International Journal of Scientific Research in Computer Science and Engineering
Vol.5, Issue.3, pp.42-46, June (2017)

Research Paper

E-ISSN: 2320-7639

Encryption and Decryption of Data by Genetic Algorithm

S. Dubey[1*], R. Jhaggar[2], R. Verma[3], D. Gaur[4]

[1*]International Institute of Professional Studies, Devi Ahilya University , Indore, India
[2]International Institute of Professional Studies, Devi Ahilya University , Indore, India
[3]International Institute of Professional Studies, Devi Ahilya University , Indore, India
[4]School of Computer Science and Information Technology, Devi Ahilya University, Indore, India

[*]*Corresponding Author: shubhamdubey1312@gmail.com, Tel.: +00-12345-54321*

Available online at: www.isroset.org

Received 12th Mar 2017, Revised 25th Mar 2017, Accepted 25th Apr 2017, Online 30th Jun 2017

***Abstract*—** This is the age of science where we deal with a huge set of data daily. Every day user shares huge amount of personal data in social sites, messaging applications, commercial sites and in other service based platforms. To accomplish transactions we need to share our credit/debit card number with passwords too, which makes the transaction very much sensitive. Randomness in the data is called Entropy. The entropy of data is directly proportional to the security of corresponding data. Security is the most favorable and mandatory feature of data transfer and storage based services. Since the quantity of data travel through the networks growing rapidly with respect to time thus enhancement in security is highly needed. According to the described variation of genetic algorithm users will have to give message as well as key also the help of these data sets, algorithm will give ciphertext and hence encryption has been achieved. At receiver's end decryption of data takes place. The key by which encryption has been done in this algorithm is combination of two matrix of equal length. It will increase the security because of dependency on both the matrix.

***Keywords*—** Cryptography, Genetic Algorithm, Encryption, Decryption, Key, Cipher text

I. INTRODUCTION

It was when 1978, Martin E. Hellman drew attention on the essentiality of Cryptography. He mentioned that cryptography is an essential ingredient to preserve the privacy. He also emphasized on the public key and digital signature concepts which are necessary in commercial systems. Hellman also underlined the major problem that tackles cryptography is the certification of these systems. What is strength of an algorithm or what is the degree of security associated with algorithm, it was a great Question introduced first. This brought revolution in the field of cryptography. It was assumed that the theory of computational complexity and other proofs may be possible in the future. This research work is intended to support information security through "variance of genetic cryptography". This area contains a large range of cipher generation techniques for secure information exchange [1]. Cryptography approaches are very was those cover some cryptic algorithms and some current techniques which are capable to protect data [2][3]. However, on increase in computing power and decrease in the cost of hardware, stronger cryptanalysis attacks become doable. In the variation of Symmetric Cryptography modern algorithms (such as AES, RSA, QMatrix etc.), key plays a crucial role in the design of the cryptosystem [4]. Increasing the key size is one of the easiest defenses [3]. Genetic Algorithm, which is intended to implement in this project is also counted in the symmetric key cryptography. GA (genetic algorithm) currently operates in the basis of mutation and crossing over of the Gene patterns. The aim of this work is to find, the better alternative approach (variation of GA) for securing information, which will more secure and robust as well as time and power efficient. The aim is to," Prepare a tool for Data Encryption & Decryption using variation of Genetic Algorithm " implemented in MATLAB which will give better performance with respect to memory and power consumption . An algorithm is called as secure as it is tough to decipher it's ciphered text. The degree of inconsistency is called entropy. So an algorithm's security feature is directly proportional to the entropy of cipher text generated by it[10]. Section II of the study is associated with the related works have been done so far. Although it is a very vast domain but we have taken very few of them those are mentioned in this section. Approach of implementation and algorithm's descriptions are mentioned in Section III titles as methodology. Section IV throws light about the results gained from section III. Last and final section V has all details about the conclusion.

II. RELATED WORK

In [4],tells that Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data Now, in order to achieve these goals various cryptographic algorithms are developed by various people. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. The aim of this work was to design and implement a new algorithm to address this issue so that we don't have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but of-course not sacrificing the security issues. A single is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm, but as public key. Cryptography is more secured then secret key cryptography our next task would be to develop and design a public key cryptographic algorithm in a simple manner as it is done in this paper.

In [5], tells that Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the send data now, in order to achieve these goals various cryptographic algorithms are developed by various people. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data. The aim of this work was to design and implement a new algorithm to address this issue so that we don't have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data. Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but of-course not sacrificing the security issues. A single is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm, but as public key.

