Haithem and Lateef

Iraqi Journal of Science, 2019, Vol.60, No.9, pp: 2058-2066 DOI: 10.24996/ijs.2019.60.9.21





ISSN: 0067-2904

# **Intelligent TRIPLE DES with N Round Based on Genetic Algorithm**

### Mazin Haithem<sup>\*1</sup>, Rana Abdul Rahman Lateef<sup>2</sup>

<sup>1</sup>Department of Financial and Banking, Baghdad College of Economic Sciences University, Baghdad, Iraq <sup>2</sup>Department of Computer Science, Baghdad College of Economic Sciences University, Baghdad, Iraq

#### Abstract

This work presents an approach for the applying Triple DES (TRIPLE DES) based on using genetic algorithm by adding intelligent feature for TRIPLE DES with N round for genetic algorithm. Encapsulated cipher file with special program which send an acknowledgment to a sender to know who decipher or broken to crash it, Thus it is considered as the initial step to improve privacy. The outcome for proposed system gives a good indication that it is a promising system compared with other type of cipher system.

**Keywords:** TRIPLE DES, Cryptography, privacy, security, round, encapsulation cipher file, Genetic algorithm.

مازن هيثم<sup>1</sup>، رناعبدالرحمن لطيف<sup>2</sup>

<sup>1</sup>قسم المالية والمصرفية، كلية بغداد للعلوم الاقتصادية الجامعة<sup>،</sup> بغداد، العراق

<sup>2</sup>قسم علوم الحاسبات، كلية بغداد للعلوم الاقتصاديه،جامعة بغداد، بغداد، العراق

الخلاصة

ان هذا العمل يبين طريقة تطبيق ال TRIPLE DES اعتمادا على الخوارزمية الجينية عن طريق اضافة ميزة ذكية لل TRIPLE DES مع N من الدورات للخوارزمية الجينية وتغليف الملف المشفر ببرنامج خاص يقوم بأرسال اشعار الى المرسل ليعلمه من الذي قام بفك شفرة الفايل لاجل كسرها اوتحطيمها وبالتالي يمكن اعتبارها الخطوة الاولى لتحسين الخصوصية. النتائج التي تم الحصول عليها من النظام المقترح اعطىت مؤشر بان النظام وإعد مقارنة مع الانظمة الاخرى.

#### Introduction

The essential part of information technology is to achieve data security and privacy. Information security in data storage and transmission is becoming important as the fast grew of exchanging digital data in an electronic way. Cipher system considers to be the basic element for improving data security, in other hand decipher system is an important step for attack to broken secure data in all time, thus it must create a stamp for sender (cipher data) and one for who received(decipher) to guarantee the data received by a specific user [1]. Development of human intelligence with the art of cryptography has become more sophisticated in order to make information more secure. Cryptography using genetic algorithm has attracted more interest in recent years. There are primary types of cryptography a secret and a public key. Secret key cryptography is known as symmetric key cryptography where the encrypted (sender) and the decrypted (received) files has the same key. Public key cryptography is called asymmetric key cryptography which uses a pair of keys called private and public for encryption and decryption [2].

\*Email: mazin\_haitham@yahoo.com

There are two ways of key production, the first one is mathematical like AES, DES and the other one is based on the theory of natural selection [1, 2].

Cryptography generally uses DES algorithm for the Encryption and Decryption. DES using round and round strategy. The DES uses private key and its works by using the same key to encrypt and decrypt a data [3].

Many genetic algorithms based encryption algorithms have been successfully used in many papers. The basic idea of research on GAs has been introduced in many researches which gives it a robustness in security confidence.

