International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# A New Approach to DNA Cryptography Using 8x8 Playfair Cipher and Ramanujam Square Matrix

**Dr. K. Meena[1], Dr. K. Menaka[2]**

[1]Former Vice-Chancellor, Bharathidasan University, Tiruchirappalli-620024, India

[2]Assistant Professor, Department of Computer Science, Shrimati Indira Gandhi College, Tiruchirappalli-620002, India

**Abstract:** ***Cryptography can be characterized as a process of renovating the sender's message to a furtive format that can only be understood by the intended receiver. The DNA cryptography is a novel area to achieve advanced stage of information which has enthralled massive implication in the field of information security. With the strange availability of information in DNA sequences, it is possible to efficiently make a secure system. Though many algorithms have been developed for hiding the data, DNA sequences based data encryption seems to be a promising approach for satisfying the current information security needs. In this paper, a new approach to DNA Cryptography has been developed using 8x8 Playfair Cipher and Ramanujam Square Matrix in which some blending steps are added to scramble the message thereby providing more randomness. The proposed algorithm offers very low correlation between the original and encrypted messages and confirms a strapping robustness against intruder attacks.***

**Keywords:** DNA cryptography, Playfair Cipher, Ramanujam Square Matrix, Data Hiding, Secure Transmission and Reception

## 1. Introduction

At the time of transmitting a message, the main focus is on the security of the information. Because of this reason, the cryptography concepts were introduced in which a known text is converted to some other form, which only the sender and the receiver know and could not be revealed by any intruders. Over the years, several cryptography approaches have been proposed by a lot of researchers. In their approaches they carried out varieties of difficult mathematical computations to enhance the security of the information. In order to improve data security and to make the data more confidential, effective encryption algorithms are required. DNA based encryption method is one of the recent techniques in cryptographic field. In this paper a DNA based cryptographic approach is proposed where the message integrity is also preserved. A key (key1) is shared among the sender and the receiver that will be used in the encryption phase. Using this secret key, the original message is converted to cipher text (partial) by applying the 8x8 playfair cipher[1] concept. Later on, it will also be transformed to a DNA sequence to make it more secure and not understandable.

The Playfair cipher is a symmetric substitution cipher which encrypts pairs of letters (digraphs). This method uses a 5 x 5 table that is originally built using a key word and the ciphering process is done according to few simple rules. In addition, the plain-text needs to be systematically preprocessed to eliminate spaces and handle any double-letter digraphs. Recent research in cryptography provided some new ways to improve the security of the playfair cipher. An extended 8x8 playfair cipher was proposed in [2]. The proposed system was able to encrypt alphabets, numbers, and some special characters. Spaces and duplicate characters are handled using the symbols | and ^ respectively. Another alteration emerged in [3] with a sturdy new cipher based on the ASCII codes of characters. Another comprehensive 8x16 Playfair cipher was introduced in [4], which considered the 128 ASCII characters instead of the 26 characters of the English language. Thus, the main realization of this work is to identify the DNA cryptosystem, which is a novel science in information security. A new DNA cryptography algorithm has been designed and implemented in this work using 8x8 Playfair Cipher and Ramanujam Square Matrix.

## 2. Literature Review

The following are some of the prospective DNA based data hiding schemes reported recently. Mohammad Reza Abbasy, et al. [5] proposed a data hiding method where data were efficiently encoded and decoded by using the properties of DNA sequence. Complementary pair rules of DNA were used in their method.

DNA cryptography is based on DNA computing where message is encrypted in the form of DNA sequence. DNA computing can be used as subtle scheme for data encryption and decryption by using symmetric or asymmetric key. It can provide a hybrid security by combining traditional cryptography with it [6]. In recent years, many new Cryptographic techniques are proposed by the researchers. Bibhash Roy et al [7] [8] [9] proposed numerous schemes on DNA sequencing based encryption and decryption process.

## 3. Biological Aspects of DNA

The DNA actually stands for Deoxyribonucleic acid. In human body each cell contains a nucleus which characterizes all the physical and behavioral features of human body. They are packed into chromosomes. A DNA is nothing but a double helix made up of two strands where each strand can have either a purine or a pyramidine base. The purine bases are adenine (A) and guanine (G), while the pyrimidines bases are thymine (T) and cytosine (C). In a double helix DNA the two strands are coupled together where bases are bonded each other by hydrogen bonds: A with T and C with G, which is called the complementary pairs of DNA strands. Hence, a

sequence of DNA base pairs can be represented as a string made of these four characters i.e. <AAGTCGATCGATCATCGA>.

DNA cryptography is a division of biological science, which has large data storage capacity. It stores information of living organisms. Living organisms have unique DNA information. Cryptography when combined with molecular biology, gives more secure data transmission and data hiding. DNA cryptography skill is needed in information security to guard and hide data. In conventional cryptography methods, encrypted messages are detectable by attacker. DNA has ability to store enormous information rather than existing algorithm.

## 4. Proposed Method

The Encryption scheme used in the proposed methodology differs from other encryption algorithms significantly. This scheme provides a novel perspective on DNA Cryptography using 8x8 Playfair cipher and Ramanujam Square Matrix (RSM).The proposed method starts with a DNA-encoding step followed by the construction of the substitution matrix that will be used later to apply the 8x8 Playfair cipher. Thus, a Partially Encrypted Message (PEM) is obtained. The PEM is then represented as a 4x4 square matrix. The representation procedure is as follows: Each and every cell in this 4x4 representation is subtracted from each and every cell of the Ramanujam Square Matrix (RSM). This is taken as Key2 for the algorithm.

The Key2 thus formed is represented in binary form of 128 bits and every two bits of it is taken and represented into corresponding DNA codes as per Table – I.

