ISSN: 0067-2904

Intelligent TRIPLE DES with N Round Based on Genetic Algorithm

Mazin Haithem*[1], Rana Abdul Rahman Lateef[2]
[1]Department of Financial and Banking, Baghdad College of Economic Sciences University, Baghdad, Iraq
[2]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.

التشفير الثلاثي القياسي الذكي مع عدد غير محدد من الدورات اعتمادا على الخوارزمية الجينية

مازن هيثم*[1]، رناعبدالرحمن لطيف[2]
[1]قسم المالية والمصرفية، كلية بغداد للعلوم الاقتصادية الجامعة، بغداد، العراق
[2]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 اعطت مؤشر بان النظام واعد 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 two-round 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 ≠ K2 ≠ K3 ≠ K1). It gives key space of 3 × 56 = 168 bits.

2-Implement two commonly autonomous keys and a third key that is the same as the main key (K1 ≠ 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= **A B C D E F G H**
as input for TRIPLE DES and output of TRIPLE DES as:
Line 2= 9 ☼ G ي â 6 ك ≡

And ASCII cod

57	15	71	239	131	231	54	232	240

Then binary convert as

00111001	00001111	10000011	11100111	00110110	11101000	11110000

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

A→ 65 →57 → 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= true
3-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 = false
6- 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-3and 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).