Jun Song, et. al., 2007[4], Their paper stated a way for using genetic algorithm in cryptanalysis of tworound DES .Depending on fitness function they adopted a known plaintext attack to produce a variety of optimum keys and count every bit of them one by one to find some valuable bits, which generate a significant deviation from the other bits, thus, the 56-bit key is successfully gained without searching the whole search space. An experimental result specified that this is a promising method and can works with the other complex block ciphers. Gove Nitinkumar Rajendra, et. al., 2011[5], they proposed a new method to data security based on brain mutually waves and genetic algorithm and with pseudorandom binary sequence for encrypt and decrypt the data. The properties of such a method comprise a high data security and high feasibility for practical application. Poornima Naik, et. al., 2014[6], in their paper they try to exploit the randomness in crossover and mutation processes for generating a pair of asymmetric key used for encrypt and decrypt a messages. In their work they have used four crossover points, three mutation points and a single random byte and a permutation factor. The use of randomness with permutation makes the algorithm more robust and hard to break. Suvajit Dutta, et. al., 2014[7], their paper deals with the confidentiality of electronic data which is transmitted over the internet by using the concept of genetic algorithms with pseudorandom function to encrypt and decrypt data stream. The encryption process is applied over a binary file. They proposed genetic algorithm depends on a method of encrypt a secret key which obviously it satisfied the goals that are required in any encryption method for encrypt binary files. Purvi Garg, et.al. 2015[8], in their paper they stated that ring crossover operator using genetic algorithms has been used in performing cryptanalysis of SDES. The scope of this paper is restricted to a cipher text attack. Keys are generated by different combinations using Genetic Algorithm and hence it is deduced that Genetic Algorithm is a better method than the Brute Force for analyzing SDES. Ms. B. D. Nagpure, et. al., ,2016[9],their paper stated at a cryptography based on Genetic Algorithm to implement security of information and data transmission so as to provide confidentiality, integrity, authentication and non-repudiation of the messages. A private key is used to encrypt a plain text of receiver to outcome an intermediate cipher which encrypted again using genetic algorithm to outcome a final cipher.

#### Genetic algorithm

The Genetic Algorithm (GAs) is a planning to move from one populace of "chromosomes" (or "bits") to another populace by utilizing a kind of "normal choice". Every chromosome comprises of "qualities" (e.g., bits), every quality being an example of a specific "allele" (e.g., 0 or 1). Hereditary calculations can be isolate into the accompanying three sorts of fundamental operation: selection, hybrid, and change. Selection depends on the wellness incentive to choose chromosomes in the populace for multiplication. The fitter the chromosome, the more circumstances it is probably going to be imitated. In Crossover a hybrid administrator has an essentialness as that of hybrid in a characteristic hereditary process. For instance, a strings 10000100 and 11111111 could be traversed after the third locus in each to deliver the two posterity 10011111 and 11100100. The hybrid administrator generally imitates natural recombination between two single chromosome creatures [10]. In Mutation: it is a hereditary administrator arbitrarily flips a portion of the bits in a chromosome. For instance, the string 00000100 may be transformed in its second position to yield 01000100. Transformation can happen at each piece position in a string with some likelihood, typically little. [11, 12]

#### **TRIPLE DES**

TRIPLE DES or the Triple Data Encryption Algorithm (TDEA) was produced to address the conspicuous blemishes in DES without outlining a radical new cryptosystem. It additionally has the benefit of demonstrated unwavering quality and a more extended key length that takes out a large number of the assaults that can be utilized to lessen the measure of time it takes to break DES [13]. Information Encryption Standard (DES) utilizes is a 56-bit key and isn't considered appropriate to

encode oversensitive information. TRIPLEDES essentially broadens the key size of DES by execute the calculation three times in progression utilizing three different keys. The consolidated key size is in this manner 168 bits (3 times 56). TDEA includes with three 64-bit DEA keys (K1, K2, K3) in the mode Encrypt-Decrypt-Encrypt (EDE), that is, the plain content is scrambled with K1, at that point unscrambled with K2, and afterward encoded with K3 [14]. The guidelines represents three of keying choices:

1-The more favored alternative, actualizes three commonly free keys (K1  $\neq$  K2  $\neq$  K3  $\neq$  K1). It gives key space of  $3 \times 56 = 168$  bits.