In [6] , it throws light that Cryptography plays vital role in explosive growth of digital data storage and communication. It is used to achieve the mains of security goals like confidentiality, integrity, authentication, non-repudiation. In order to achieve these goals, various cryptographic algorithms are developed. In which some of the algorithms are succeed and others failed due to lack of security. The algorithm for encryption can be selected based on the type of data being communicated and type of channel through which data is being communicated. The main purpose of this paper is to disseminate the basic knowledge about the cryptographic algorithms and comparison of available symmetric key encryption techniques based on some parameters like vulnerability to attack, Uniqueness about the technique, etc.

In [7] this paper the application of Genetic Algorithm for stream cipher is discussed. Genetic algorithm gives optimal solution and it can be used for generation random stream of numbers for cryptography. Random number generation reflects the generation of Key done by repetition of genetic algorithm. The key with highest fitness degree is selected and compared with threshold value. This paper concludes that when key is generated with Genetic Algorithm it is atomically unique and have huge security. In this paper a model has been proposed to generate stream cipher key of the stream cipher using genetic algorithm. The main aim of this work is to produce random and unique key for encryption and efficient performance. Security is also enriched due to purely random key.

In [8], The genetic algorithm is briefly introduced and its complete programming is provided in detail by MATLAB7.0. In addition, the application in optimization of functions and solution of equation is shown through three examples and the method of avoiding local optimization by increasing the value of pm is also discussed. The given instances in this article show that the genetic algorithm can be applied to find optimal solution and to solve equations and indicate that the genetic algorithm is a powerful global searching tool. In order to avoid local optimal solution, we can increase individual rate of mutation and increase the hereditary generations of population.

In [9], it is discussed that Genetic algorithms are based on evolutionary ideas of natural selection and genetics. Genetic algorithms solve the problems step by step and produce next generation. All evolutionary algorithms including Genetic Algorithm can find near optimal solution. A set of test functions including unimodal and multimodal benchmark functions is employed for optimization.

III. METHODOLOGY

A. Terminology:

- *Plaintext*: This is the information to be protected during transmission.
- *Encryption Algorithm:* It is a mathematical course of action that gives ciphertext for known plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and encryption key as input and generates ciphertext.
- *Ciphertext:* Ciphertext is the denatured version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not watched over. It flows on network.
- *Decryption Algorithm:* This is a mathematical routine that generates plaintext for ciphertext and decryption key. It is a cryptographic algorithm that seizes ciphertext and decryption key as input, and outputs plaintext. Decryption algorithm fundamentally reverses the encryption algorithm and hence is closely related to it.
- *Encryption Key* - It is a Key that is known to the sender. The sender inserts the encryption key into the

encryption algorithm along with the plaintext in crux to compute the ciphertext.

- *Decryption Key*: It is an entity that is known to the receiver as well as sender. The decryption key is related to the key of encryption, but it is not always identical to it. The receiver gives the decryption key into the algorithm of decryption along with the ciphertext in order to compute the plaintext.

There are two types of cryptography based on the mode in which encryption-decryption is carried out in the system, Symmetric Key Cryptography and Asymmetric Key Cryptography[3][4]. The main difference between these cryptography is the correlation between the encryption and the decryption key.

B. Algorithm

The tool used for implementation was MATLAB R2008b Version. Since, this concept somewhere down the line exist as mentioned above, but we have added some new concept on it . These variations support symmetric cryptography. Result of this study is to creation a variation of genetic algorithm that is efficient and will give better performance as well.

- ***Encryption Process***

Steps of algorithm for encryption:

1. Give Keys K_1, K_2 of equal length each and convert them in ASICII value type matrix.
2. Pass message P_t and convert it in double type matrix, call it M.
3. Find N = length of M.
4. Combine K_1 and K_2 name new matrix $C_m = [K_1: K_2]$.
5. Find Q = length of C_m.
6. If (N>=Q)
   { Calculate number of repetition of R_p = N/Q;
   Find length of matrix for padding L_{Pd} = N % Q;
   Create a matrix of Zero with L_{Pd} Length, Name it P_d;
   Create Matrix of length N, i.e. Key for encryption
   K_m= [(Repeat P_t , R_p times) + (append with P_d)]
   $C_i = P_t + K_m$;
   }
   Else
   {
   Find L_{Pd} = Q % N;
   Omit C_m by L_{pd} ;
   Find K_m = Omitted C_m;
   Find $C_i = P_t + K_m$;
   }
7. Convert C_i in Character/ Unicode..
8. Send Converted Character set or Cipher text C_i.

Figure 1 shows flow chart of encryption.