**Table 1:** DNA Codes

| | |
|---|---|
| A | 00 |
| C | 01 |
| G | 10 |
| T | 11 |

The message to be sent is first converted into its binary equivalent. The concept of Table – I above is as follows: if we have „00" in the binary string it is converted to „A", or if we have „01" it is converted to „C". This process continues to convert all the binary information into a DNA sequence. Obviously, the decryption process carries out the inverse of the steps in the encryption process. That is, the DNA code is converted into binary form. Afterwards, the inverse process is carried out to reveal the contents of the encrypted sequence. The eventual goal of the proposed scheme is to scramble data in the way that the person, who doesn't know the key, can't read or change the data.

Consider the following example,
**Key1: Goodday**
**Message: Welcome Everyone**

WE LC OM Ex EV ER YO NE
**G O O D D A Y**
**B C E F H I J**
**K L M N P Q R**
**S T U V W X Z**

As per the algorithm,
Replace WE with UH; Replace LC with OT; Replace OM with OL; Replace Ex with xI
Replace EV with FU; Replace ER with JM; Replace YO with OA; Replace NE with MF
Thus, The message becomes: UHOTOLXIFUJMOAMF. Now, represent this Partially Encoded Message (PEM) in a 4x4 square matrix as below:

| | | | |
|---|---|---|---|
| **U** | **H** | **O** | **T** |
| **O** | **L** | **X** | **I** |
| **F** | **U** | **J** | **M** |
| **O** | **A** | **M** | **F** |

**Figure 1:** Representation of the PEM in 4x4 Square Matrix

Now, take the Ramanujam Square Matrix (RSM):

| | | | |
|---|---|---|---|
| 22 | 12 | 18 | 87 |
| 88 | 17 | 9 | 25 |
| 10 | 24 | 89 | 16 |
| 19 | 86 | 23 | 11 |

**Figure 2:** Ramanujam Square Matrix(RSM)

Every element in the 4x4 square matrix of PEM is an alphabet. The alphabets are represented as numbers like A as 1, B as 2 and so on Z as 26. After representing the numbers to the elements of PEM, each and every element in the PEM is subtracted from the RSM, thus forming the following 4x4 matrix which is taken as Key2 for the proposed algorithm.

| | | | |
|---|---|---|---|
| 1 | 4 | 3 | 67 |
| 73 | 5 | -15 | 16 |
| 4 | 3 | 79 | 3 |
| 4 | 85 | 10 | 5 |

**Figure 3:** Key2 for the proposed algorithm

The next step is to convert all the elements of Key2 into their corresponding 8-bit binary representation as below:

**00000001 00000100 00000011 01000011**
**01001001 00000101 -00001111 00010000**
**00000100 00000011 01001111 00000011**
**00000100 01010101 00001010 00000101**

Each and every 2 bits of the above representation is taken and converted as per Table – I. Thus, the following sequence is obtained:

**AAAC AACA AAAT CAAT**
**CAGC AACC -AATT ACAA**
**AACA AAAT CATT AAAT**
**AACA CCCC AAGG AACC**

The „-" sign in the formed sequence implies that the particular element is represented as negative number. This is the cipher text which is sent to the receiver.

## 5. Conclusion

The proposed algorithm has abundant steps to break and to get the original message. Any intruder who receives the intermediate message will never be able to retrieve the original message as intended by the sender. Here, it is possible to convert binary data into a DNA strand (DNA coding technology). This field requires a lot of research work to have a place in which it can be implemented and used for practical purposes. There is a need that people from conventional cryptography and DNA technology should exchange facts among each other and cryptosystems should be developed in such a way that benefits arise for the society from both the fields.

## References

[1] S. Hamad, "A Novel Implementation of an Extended 8x8 Playfair Cipher Using Interweaving on DNA-encoded Data", International Journal of Electrical and Computer Engineering IJECE), Vol. 4, No. 1, Feburary 2014, pp. 93~100, ISSN: 2088-8708.
[2] S S Srivastava, N Gupta and R Jaiswal, " Modified Version of Playfair Cipher by using 8x8 Matrix and Random Number Generation", IEEE 3rd International Conference on Computer Modeling and Simulation. 2011, Mumbai.
[3] S S Srivastava and N Gupta, "A Novel Approach to Security using Extended Playfair Cipher", International Journal of Computer Applications. 2011; 20(6): 0975 – 8887.
[4] V.U.K.Sastry, N.R Shankar and S.B Durga, "A Generalized Playfair Cipher involvingIntertwining, Interweaving and Iteration", International Journal of Network and Mobile Technologies. 2010; 1(2): 45-53.
[5] Mohammad Reza Abbasy, Azizah Abdul Manaf, and M.A. Shahidan, "Data Hiding Method Based on DNA Basic Characteristics", International Conference on Digital Enterprise and Information Systems, July 20-22, (2011), London, UK, pp. 53–62.
[6] Tushar Mandge Vijay Choudhary, "A DNA Encryption Technique Based on Matrix
[7] Manipulation and Secure key Generation Scheme" , ICICES Journal 2013.
[8] Bibhash Roy, Gautam Rakshit, Pratim Singha, Atanu Majumder, Debabrata Datta, "An improved Symmetric key cryptography with DNA Based strong Cipher", ICDeCom 2011, Feb‟ 24 25‟2011, pp.1 5.
[9] Bibhash Roy et al, "A DNA based Symmetric key Cryptography", ICSSA 2011, 24 - 25 Jan‟11.
[10] Bibhash Roy, Gautam Rakshit, Pratim Singha, Atanu Majumder, Debabrata Datta,
**[11]** "An Enhanced key Generation Scheme based cryptography with DNA Logic", IJICT 2010.