2-Implement two commonly autonomous keys and a third key that is the same as the main key (K1  $\neq$  K2 and K3 = K1). This gives key space of 2 × 56= 112 bits.

3-a key heap of three comparable keys (K1 = K2 = K3). This choice is comparable to DES Algorithm. In TRIPLEDES the three times emphasis is connected to build the encryption level and normal time [15, 16]. Triple DES runs three times slower than DES, however is considerably more secure and confident if utilized appropriately [17].

## **Proposed system:**

The information transferring through e-environment thus must improve the data privacy and security between sender and receiver to avoid any intrusion or damage on transfer data. In this section a new feature to TRIPLE DES add by merge it with genetic Algorithm and then covered with any executable file with track ability.

The first step to re-code TRIPLE DES file is start with genetic algorithm thus dealing with data that based on ASCII.

Note ASCII code start from 0 to 255 in binary system  $=2^8$  refer to 8bit for all character of input file as shown in Table-1.

In this work the following algorithms have been used to implement the proposed system:

#### Algorithm 1

## Main algorithm

Input (TRIPLE DES file)

Output (cipher file)

1- initial population from plan-text(TRIPLE DES output) (by div block as chromosomes )

- 2- Genetic sub
- 2.1 calculate fitness function (depend on privilege )
- 2.2 genetic operation
- 2.3 save data
- 2.4 goto 2.1
- 3- Detect sender TX and receiver RX
- 4- truck it
- 5- if attack occurring then save in log file TX /RX (depend on acknowledge  $\ )$
- 6- encapsulation function
- 7- goto 2 increment privilege

## Algorithm 2

fitness function

/\*

depend on privilege

privilege mean as the following example

if current string

 $Line1 = \underline{\mathbf{A} \ \mathbf{B} \ \mathbf{C} \ \mathbf{D} \ \mathbf{E} \ \mathbf{F} \ \mathbf{G} \ \mathbf{H}}$ 

as input for TRIPLE DES and output of TRIPLE DES as:

Line 2=	9	ф	G	ى	â	6	ای	Ξ
And ASCII cod			-	÷		-		

 57
 15
 71
 239
 131
 231
 54
 232
 240

 Then binary convert as

00111001000011111000001111100111001101101110100011110000Check if random number add to current ASCII is not near to source data and not same number.

example

code cod

 $A \rightarrow 65 \rightarrow 57 \rightarrow 9$ Which refer to random increased code \*/Input( process TRIPLE DES line of 8 character ) Output( new line) 1-start 2-if call function(sum of random) >3 then line ok = true3-end Algorithm 3 function(sum\_of\_random) as integer input (line1, line 2) output (integer value of randomity) 1- start 2-loop check l6ine 1[i], line 2[i] different if different > 3 and i <6 then exit i++ until i>8 3- end algorithm 4 // track algorithm Input (cipher file) Output(cipher with sender and receiver rout [primary and secondary], flag ) 1- start 2- read cipher file and detect sender 3- read receiver by detect Primary rout and secondary rout) 4- send file and check 5- if same rout then flag = true else flag = false6- end algorithm 5 // same rout (using to track) Input (sender and receiver rout [primary and secondary], acknowledge) Output(true |false) 1- start 2- sum++ 3- read current station 4- if current station in( primary or secondary)station list then sum --5- if sum=0 then output=true else output=false end if 6- end algorithm 6 // encapsulation output Input (cipher data) Output(encapsulation cipher data) 1- start 2- select encapsulation method with (exe format, JPG format .....etc.) 3- implementation of selection method on input 4- end **Experimental result:** 

Using a simple file of TRIPLE DES as a segment test to implement it is shown in Figure-1 and Figure-2. The complexity test depends on irregular value that come and give final cipher file as shown in a curve in Figure-3 and Figure-4 represent the complexity chart result from Table-2.