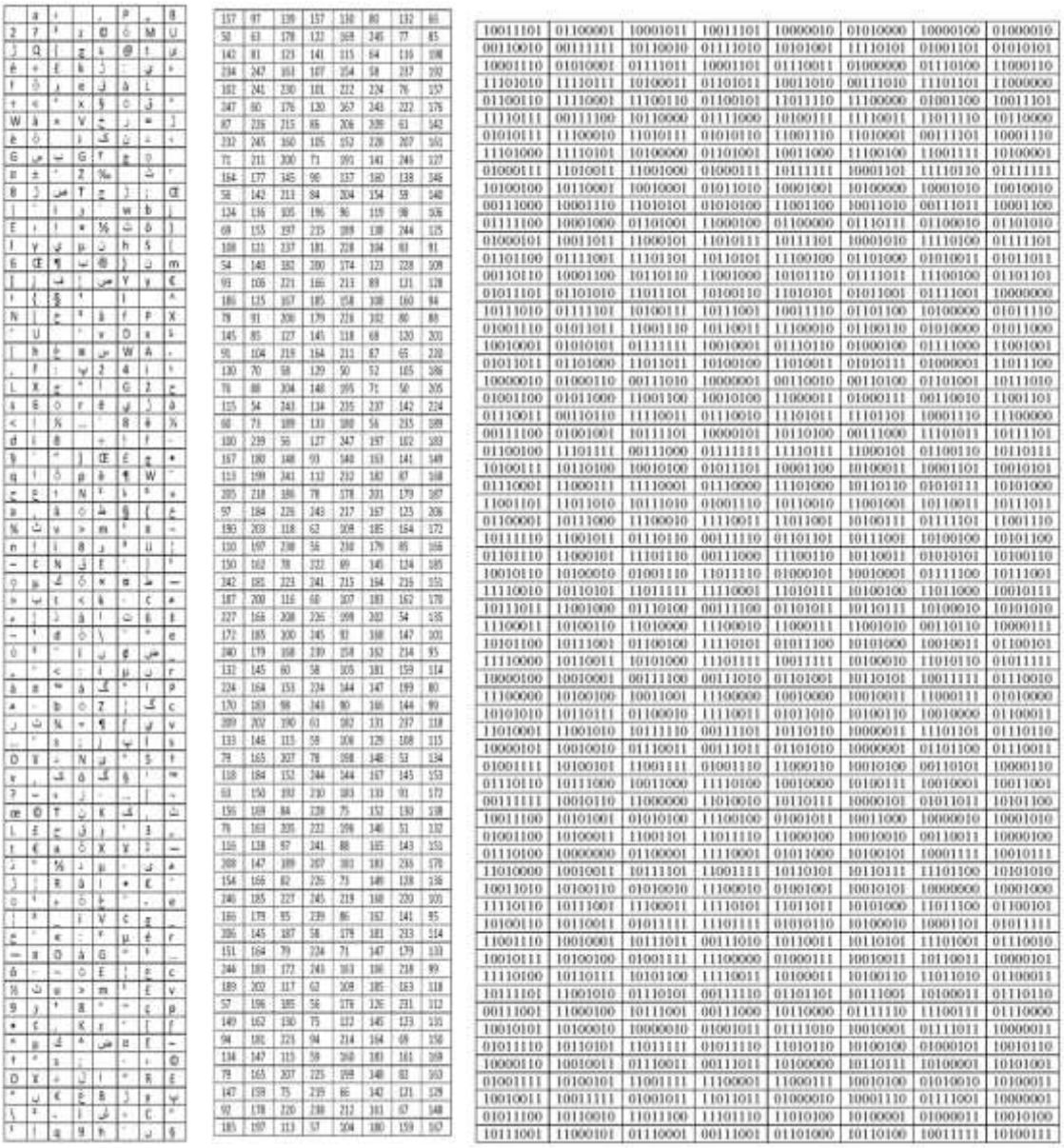

Figure 1-initial input of 64 line of 8 character to process

(a) IIIDES block (b) ASCII code for input (c) convert input ASCII to binary

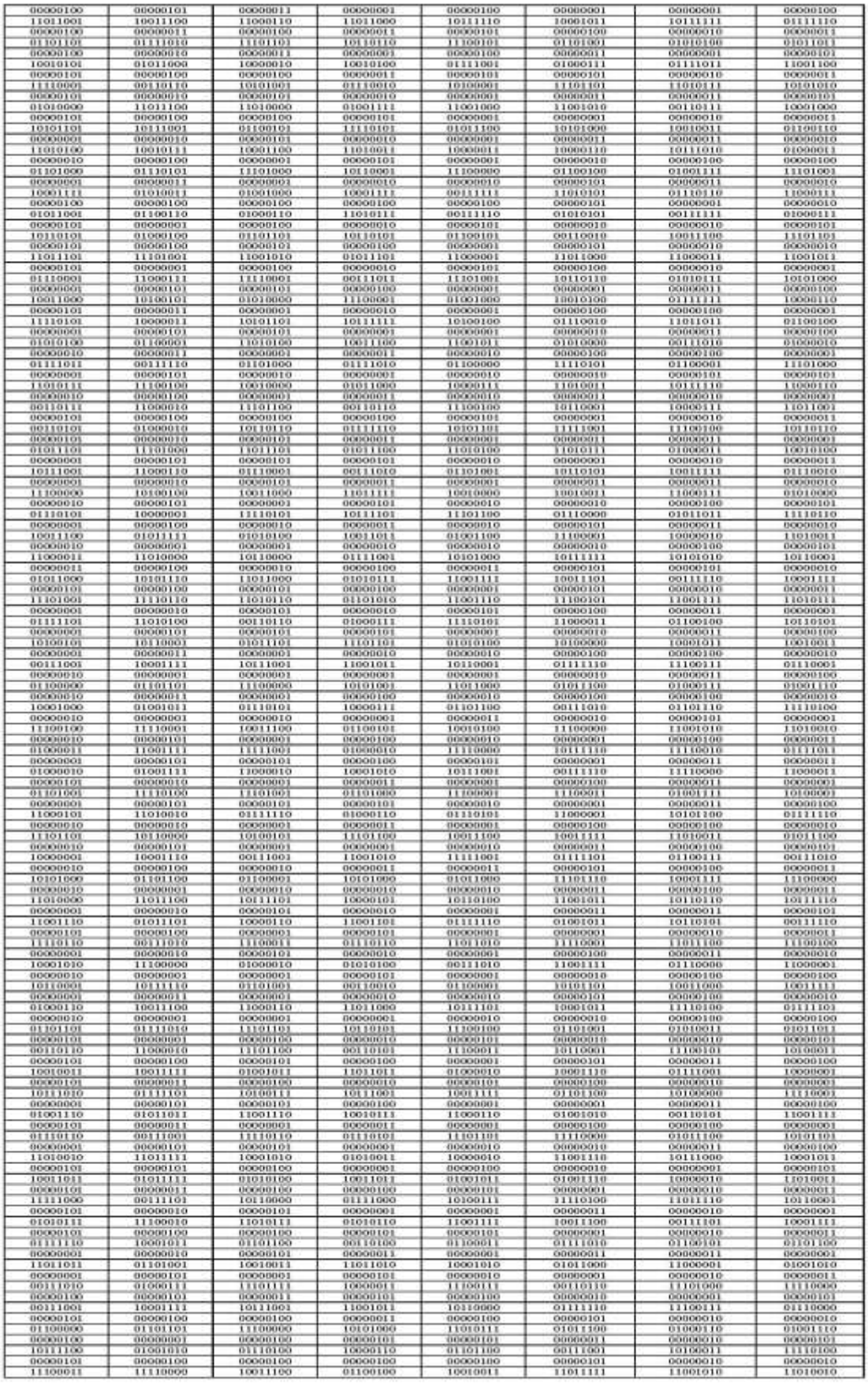

Figure 2-process result for TRIPLE DES

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
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
154	159	5
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
76	79	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
