International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT2063210

Advanced Symmetric Key Cryptography Algorithm: Application of Pseudo Biotic DNA Method(ASKCA VER-1.0)

Asoke Nath*, Ankita Kedia, Sunanda Pal, Moumita Sen

Department of Computer Science, St. Xavier's College(Autonomous), Kolkata, west Bengal, India

ABSTRACT

In today's world with advancement in technologies as networking is growing at a fast pace providing security to data becomes the biggest concern. Hence, cryptography is the major area of concern when it comes to data security. DNA cryptography is a promising approach in encrypting, storing and transmitting data over a network. In our work we will be trying to design an encryption and corresponding decryption algorithm based on pseudo biotic DNA cryptography method. The algorithm will make use of basic concepts of DNA cryptography, crossover, mutation, transcription, splicing system for get spliced key, DNA Vigenere table and also a lot of steps to perform randomization of the plain texts in order to produce cipher texts which cannot be easily breakable. The encryption algorithm can be used in cellular and electronic communication.This document provides some minimal guidelines (and requirements) for writing a research paper. Issues related to the contents, originality, contributions, organization, bibliographic information, and writing style are briefly covered. Evaluation criteria and due dates for the research paper are also provided.

Keywords : Data security, DNA cryptography, crossover, mutation, transcription, splicing system, DNA Vigenere table, randomization

I. INTRODUCTION

Securing the Internet presents great challenges and research opportunities. There are many sectors such as Banking, E-business, E-commerce, Railway or Air Reservation system where the data should not be tampered or intercepted by an unauthorized person The epidemic of hacker attacks on personal computers and web sites only highlights the inherent vulnerability of the current computer and network infrastructure.

Cryptography is the technology which is incredible for protecting information or data which needs to be transferred via some secure channel. Modern cryptography provides a robust set of techniques to ensure that the malevolent intentions of the adversary are thwarted while ensuring the legitimate users get access to information.

But one can use an unbreakable cryptography algorithm which maybe theoretically possible, but if other errors occurs while systems designing or data handling part then confidential information may still be revealed. Multiple cryptographic techniques are used for securing the data over the network. Cryptography is the art of converting the original message into human unreadable code, which cannot be reversed to the original message. Cryptography plays a very important role in data integrity in the three components of the CIA triad (Confidentiality, Integrity, and Availability). CIA is the fundamental concept in security.

DNA cryptography is one of the rapid emerging technology which works on concepts of DNA computing. A new technique for securing data was introduced by Adleman's research[1] using the biological structure of DNA called DNA Computing (aka molecular computing or biological computing). DNA can be used to store and transmit data. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology that may bring forward a new hope for unbreakable algorithms. The main objective of our work is to provide a highly secured cryptographic algorithm which is practically impossible to break by any intruder even if he is able to intercept it. Here the main key also known as spliced key is generated from the pre cipher text itself. There is no need to share it as previously. DNA based bimolecular cryptography design is a technique that uses the huge parallel processing capabilities of bio molecular computation which converts short messages from hexadecimal and ASCII forms and then back to encrypt and decrypt the information[2]. DNA is considered as a medium for ultra-compact information storage, exceeding capability of conventional electronic media[2]. A few grams of DNA may hold all data stored in the digital mediums in the world [3].

II. BIOMOLECULAR TECHNOLOGY BACKGROUND

The DNA, stands for Deoxyribose Nucleic Acid, is a sequence of nucleotides. The exact sequences of the nucleotides determine the code of each gene. DNA sequences represent biological information such as skin colour, weight, nose shape, eye, and hair as well as other features[2]. A DNA sequence is of a long molecule with four bases called nucleotides Adenine (A), Guanine (G), and Cytosine (C) and Thymine (T). DNA Sequences is succession of those letters that indicate order of nucleotides.

Ribonucleic acid (RNA) is a single strand of ribonucleotides, in which thymine (T) which is replaced with uracil (U).

The genetic information flows from DNA into RNA by process known as transcription and then RNA into mRNA (messenger RNA) process known as transcription and from mRNA to protein, known as translation, defining what is known as the central dogma of molecular biology.

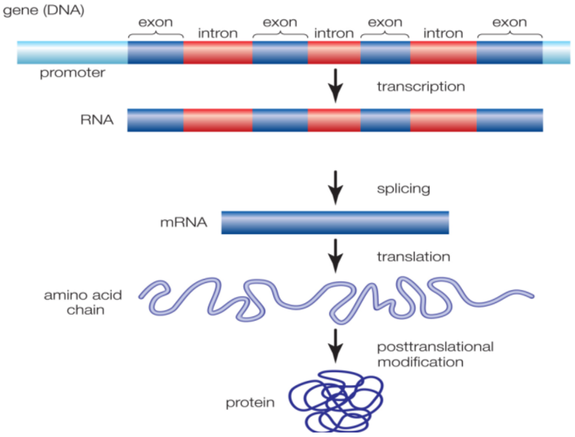


Figure 1. Central Dogma of DNA

The goal of this algorithm is to find mRNA from the DNA sequence and later turning that mRNA into the cipher text and vice versa. The DNA sequence is made of two parts. One is called exon and another part is called intron. To be able to get mRNA from the DNA sequence two process is being done. First we will apply transcription to get RNA then we apply splicing system to avoid the introns and extract the mRNA from it.