#### Conclusion

1-cipher /decipher time is high speed when comparing current algorithm with another cipher algorithm using genetic as main engine.

2- new feature for algorithm add with detect whom receive.

3-while increasing cipher file size then increase complexity because of need more time to analysis file. 4-security while any problem appear with file automatic acknowledgement will be send to sender(as new function).

1         1	a + , P, 8	Com First Long Long Long Long Long Long Long Long	
1         2         3         1		157 97 139 157 138 80 132 46	Transmission and a second to a second the second se
i         i	Property and the department of the property of the second se	history and any manufactory and all an \$4,000 all and a statement \$10,000 all	
1         2         2         3         4         3         4         3	The second s		
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	provide states and a state of states and states an	and the second	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		152 244 230 181 212 224 76 152	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		347 50 176 120 367 248 222 178	
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	W A * V 2 J * 1	87 735 715 88 706 339 61 542	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		332 245 350 115 257 228 207 551	
$ \begin{array}{  c  c  c  c  c  c  c  c  c  c  c  c  c$	6 6 T z 0		
$ \begin{array}{  c  c  c  c  c  c  c  c  c  c  c  c  c$	2 ± 1 2 % 1	provide and an a state of the s	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	D : L = T + C	has been addressed on the second se	10100100 10110001 10010001 01011010 10001001
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$		anteriors and statement and an inclusion of the province and the province and province and province of the pro	00111000 10001110 11010101 01010100 11001100 10011010 00111011 10001100
		and the second	01111100 10001000 01101001 11000100 01100000 01110111 01100010 01101010
			01000101 10011011 11000101 11010111 10111101 10001010 11110100 01111101
$ \begin{array}{  c c c c c c c c c c c c c c c c c c $			01101100 01111001 11101101 10110101 11100100
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$		became and the problem of the second se	
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$			01011101 01101010 11011101 10100110 11010101 01011001 01111001 1000000
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	1.13		<ul> <li>Non-statistical and additional and additional additionadditional additional additional additional additional additional</li></ul>
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$		The second	
$ \begin{array}{  c   c  c  c  c  c  c  c  c  c  c  c  $	present spines by provide and a single provide provide strength		
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	In the second seco		
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$			
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $			
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	4 6 0 1 8 4 5 6	125 54 241 134 235 237 142 224	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	< 3 - 8 - 7	66 73 189 133 180 56 233 589	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		100 239 56 137 347 157 102 589	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	3 4 1 E E g +	157 180 148 90 540 153 141 349	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	a 1 5 a 5 4 W	125 199 341 112 212 181 87 168	
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$			
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	3 3 6 4 8 1 5	Instantian and the second design of the second se	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $			
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		and a second	10111110 11001011 01110110 00111110 011011
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	0 1 4 0 1 0 1	and the second	01101110 11000101 11101110 00111000 11100110 10110011 01010101 10100110
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	present and the second state of the second sta	and the second	10010110 10100010 01001110 11011110 01000101 100100
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	interesting the second states of the second states and the second	and the second sec	11110010 10110101 11011111 11110001 11010111 1010010
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		testilizer andri den internal erizieren stilten erizierte erizierte alleratione	10111011 11001000 01110100 00111100 01101011 101101
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $			11100011 10100110 11010000 11100010 11000111 11001010 0011011
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	provide a state of the second state of the sec		10101100 10111001 01100100 11110101 01011100 10101000 100100
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	and the second state of th	International sectors to an entering a constant of the sector of the sec	11110000 10110011 10101000 11101111 10011111 10100010 11010110 01011111
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $			
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	· · ·	and the set of the set	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	4 - b 0 Z   5 c	170 181 98 341 90 186 144 99	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	3 4 8 7 9 7 9 9	389 707 190 61 197 131 297 118	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	- 1 3 : ) 4 1 5	133 146 115 58 108 129 308 115	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	DT=NJ*5+	79 165 307 78 398 348 53 134	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	- 10 L 0 L - X	118 184 151 344 344 167 145 553	produced by additional and a definition of the product of the prod
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$		53 150 393 230 383 333 49 572	
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	0 0 T 0 K 4 . C		
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	A real property of the second s		
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	The second se	and the second	
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$	the second	and wai and a state to a state of the state	
$ \begin{array}{ c c c c c c c c c c c c c c c c c c c$			
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $			
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	In the local division of the local divisione		
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	international Property in the Property of the		
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $			
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		particular in the second se	10010111 10100100 01001111 11100000 01000111 100100
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	and the second s	The second secon	11110100 10110111 10101100 11110011 10100011 10100110 110110
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	the second	Instance of the second se	10111101 11001010 01110101 00111110 011011
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		and the second	00111001 11000100 10111001 00111000 10110000 0111111
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	the same strength of the same	includes a finite of a first of the second state of the second sta	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	- ] ۲ ش ۴ 1 و ۴		
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	1 2 2 4 0	Instance of the second s	
*         U         €         8         J         y         -         H2         198         75         128         6         140         121         128         10010011         100101011         101010101         01000010         00001110         01111001         011000010         10000001         100000001         100000001         100000001         100000001         100000001         100000001         1	3 F 1 L + X C		
1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	the second descent second side is a second se	147 159 75 239 66 140 121 129	
		92 1.18 220 238 212 381 67 548	
		185 197 113 37 204 180 199 197	
	1		Tratting Lingen Lating Lating Lating Lating Lating