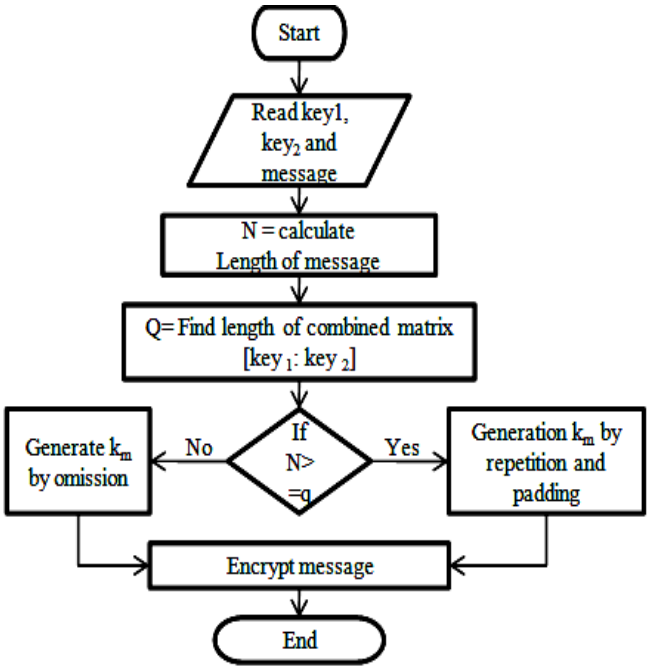

Figure 1. Encryption process flow chart.

- ***Decryption Process***

Steps of algorithm for decryption:

1. Get C_i, Convert it in the form of double. C_i= Double [C_i].
2. Find double conversion of K_1, K_2.
3. Find C_m = combined matrix of [K_1:K_2].
4. Find length of C_m , R = length of C_m.
5. Find length of C_i , M = length of C_i.
6. If (R>=M)
   {
   Find length of Padded matrix
   I.e. L_{Pd} = M%R.
   Construct matrix of last L_{pd} elements of C_i name it P_d;
   Omit P_d from C_i ;
   $P_t = C_i - C_m$;
   }
   Else
   {
   Find length of Omitted matrix
   I.e. L_{Pd} = M%R.
   Construct matrix of last L_{pd} elements of C_m name it P_d;
   $K_m = C_m - P_d$;
   $P_t = C_i - K_m$;
   }
7. Convert P_t in Character/ Unicode.
8. Plain text achieved

Flow chart of decryption process is given in figure 2.

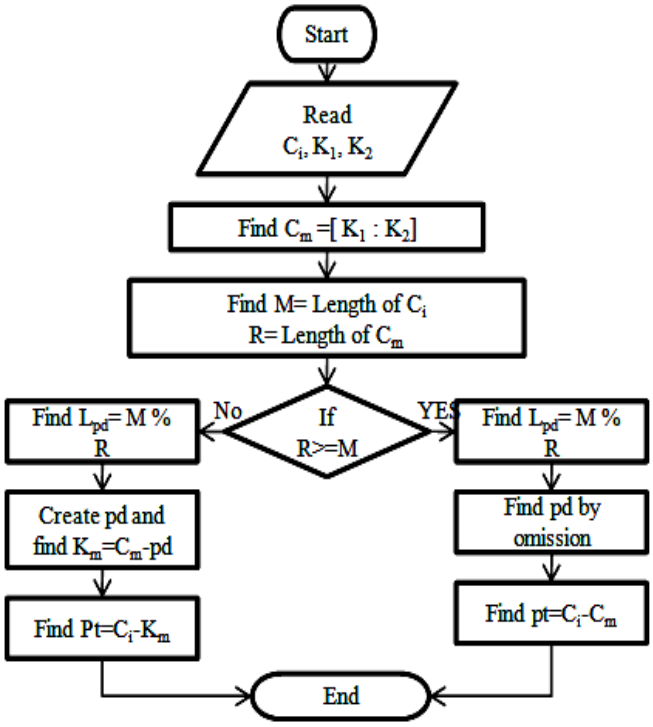

Figure 2. Flow chart of Decryption Process.

IV. .RESULTS AND DISCUSSION

A. *Length of Message is greater than the length of Key given*

- Encryption Process

After first iteration Key was made. Then converted intermediate cipher message has been shown. Level 3 gives cipher generated by adding Key matrix K_m. After that algorithm has generated corresponding Unicode. Hence we get our cipher. Table gives brief about this process of data encryption.

Table 1. Encryption process level by level, when N >= Q

Level of processing	Process
Level 1	Your encryption key is Km = w7#j4@%ee%
Level 2	ENCRYPTION BIGIN 72 101 108 108 111 32 85 115 101 114
Level 3	191 156 143 214 163 96 122 216 202 151
Level 4	YOUR ENCRYPTED MESSAGE IS ¿ • Ö£`zØÊ

Here figure 3 tells all brief about encryption.