.

III. LITERATURE SURVEY

DNA based cryptography is a relatively new paradigm that has attracted great interests in the field of security. Since scientists have found out that binary computers have physical limitations, especially in data storage and computation, they have concentrated on DNA computers and tried to implement this new science in the field of IT. DNA cryptography is a new concept that needs many improvements.

In 3-Dimensional Bit Level Encryption Algorithm (3DBLEA) authors made use of DNA encryption and several 3-D matrix operations in order to encrypt plain text[4].

In 3-Dimensional Bit Level Encryption Algorithm (3DBLEA-2) authors have used DNA encryption and genetic algorithm along with 3-D matrix operations to encrypt a plain text[5]. In that mentioned paper only one key is used. Use of genetic algorithm made the algorithm more complex so that it cannot be easily cracked.

In 3-Dimensional Bit Level Encryption Algorithm Version-3 (3DBLEA-3)[7], along with the previous methods authors incorporated the idea of message digest there to make it more secure.

In our novel approach along with DNA operations like transcription, translation, splicing, crossover and mutation, DNA Vigenere table is used and also instead of 3-D matrix only 2-D matrix operations are used. Also most importantly along with the symmetric key a spliced key is used which is derived from symmetric key and this spliced key acts as a private key and upon this the encryption procedure matters a lot. In our approach to develop a new DNA based cryptography algorithm. We first applied randomization technique on bits of plain text, i.e., matrix shuffling, XOR operations and prime position complementing. Then, we followed the procedure of pseudo biotic DNA where mRNA is produced from DNA. Hence this approach is more secure and the encrypted text cannot be easily hacked.

IV. DEFINITIONS OF METHODS

There are several methods that are used in encryption algorithm and followings are their explanations.

A. DNA encryption

Binary data can be encoded in DNA bases, Adenine (A), Cytosine (C), Guanine (G) and Thymine (T), by using sequence of alphabet. It is known as DNA encryption.

00 converts to A.   01 converts to C.

10 converts to G.   11 converts to T.

For example, a binary string like ‘00011011’ is converted to ‘ACGT’. Here the authors have first implemented few bit level encryption techniques and then they converted the bits to DNA sequences to apply genetic operations like mutation.

B. Mutation

After crossover process, mutation process is applied on the chromosome population. Mutation is the alteration of string elements. Two types of mutation are used. In the first one, two mutation points are selected between the entire lengths of the bit string. Then the bits in between these two points are complemented that is, single point mutation changes a 1 to a 0, and vice versa.

Example: Before mutation:11 0110 0100 1001 0010 11
After mutation: 11 0101 1011 0110 1010 11

In the second mutation type that is DNA mutation, four bits are converted to two bases of DNA. Here each DNA base is treated as two bits and the second bit is complemented for mutation. Thus G=’10’ is mutated to ‘11’=T and vice versa

Example: Before mutation: … G G A C T G C G A T
After mutation: …... T T C A G T A T C G

C. Crossover

The crossover operator is analogous to reproduction and biological crossover. In this more than one parent is selected and one or more off-springs are produced using the genetic material of the parents.

Crossover is usually applied in a GA with a high probability.

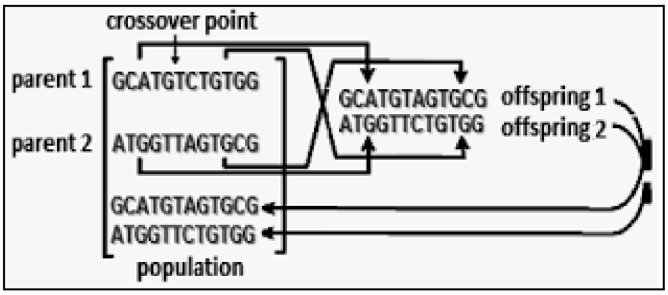


Figure 2. Crossover

D. Translation

Translation is the process of translating the sequence of a messenger RNA (mRNA) molecule to a sequence of amino acids during protein synthesis. The genetic code describes the relationship between the sequence of base pairs in a gene and the corresponding amino acid sequence that it encodes. In the cell cytoplasm, the ribosome reads the sequence of the mRNA in groups of three bases to assemble the protein. Here we replace 4 DNA sequence to binary code and then to ASCII character.