Figure 1-initial input of 64 line of 8 character to process

(a) IIIDES block (b)

ASCII code for input

convert input ASCII to binary

(c)

00000100	00000101	00000011	00000001	00000100	00000001	00000001	00000100
11011001 00000100	10011100 00000011	11000110 00000100	11011000 00000011	10111110 00000101	10001011	10111111	01111110 00000011
01101101 00000100 10010101	01111010 00000010 01011000	11101101 60000011 10000010	10110110 00000001 10010100	11100101 00000100 01111001	01101001 00600011 01000111	01010100 00000001 01111011	01011011 00000101 11001100
00000101	00000100	00000100	00000011	00000101	00000101	00000010	00000011
00000101 01010000	00000010	00000101	00000010	00000001 11001000	00000011 11001010	00000011	00000101 10001000
00000101	00000100	00000100 01100101	00000101	00000001	00000001	00000010	00000011 01100110
00000001	00000010	00000101 10001100	00000010	00000001 10000011	00000011 10000110	00000011 10111010	00000010
00000010 01101000	00000100 01110101	00000001 11101000	10110001	0000001 11100000	00000010 01100100	00000100	00000100 11101001
00000001 10001111	00000011 01010011 00000100	00000001	00000010	00000010	00000101 11010101	00000011	00000010
00000100 01011001 00000101	01100110	00000100 01000110 00000100	11010111 00000010	00000100 00111110 00000101	00000101 01010101 00000010	00000001 00111111 00000010	00000010 01000111 00000101
10110101	01000100	01101101 00000101	10110101	01100101 00000001	00110010 00000101	10011100	11101101 60000010
11011101	11101601 00000001	11001010	01011101	11000001 00000101	11011000	11000011	11001011 00000001
01110001	11000111 00000101	11110001 00000101	00111011 00000100	11101001 00000001	10110110 00000001	01010111 00000011	10101000
10011000 00000101	10100101 00000011	01010000	11100001 90000010	00000001	18010108 08060108	01111111 00000100	10000110 00000001
11110101 00000001	10000011 00000101	10101101 00000101	10111111	10100100	01110010 00000010	11011011 00000011	01100100 00000100
01010100 00000010 01111011	01100001 00000011	11010100 00000001 01101000	10011100	11001011 00000010 01100000	01010000	00111010 00000100 01100001	01000010
00000001	00111110 00000101 11100100	00000010	01111010 00000001 01011000	00000010	11110101 00000010 11010011	00000101	11101000 00000101 11000110
00000010	00000100	00000001	00000011	00000010	00000011	0000010	00000001
00000101 00110101	00000100	00000100 10110110	00000100	00000101 10101101	00000001	00000010	00000011 10110110
00000101 01011101	00000010	00000101 13011101	00000011 01011100	0000001	00000011	00000011	00000001
00000001 10111001 00000001	00000101 11000110	00000101 01110001 00000101	00000101	00000010 01101001 00000001	00000001 10110101 000000011	00000010	00000011 01110010 00000010
11100000	00000010 10100100 00000101	10011000	00000011 11011111 00000101	100000001 10010000 00000010	10010011 00000010	00000011 11000111 00000100	00000010
01110101	10000001	11110101 00000010	10111101	11101100	01110000	01011011	11110110
10011100 00000010	01011111	01010100 0000001	10011011 00000010	01001100	11100001 00000010	10000010	11010011 00000101
11000011 00000011	11010000	10110000 00000010	01111001 00000100	10101000 00000011	10111111 00000101	10101010 00000101	10110001 00000010
01011000 00000101	10101110 00000100	11011000 00000101	01010111	11001111 00000001	10011101 00000101	00111110 00000010	10001111 00000011
11101001 00000001 01111101	11110110 00000010 11010100	11010110 00000101 00110110	01101010 00000010 01000111	11001110 00000101 11110101	11100101 00000100 11000011	11001111 00000011 01100100	11010111 00000001 10110101
00000001	00000101	00000101	00000101	00000001	00000010	00000011	00000100
00000001 00111001	00000011 10001111	00000001	00000010	00000010 10110001	00000100	00000100	00000010
0000010	00000001 01101101	00000001	00000001 10101001	0000001	00000010 01011100	00000011 01000111	00000100