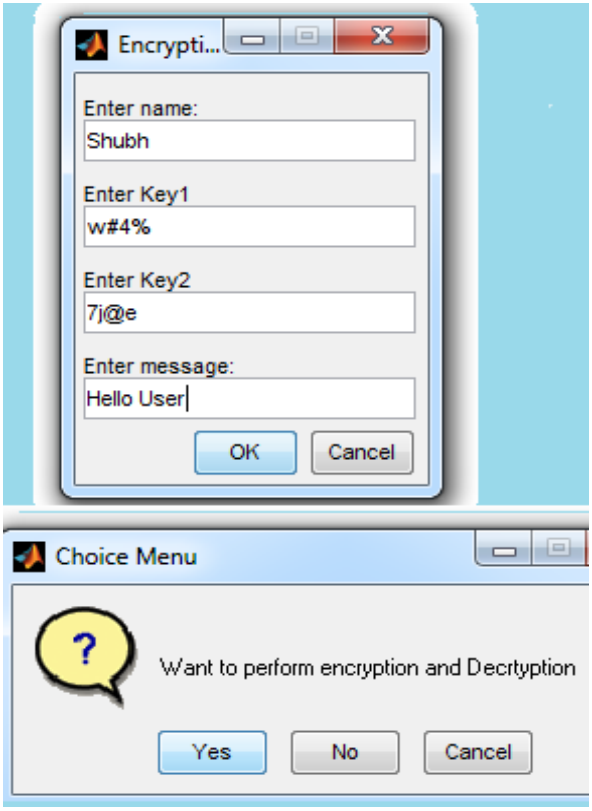

Figure 3. Input and corresponding forward processing for encryption

- Decryption Process

In first level of table 2, cipher has been shown. Level second is the double value of cipher, i.e. conversion from Unicode to Double has been done. Level 3 is the matrix of plain text with double value of it. This has been achieved by subtracting key on cipher text. Table 2 provides complete processing levels.

Table 2. Decryption process level by level, when N >= Q

Level of processing	Process
Level 1	DECRYPTION BEGIN ¿ • Ö£`zØÊ
Level 2	19 156 143 214 163 96 122 216 202 151
Level 3	72 101 108 108 111 32 85 115 101 114
Level 4	YOUR DECRYPTED MESSAGE IS Hello User

As it can be seen in figure 4, the message "Hello User" was supplied for that Cipher text "¿□ Ö£`zØÊ" has been achieved. Same testing has been performed with the message has length greater than the Key length. Figure 4 gives idea for input supplied to the algorithm. Visualization of the process can be seen in figure 4.

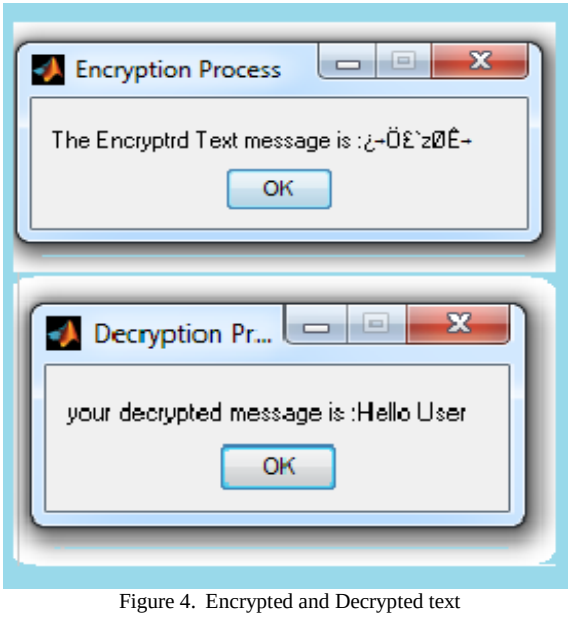

Figure 4. Encrypted and Decrypted text

B. Length of Message is less than the length of Key given

- Encryption Process

In this case Message "Hello" was supplied which has less length of plain text than length of key i.e. 5 < 8.
Processing for the data given as in figure 5 is mentioned in the table 3 and 4, for encryption and decryption respectively.

