An improved DNA cryptosystem based graph labeling techniques

Cite as: AIP Conference Proceedings **2516**, 120001 (2022); https://doi.org/10.1063/5.0108504
Published Online: 30 November 2022

B. Deepa and V. Maheswari

An Improved DNA Cryptosystem Based Graph Labeling Techniques

B. Deepa[1b)] and V. Maheswari[1a)]

Department of Mathematics, Vels Institute of Science, Technology and Advanced Studies
Chennai -600117, India.
[a)] Corresponding author: maheswari.sbs@velsuniv.ac.in
[b)] balaraman.deepa@gmail.com

Abstract. Cryptography involves in confidentiality, authentication and data security which is an Art of converting readable text or image into an unreadable format, which is easily unbreakable. In recent times, cryptography adopting a many new techniques to protect or hide our communication from any malicious party. In this paper, we proposed a method of encrypting a message using DNA Cryptosystem together with Graph labeling techniques. Thus, our message is converted in the form of human deoxyribonucleic acid by the use of ASCII and Binary value. Finally which is presented as a cipher graph using product edge labeling techniques which is sent to the receiver along with some kind of clues. The receiver has to use the clue to trace our message which is shared by the sender. Here we used complete graph K_5 to pass our secret message. In this method a common key is shared between sender and receiver. The advantage of symmetric cryptosystem is faster and secure.

Key words: ASCII value, DNA Cryptography, Product edge labeling, complete Graph, Non-Planar Graph.

AMS Subject classification MSC (2010) No: 05C78

INTRODUCTION

DNA has a countless cryptographic strength. Here we carry out DNA cryptography together with the Graph labeling technique to make sure data security for our communication. The proposed algorithm has five stages of encryption and decryption process. Which constructs the encryption process more strong compared with other encryption techniques. DNA (De-oxyribo Nucleic Acid) consists of four nitrogen bases namely adenine (A) and thymine (T) or cytosine (C) and guanine (G). By making use of the above concept with ASCII value in the encryption process, our message converts in the form of Amino acid. Further great use of product edge labeling, our secret message presented as a cipher graph which is sent to the receiver along with clues. The receiver has to decrypt the message by using symmetric key techniques.

LITERATURE SURVEY

Prasanna Balaji Narasingapuram, M. Ponnavaikko [1] explained DNA cryptography based user level security for cloud computing. Anurag Roy, Asoke Nath [2] showcases DNA based encryption, scope of symmetric key cryptography. Also [3, 4 and 5] elaborates the concept of DNA based encryption techniques. Udepal Singh, Upasna Garg [6] described the concept of ASCII based encryption techniques. For various graph labeling techniques, basic definitions of graph structures we refer J.A. Gallian [7] and F. Harary [8]. [9, 10 & 11] showcased product edge labeling techniques through graph.

2nd International Conference on Mathematical Techniques and Applications
AIP Conf. Proc. 2516, 120001-1–120001-9; https://doi.org/10.1063/5.0108504
Published by AIP Publishing. 978-0-7354-4234-4/$30.00

PRELIMINARIES

Definitions

DNA Cryptography

DNA Cryptography is the process of transforming readable text in the form of DNA structure.

ASCII

ASCII it's a shortening of American Standard Code for Information Interchange, developed by the American National Standards Institute (ANSI) and published in the year of 1963. Which is used to represent 128 English alphabets as numerical value (a range of 0-127).

Complete Graph

Complete graph is a graph in which every pair vertex contains at least one edge.

Planar Graph

A Planar Graph is a graph in which no two edges crossing each other. It can draw in a Plane is known as Planar Graph.

Non – Planar Graph

A graph that is not a Planar is known as Non Planar Graph.

Symmetric Key

In cryptography, Symmetric key is the same key used for both encryption and decryption process.

THEOREM

Any Complete Graph is a product labelled Graph.

Proof:

Let K_n be the Complete Graph with different vertices $v_1, v_2, v_3, \ldots v_n$.

Consider $f: V(K_n) \rightarrow 3N$ by $f(u_i) = 3i$ for all $i = 1,2, \ldots . n$.

Define the labeling $f(uv) = (f(u) \times f(v)) \bmod 26$ then the distinct edge labels are 1, 2, 4, 5, 10,…. Etc.

ALGORITHM FOR ENCRYPTION AND DECRYPTION PROCESS

For Encryption Process

Step: 1

Consider a Plaintext P

Step: 2

Find Binary string using the ASCII code for all characters of Plaintext.

Step: 3

Find the DNA code for each value of Binary string.

Step: 4

Represent the DNA sequence as an Amino acid form.

Step: 5

Represent the index value of Amino acid in the Cipher graph using Product edge labeling,

I.e. $\big(f(u) \times f(v)\big) \bmod 26$.

For Decryption Process

Decryption is the just inverse process of Encryption process.

ILLUSTRATION

For Encryption Process

Consider a plaintext be “At 4’o clock”

Step: 1

Find Binary string using ASCII value of each character of plain text.