00000010 10001000	01001011	00000001	00000100 10000111	00000010 01101100	00000100	01101110	0000010
00000010 11100100 00000010	00000001 11110001 00000101	00000010 10011100 00000001	00000001 01100101 00000100	00000011 10010300 00000010	00000010 11100000 00000001	00000101 11001010 00000100	00000001 11010010 00000011
01000011 00000001	11001111	11111001	010000100	11110000	10111110	11110010	01111011
01000010 00000101	01001111	11000010 00000001	10001010 00000011	10111001 00000001	00111110	11110000	11000011 00000001
01101001 00000001	11110100	11101001 00000101	01101000 00000101	11100001 00000010	00000001	01001111 00000011	10100001 00000100
11000101 00000010	11010010 00000010	01111110 00000001	01000110	01110101 00000001	11000001 00000100	10101100	01111110
11101101 00000010 10000001	10110000 00000101 10001110	10100101 00000001 00111001	11101100 00000001 11001010	10011100 00000010 11111001	10011111 00000011 01111101	11010011 00000100 01100111	01011100 00000101 00111010
00000010	00000100	00000010	00000011	00000011	00000101	00000100	00000011 11100000
00000010	00000001	00000010	00000010	00000010	00000011	00000100	00000011
00000001 11001110	00000010 01011101	00000104 10000110	11001101	00000001 0111110	00000011 01001011	00000011 10110101	00000101 00111110
00000101 11110110	00000100	00000001 11100011 00000101	00000101	0000001 11011010	0000001	00000010	11100100
00000001 10001010 00000010	00000010 11100000 00000001	010000101 00000001	00000010 01010100 00000101	00000001 00111010 00000001	00000100 11001111 00000010	01110000	00000010 11000001 00000100
10110001	10111110	01101001 00000001	00110010	01100001 00000010	10101101 00000101	10011000	10011111 00000010
01000110 00000010	10011100 00000001	11000110 00000001	11011000 0000001	10111101 00000010	10001011 00000010	11110100 00000100	01111103 00000100
01101101 00000101	01111010 00000001	11101101 00000100	10110101 00000010	11100100 00000101	01101001 00000010	01010011 00000010	01011011 00000101
00110110 00000101 10010011	11000010	00000101	00110101 00000100	11100011 00000001 01000010	10110001 00000101	00000011	10100011 00000100 10000001
00000101	10011111 00000011 01111101	01001011 00000100 10100111	11011011 00000010 10111001	00000101	00001110 00000100 01101100	01111001 00000010 10100000	00000001
00000001	00000101 01011011	00000101 11001110	00000100	00000001 11000110	00000001 01001010	00000011 00110101	00000100
00000101 01110110	00000011 00111001	00000001	00000011	0000001	00000100	00000100	00000001 10101101
00000001 11010010	00000101	00000101	00000001 01010011	00000010 10000010	00000010 11001110	00000011 10111000	00000100 10001011
00000101 10011011 00000101	00000101 01011111 00000011	00000100	00000001 10011011 00000100	00000100 01001011 00000101	00000010 01001110 00000001	00000010	00000101 11010011 00000011
11111000 00000101	00000011 00111101 00000010	10110000	00000100 01111000 00000001	10100111 00000001	00000001 11110100 00000011	11011110	10110001 00000001
01010111	11100010 00000100	11010111	01010110 00000101	11001111	10011100 00000001	00111101 00000010	10001111
01111110 00000001	10001011 00000010	01101100 00006101	00110100 00000011	01100011 00000001	01111010 00000011	01100101 00000011	01101100 00000001
11011011 00000001	01101001 000000101	10010011	11011010 00000101	10001010 00000010	01011000	11000001	01001010
00111010 00000100 00111001	01000111 00000101 10001111	11101111 00000011 10111001	10000011 00000101 11001011	11100111 00000100 10110000	00110110 00000010 0111110	11101000 00000001 11100111	11110000 00000101 01110000
0000101	00000100	00000100	00000011 10101000	00000100	00000101 01011100	00000010	00000010
00000100	00000001 01001010	00000100	00000101 10000110	00000101 01101100	00000011 00111001	00000010	00000101 11110100
00000101 11100011	00000100	00000100 10011100	00000100 01100100	00000100 10010011	00000101 11011111	00000010	00000010 11010010