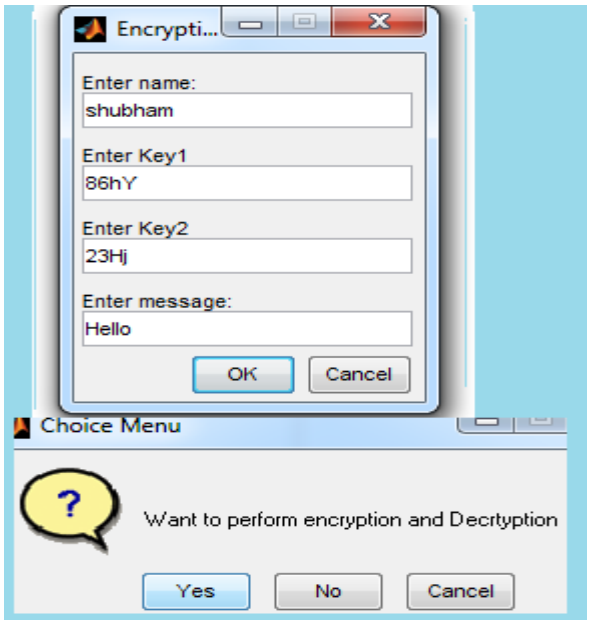

Figure 5. Input and corresponding forward processing for encryption

Table 3. Encryption process level by level, when N< Q

Level of processing	Process
Level 1	your encryption key is hgytf
Level 2	ENCRYPTION BIGIN 72 101 108 108 111
Level 3	176 204 229 224 213
Level 4	YOUR ENCRYPTED MESSAGE IS °ÌåàÕ

- Decryption

After the conversion of Unicode Key has been subtracted from Cipher to get plain text, That is shown in table 4.

Table 4. Decryption process level by level, when N < Q

Level of processing	Process
Level 1	DECRYPTION BEGIN °ÌåàÕ
Level 2	176 204 229 224 213
Level 3	72 101 108 108 111
Level 4	YOUR DECRYPTED MESSAGE IS Hello

The process of encryption and decryption totally depends upon the key matrices supplied by user i.e. K_1 and K_2. Here in the implementation the work done has been tested and well analyzed in both the cases.

V. CONCLUSION AND FUTURE SCOPE

The aim of the study was, to design a variation of genetic algorithm. Tables of result sections are signaling that the algorithm is working well, with least need of computations. In this study the variation of Genetic algorithm was targeted in such a way so that it will maintain the security of message. The outputs achieved in both the cases were up to the mark and are true without any error. In both the cases either length of plaintext is less than the length of key provided or greater, the entropy is cipher text is high. It reflects that the security aspect of system is very good. The main feature which makes system more reliable is, user is itself able to decide the Encryption Key. This increases the atomicity and confidentiality of the system. Since security is the subject to increases thus this study is providing a solid track to work towards genetic algorithm based encryption system. In this paper the research was limited up to text messages only. So in future a study for Image, Audio, and Video types of data can be done. This research fully wraps Static data and Dynamic data (Streaming data) thus other aspects of this combination can be enhanced.

REFERENCES

[1] U. Bodenhofer "*Genetic Algorithms: Theory and Applications"*, Fuzzy Logic Laboratorium Linz- Hagen berg, Austria, pp. 53-57, 2003.

[2] A. Soni, S. Agrawal, "*Using Genetic Algorithm for Symmetric key Generation in Image Encryption*", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol.1, Issue.10, pp. 137-141, 2012

[3] S. Prajapat, A. Jain, R.S.Thakur, "*A Novel Approach For Information Security with Automatic Variable Key Using Fibonacci QMatrix*", International Journal of Computer & Communication Technology (IJCCT), Vol.3, Issue.3, pp. 54-57, 2012,

[4] S. Mewada, P. Sharma, S.S. Gautam, "Exploration of efficient symmetric algorithms", *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, India, pp. 663-666, 2016.

[5] A. Sharma, RS Thakur, S. Jaloree, "*Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.5, pp.5-11, 2016.

[6] W. Stalling, "*Cryptography and Network Security*", Pearson Education, USA, pp.327-365, 2008.

[7] A. Kumar , K. Chatarjee, "*An Efficient Stream Cipher using Genetic Algorithm*", Proceedings IEEE-WISPNET, India, Page-2322-2326, 2016

[8] C. Guo, X. Yang, "*A Programming of Genetic Algorithm in Matlab7.0*", Modern Applied Science, Vol.5, Issue.1, pp. 230-236, 2015.

[9] C.R. Gaidhani, V.M. Deshpande, V.N. Bora, "*Image Steganography for Message Hiding Using Genetic Algorithm*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.67-70, 2014.

[10] S. Prajapat, R. S. Thakur, "*Various Approaches towards Cryptanalysis*", International Journal of Computer Applications, Vol.127, Issue.14, pp.15-24, 2015.