Which is shown in the table 1 below.

TABLE 1. ASCII & Its Binary Value

Plaintext Characters	ASCII Value	Binary value
A	65	1000001
t	116	1110100
4	52	110100
‘	39	100111
o	111	1101111
c	99	1100011
l	108	1101100
o	111	1101111
c	99	1100011
k	107	1101011

Step: 2

The Binary value broken as 4 blocks of 2 letters or 1 letter from left to right, the Blocks of Binary values is then adopted the nucleotides such as A =00, A=0, C=01,G=10,T=11,T=1.

DNA codes for the Binary value is stated in the table 2.

TABLE 2. DNA Code for Binary value

Binary Value	DNA Code
10|00|00|1	GAAT
11|10|10|0	TGGA
11|01|0|0	TCAA
10|01|1|1	GCTT
11|01|11|1	TCTT
11|00|01|1	TACT
11|01|10|0	TCGA
11|01|11|1	TCTT
11|00|01|1	TACT
11|01|01|1	TCCT

Step: 3

Convert the codons in the DNA sequences into its corresponding amino acids by splitting it as a 3 letter sequence, the last block is padded with dummy characters to make it in a form of amino acid as shown in the table 3.

TABLE 3. DNA sequence in 3 letter block

GAA	TTG	GAT	CAA	GCT	TTC	TTT	ACT	TCG	ATC	TTT	ACT	TCC	TGT

Step: 4

Next stage process of amino acid cryptography is a random key generation from 1 to 25. Assign the index value for each block of amino acid. The notion of one DNA have multiple characters is itself make our concept enhances the algorithm more strength. The process is illustrated in below figure.

Assign the index value for each block of amino acid from 1 to 25. Which is shown in the figure.

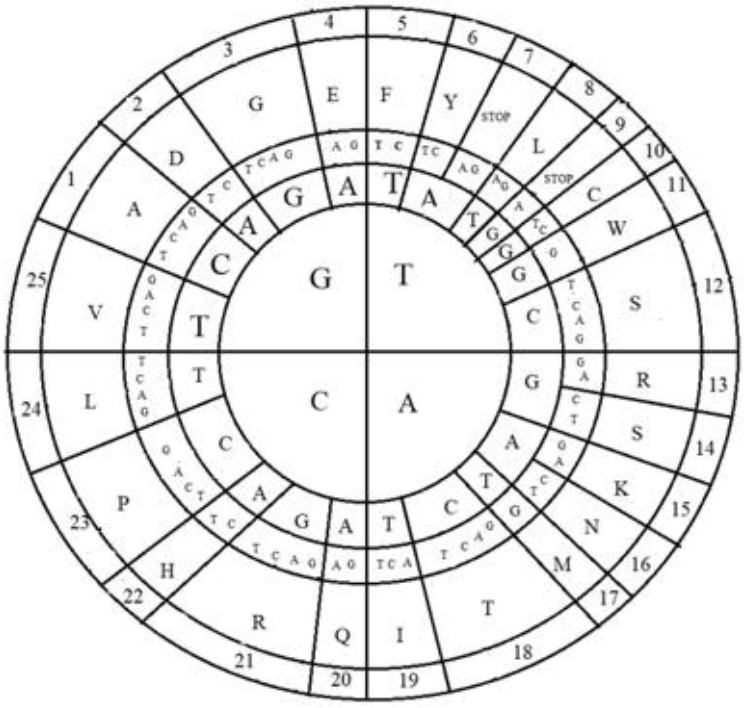

FIGURE 1. Amino acid index value

Step: 5

Convert the codons in the DNA sequences into its corresponding amino acids.

TABLE 4. Amino Acid sequence represents as English alphabets

GAA	TTG	GAT	CAA	GCT	TTC	TTT	ACT	TCG	ATC	TTT	ACT	TCC	TGT
E	L	D	Q	A	F	F	T	S	I	F	T	S	C

The index value of amino acid is then presented in the K_5 Complete Graph using product edge labeling techniques. Finally, use the Cipher Graph to pass the message to the receiver.

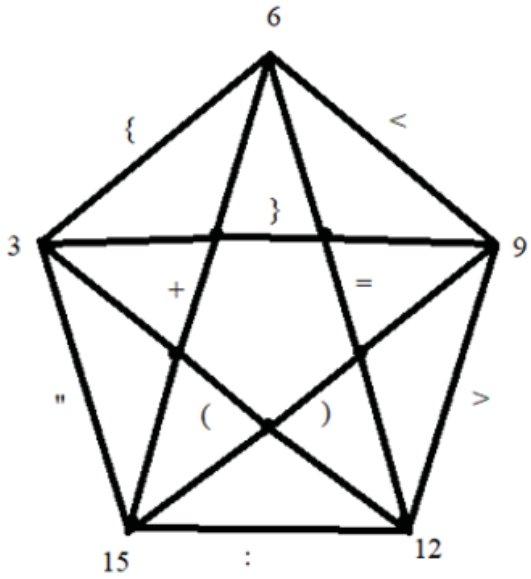

FIGURE 2. Cipher Graph

The Cipher Graph is sent to the receiver along with clues.