Figure 2-process result for TRIPLE DES

Table 1-

Table 1-		
III DES	Cipher	Different
157	160	3
97	101	4
139	141	2
157	161	4
130	132	2
80	85	5
132	137	5
66	68	2
50	52	2
63	64	1
178	181	3
122	124	2
169	172	3
245	248	3
77	79	2
85	88	3
142	146	4
81	82	1
01	02	
123	126	3
141	142	1
115	119	4
64	67	3
116	117	1
198	203	5
234	239	5
247	251	4
163	167	4
107	110	3
		5
154	159	
58	59	1
237	240	3
192	195	3
102	107	5
241	243	2
230	235	5
101	104	3
222	223	1
224	228	4
	79	
76		3
157	158	1
247	249	2
60	61	1
176	177	1
120	122	2
167	170	3
243	245	2
222	226	4
176	181	5
	90	
87	30	3
226	230	4
215	217	2
86	90	4
206	209	3
209	214	5
61	66	5
142	146	4
232	237	5
245	248	3
160	164	4
105	108	3
152	157	5
228	233	5
207	209	2
161	164	3

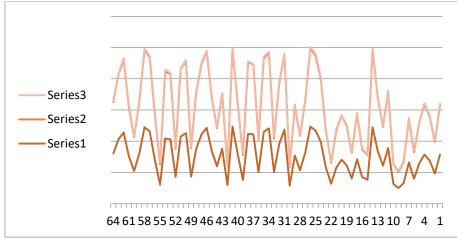


Figure 3-complexity chart for irregular value

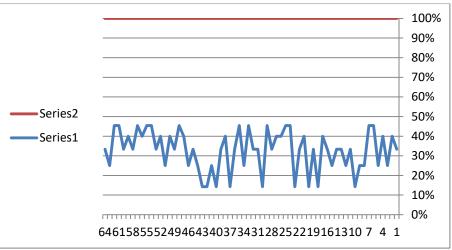


Figure 4-complexity chart for different value

Table 2- ASCII code for character and its binary representatio	m
--	---

ASCII	char	Binary
65	А	01000001
66	В	01000010
89	Y	01011001
90	Z	01011010

## References

- 1. Jhingran, R., Thada, V. and Dhaka, S. 2015. A Study on Cryptography using Genetic Algorithm", *International Journal of Computer Applications*, 118(20): 10 14.
- **2.** Goyat, S. **2012.** Cryptography Using Genetic Algorithms. *IOSR Journal of Computer Engineering (IOSRJCE)*, **1**(5): 06-08.
- **3.** Nagpure, B. D., Dhote, A. D., Rokade P. S., Kale P. B. and Kinhikar, N. S. **2016.** Implementation of Network Security Using Genetic Algorithm, *International Journal of Research in Advent Technology (IJRAT)*, Special Issue ,National Conference "Convergence 2016", 06th-07th April.
- 4. Song, J., Zhang, H., Meng, Q. and Wang, Z. 2007. Cryptanalysis of Two-Round DES Using Genetic Algorithms", Springer-Verlag Berlin Heidelberg, pp: 583–590.
- 5. Rajendra, G. N. and kaur, B. R. 2011. A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves", *International Journal of Scientific and Engineering Research*. 2(5): 01-04.

