEE), 2*(1), 82-86.

Patel, P., Shah, K., & Shah, K. (2014). Enhancement of Des Algorithm with Multi State Logic. *International Journal of Research in Computer Science, 4*(3).

Albassall, A.M.B., & Wahdan, A.M. (2004). Genetic algorithm cryptanalysis of a feistel type block cipher. *In International Conference on Electrical, Electronic and Computer Engineering, ICEEC'04,* 217-221.

Sharma, A.K., & Sharma, H. (2015). New Approach to Des with Enhanced Key Management and Encryption/Decryption System (Des Ultimate). *International Journal of Advances in Engineering & Technology, 8*(3), 368-377.

Krishnamurthy, G.N., & Ramaswamy, V. (2008). Making AES stronger: AES with key dependent S-box. *IJCSNS International Journal of Computer Science and Network Security, 8*(9), 388-398.

Mahmoud, E.M., Zekry, A., Abd El Hafez, A., & Elgarf, T.A. (2013). Enhancing channel coding using AES block cipher. *International Journal of Computer Applications, 61*(6), 28-33.

Zahid, A.H., Al-Solami, E., & Ahmad, M. (2020). A novel modular approach based substitution-box design for image encryption. *IEEE Access, 8,* 150326-150340.

Oukili, S., & Bri, S. (2017). High speed efficient advanced encryption standard implementation. *In International Symposium on Networks, Computers and Communications (ISNCC),* 1-4.

Alabaichi, A., & Salih, A.I. (2015). Enhance security of advance encryption standard algorithm based on key-dependent S-box. *In Fifth International Conference on Digital Information Processing and Communications (ICDIPC),* 44-53.

Altaleb, A., Saeed, M.S., Hussain, I., & Aslam, M. (2017). An algorithm for the construction of substitution box for block ciphers based on projective general linear group. *AIP Advances, 7*(3).

Anees, A., & Ahmed, Z. (2015). A technique for designing substitution box based on van der pol oscillator. *Wireless Personal Communications, 82*(3), 1497-1503.

Akande, O.N., Abikoye, O.C., Kayode, A.A., Aro, O.T., & Ogundokun, O.R. (2020). A dynamic round triple data encryption standard cryptographic technique for data security. *In*

International Conference on Computational Science and Its Applications, Springer, Cham, 487-499.

Ullah, A., Jamal, S.S., & Shah, T. (2018). A novel scheme for image encryption using substitution box and chaotic system. *Nonlinear Dynamics, 91*(1), 359-370.

Siddiqui, N., Khalid, H., Murtaza, F., Ehatisham-Ul-Haq, M., & Azam, M.A. (2020). A novel algebraic technique for design of computational substitution-boxes using action of matrices on Galois field. *IEEE Access, 8,* 197630-197643.

Khan, F.A., Ahmed, J., Khan, J.S., Ahmad, J., Khan, M.A., & Hwang, S.O. (2017). A new technique for designing 8× 8 substitution box for image encryption applications. *In 9th Computer Science and Electronic Engineering (CEEC),* 7-12.

Nilima, S., & Nitin, A. (2019). Randamization technique for desiging of substitution box in data encryption standard algorithm. *International Journal of Mathematical Sciences and Computing, 5*(3), 27-36.

Adhie, R.P., Hutama, Y., Ahmar, A.S., & Setiawan, M.I. (2018). Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC). *In Journal of Physics: Conference Series, 954*(1).

Akhtar, T., Din, N., & Uddin, J. (2019). Substitution box design based on chaotic maps and cuckoo search algorithm. *In International conference on advanced communication technologies and networking (CommNet),* 1-7.

Khan, F.A., Ahmed, J., Khan, J.S., Ahmad, J., & Khan, M.A. (2017). A novel substitution box for encryption based on Lorenz equations. *In International conference on circuits, system and simulation (ICCSS),* 32-36.

Arshad, S., & Khan, M. (2021). New extension of data encryption standard over 128-bit key for digital images. *Neural Computing and Applications,* 1-14.

Siddiqui, N., Yousaf, F., Murtaza, F., Ehatisham-ul-Haq, M., Ashraf, M.U., Alghamdi, A.M., & Alfakeeh, A.S. (2020). A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. *Plos one, 15*(11).

Khan, M.F., Ahmed, A., & Saleem, K. (2019). A novel cryptographic substitution box design using Gaussian distribution. *IEEE Access, 7,* 15999-16007.

Riaz, F., & Siddiqui, N. (2020). Design of an Efficient Cryptographic Substitution Box by using Improved Chaotic Range with the Golden Ratio. *International Journal of Computer Science and Information Security (IJCSIS), 18*(1), 89-94.

Rahaman, Z., Corraya, A.D., Sumi, M.A., & Bahar, A.N. (2020). A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix. *arXiv preprint arXiv:2005.00157.*

Alghafis, A., Munir, N., & Khan, M. (2021). An encryption scheme based on chaotic Rabinovich-Fabrikant system and S 8 confusion component. *Multimedia Tools and Applications, 80*(5), 7967-7985.

Ahmad, M., Khaja, I.A., Baz, A., Alhakami, H., & Alhakami, W. (2020). Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications. *IEEE Access, 8,* 116132-116147.

Seghier, A., & Li, J. (2019). Advanced encryption standard based on key dependent S-Box cube. *IET Information Security, 13*(6), 552-558.

Akande, O.N., Abikoye, O.C., Kayode, A.A., Aro, O.T., & Ogundokun, O.R. (2020). A dynamic round triple data encryption standard cryptographic technique for data security. *In International Conference on Computational Science and Its Applications*, 487-499.

Özkaynak, F., & Muhamad, M.I. (2018). Alternative substitutional box structures for DES. *In 6th International Symposium on Digital Forensic and Security (ISDFS),* 1-4.

Roslan, M.F.B., Seman, K., Ab Halim, A.H., & Sayuti, M.N.A.S.M. (2019). Substitution Box Design Based from Symmetric Group Composition. *In Journal of Physics: Conference Series, 1366*(1).

Kumar, A., & Sharma, A. (2017). Systematic literature review on opinion mining of big data for government intelligence. *Webology, 14*(2), 6-47.