Clue: 1

Find the edges using the key formula of Product edge labeling, I.e. $\big(f(u) \times f(v)\big) \bmod 26$.

Clue: 2

Arrange the edges in the order of below given table.

>	:	<	=	}	)	)	{	+	“	)	{	+	(

Clue: 3

Use Amino acid figure 1 to trace the value of DNA sequence.

Clue: 4

Use Binary and ASCII value to finally yield our Plain text.

For Decryption Process

Step: 1

The Receiver has to use the key formula of $\big(f(u) \times f(v)\big) \bmod 26$ to initially trace our edges of the cipher Graph.

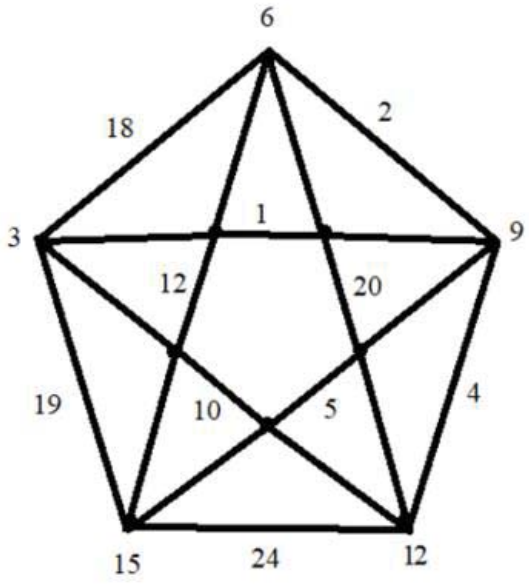

FIGURE 3. Complete Graph K_5

Further great arrangement of edges in the order as stated in clue 1 as presented in below table.

TABLE 5. Index value of edges

4	**24**	**2**	**20**	**1**	**5**	**5**	**18**	**12**	**19**	**5**	**18**	**12**	**10**

Step: 2

Obtain the Amino acid value corresponding to the index value of edges from Fig 1.

We get,

TABLE 6. Amino Acid represented as English Alphabets

E	**L**	**D**	**Q**	**A**	**F**	**F**	**T**	**S**	**I**	**F**	**T**	**S**	**C**

Step: 3

Rewrite the alphabets as an amino acid form.

TABLE 7. Amino Acid in 3 letter Block

GAA	**TTG**	**GAT**	**CAA**	**GCT**	**TTC**	**TTT**	**ACT**	**TCG**	**ATC**	**TTT**	**ACT**	**TCC**	**TGT**

Step: 4

Convert the codons of amino acid into a sequence of DNA by making each blocks as 4 letters block. The dummy value is omitted in the last block and find the Binary value for each blocks of DNA sequence. Which is shown in the table 8.

TABLE 8. Binary value for DNA code

DNA Code	Binary Value
GAAT	10|00|00|1
TGGA	11|10|10|0
TCAA	11|01|0|0
GCTT	10|01|1|1
TCTT	11|01|11|1
TACT	11|00|01|1
TCGA	11|01|10|0
TCTT	11|01|11|1
TACT	11|00|01|1
TCCT	11|01|01|1

Step: 5

Further great use of ASCII technique, we obtain ASCII value corresponding to its Binary value.

TABLE 9. ASCII value

ASCII Value	65	116	52	39	111	99	108	111	99	107
English alphabets	A	t	4	,	o	c	l	o	c	k

Finally, we trace our Plaintext is “At 4’o clock”.

CONCLUSION

The proposed method of DNA Cryptosystem based Graph Labeling Techniques has numerous processes. Which make the techniques robust that are executed to hide the information. DNA is the unique biological reference of Humans that cannot be altered or replaced by anyone but also it is difficult for a hacker to de-crypt or brake the information. In future we can try for DNA Cryptography with Different types of graphs to make tougher to hack.

REFERENCES

1. N.P. Balaji and M. Ponnavaikko, *IJRTE,* 3738-3745 (2020).
2. A. Roy and A. Nath, *IJIRAE,* 48-53 (2016).
3. B R Pushpa, *I2C2,* (2017).
4. A. Y. Yousuf and H. H. Abbas, *IJAST*, 104-108 (2020).
5. K. Halvorsen and WP. Wong, *PLOS ONE* 7(9) (2012).
6. Udepal Singh and Upasna Garg, *IJSRP,* 1-5, (2013)
7. B.Deepa, V.Maheswari and V. Balaji, *IJEAT*, 206-212 (2019).
8. J.A. Gallian, A Dynamic Survey of Graph Labeling, *Electronic Journal of Combinatorics* (2018).
9. F. Harary, Graph Theory, *Addison – Wesley*, (1969).
10. B.Deepa and V.Maheswari, *IJAEMA*, 8-15 (2019).
11. B.Deepa and V.Maheswari, *IJRTE*, 33-36 (2019).