87	90	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

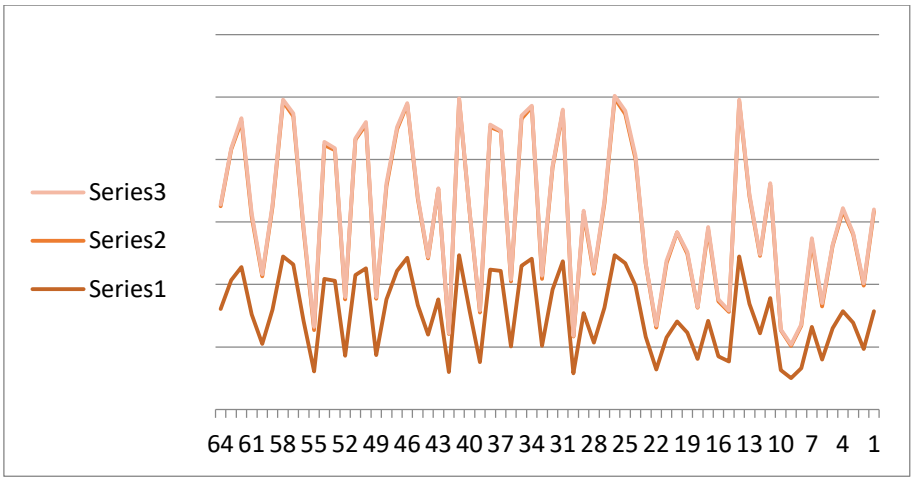

Figure 3-complexity chart for irregular value

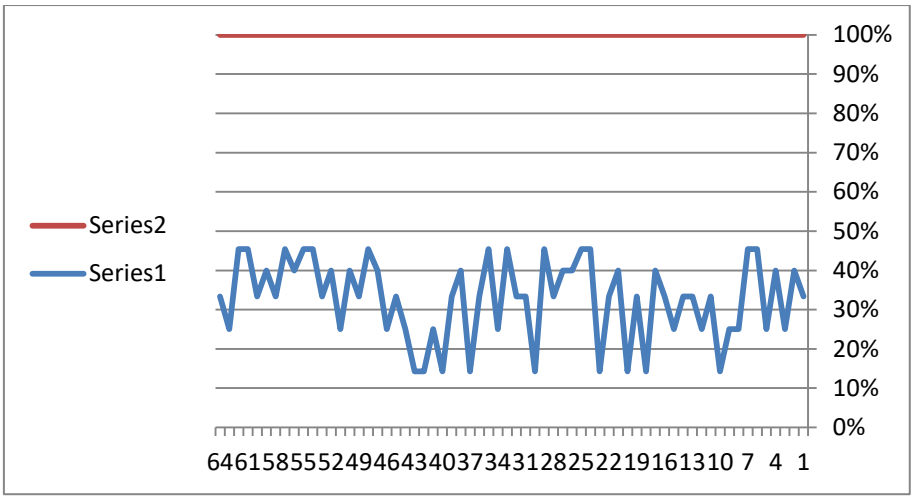

Figure 4-complexity chart for different value

Table 2- ASCII code for character and its binary representation

ASCII	char	Binary
65	A	01000001
66	B	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.

10. 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*.