- 6. Naik, P. and Naik, G. 2014. Asymmetric Key Encryption using Genetic algorithm, *International Journal of Latest Trend in Engineering and Technology*, (IJLTET), **3**(3).
- 7. Dutta S., Das T., Jash S., Patra D. and Paul P. 2014. A Cryptography Algorithm Using the Operations of Genetic Algorithm & Pseudo Random Sequence Generating Functions, *International Journal of Advances in Computer Science and Technology*, 3(5): 325-330.
- **8.** Garg P. and Bhardwaj, S. **2015.** Cryptanalysis of Simplified Data Encryption Standard Using Genetic Algorithm. *American Journal of Networks and Communications*. **4**(3): 32-36.
- 9. Nagpure B. D., Dhote A. D., Rokade P. S., Kale P. B. and Kinhikar N. S. 2016. Implementation of Network Security Using Genetic Algorithm, *International Journal of Research in Advent Technology (IJRAT) (Special Issue) National Conference* "CONVERGENCE 2016", 06th-07th April.
- Bhasin H. and Bhatia S. 2011. Application of Genetic Algorithms in Machine learning", IJCSIT, 2(5).
- 11. Mitchell Melanie. 1999. An Introduction to Genetic algorithm, A Bradford Book, The MIT Press.
- **12.** Almarimi A. **2010.** A New Approach For Data Encryption Using Genetic Algorithms, and Published in: Proceeding CERMA '10 Proceedings of the IEEE Electronics, Robotics and Automotive Mechanics Conference.
- **13.** Triple Data Encryption Standard (Triple-DES), ttps://www.vocal.com/cryptography/tdes/ Triple Data Encryption Standard (Triple-DES).html.
- 14. "3DES", http://www.cryptosys.net/3des.html.
- **15.** Kakkar A, Singh M. L. and Bansal P.K. **2012.** Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network, *International Journal of Engineering and Technology*, **2**(1): 87-92.
- **16.** Kumar A., Jakhar S. and Makkar S. **2012.** Comparative Analysis between DES and RSA Algorithm's, *International Journal of Advanced Research in Computer Science and Software Engineering*, **2**(7): 386-391.
- 17. Aamer, N. 2005. "A Performance Comparison of Data Encryption Algorithm," IEEE.