E. Spliced Key

Spliced key is the key which is being taken from the pre cipher text itself. The pattern of the key is being searched in the pre cipher text and later it is being spliced.

If DNA sequence is GAUC CG
Pre RNA- GACG
Spliced Key-UC

F. DNA Vigenere table

DNA Vigenere Table [9] is based on the properties of the Vigenere Cipher shown in the table-1.The character of the plain text of the DNA sequence show the row number of the DNA Vigenere table and the character of the random key show the column number of the table.

TABLE 1
DNA Vigenere Table

	A	T/U	C	G
A	A	T	C	G
T/U	T	C	G	A
C	C	G	A	T
G	G	A	T	C

For example, if the first character of the DNA sequence is 'A' and the first character of the random key sequence is 'G' then that means row 1, column 4 is chosen. So, we replace the first character of DNA sequence 'A' with 'G'.

G. Full DNA Vigenere encryption and decryption

Full Vigenere encryption was included to make the cipher text fully dependent on key especially in the case when the length of key is greater than the plain text.

For this the input key is converted to DNA sequence and each DNA character of final cipher text is encrypted with the DNA sequence of key until all the characters of plain text are exhausted. If some characters in the DNA sequence of key is remaining, then the characters of new cipher text from starting is encrypted using DNA Vigenere encryption with the help of remaining cipher text. This process is continued until all the DNA characters in DNA sequence of key are used.

Now if the length of final cipher text is greater than the length of key, then in similar manner encryption is done by encrypting each DNA character of cipher text by using the DNA sequence of key again and again from starting position.

For example, if plain text is 'ACUCG' and DNA sequence of key is 'GGUCAAU', then encryption takes place as

Step-a- CT-> A C U C G
Key-> G G U C A A A U
New CT-> X1X2X3X4X5
Step-b- CT-> X1X2X3X4X5

Key-> A A U

New CT-> Y1Y2Y3X4X5

For example, if plain text is ‘ACUCGUU’ and DNA sequence of key is ‘GGUC’, then encryption takes place as

Step-a- CT-> A C U C G U U

Key-> G G U C G G U

New CT-> X1X2 X3 X4 X5 X6 X7

For, full Vigenere decryption last position of cipher text is found if length of key is greater than the cipher text and then Vigenere decryption is done in reverse direction until all the DNA characters of key is fully exhausted. Similarly length of cipher text is greater than the length of key, last position of DNA sequence of key is found and then Vigenere decryption is done in reverse direction until all the DNA characters of cipher text are fully exhausted.

H. Transcription

Transcription is the first step of DNA based gene expression, in which a particular segment of DNA is copied into RNA (especially mRNA) by the enzyme RNA polymerase. Both DNA and RNA are nucleic acids, which use base pairs of nucleotides as a complementary language.

DNA sequence- AGTG CTA
RNA sequence- AGUG CUA

V. ENCRYPTION ALGORITHM

The encryption algorithm steps are:

1. Get the bit pattern of the plain text.
2. Complement the prime position of the bit stream.
3. Reverse the entire bit pattern
4. Again complement the prime position of the bit stream.
5. Perform bitwise XOR on bit 1 and n and substitute in nth position.
6. Leave the first n/2 bit as it is.
7. Repeat step 5 and 6 until all the bits are exhausted.
8. Shuffle the bit that is exchange the first half with the last half of the bit stream.
9. Repeat steps 10,11,12,13,14,15,16 and 17 ‘x’ no. of times where ‘x’ is the number of characters in random input key.
10. Store it in 2d array of n*n. n=nearest perfect square lesser than the bit stream. Residue bits in a 1d array.
11. Bit wise left shift.
12. Bit wise up shift.
13. Bit wise diagonal shift.
14. Bit wise right shift.
15. Bit wise down shift.
16. If no. of 1 in Plain text is even then right shift the 2D array by n/2 otherwise by n/4 times.
17. Shift the bits from 1d array into 2d array and same no of bits are shifted from 2d to 1d array. Reconstruct the bit stream.
18. Convert it in DNA sequence

a. 00-A 01-C 10-G 11-T.

19. Apply transcription by converting 'T' with 'U'.
20. Call method for generating random variable length spliced key using splicing system.
21. Now we remove the spliced key from the DNA sequence.
22. Encrypt the spliced key using the input key by Vigenere Encryption Method and reverse it.
23. Apply crossover to M-RNA (combined DNA sequence and encrypted spliced key) based on the position of 1 in random key.
24. Apply mutation to the above result at the places mentioned by the position of 1 in binary value of random input key.(A & G and C & U are complementary DNA)
25. Perform Full Vigenere Encryption on cipher text so that all the DNA characters of cipher text and random input key are fully exhausted in encryption purpose.
26. Replace each 4-bit pattern from the DNA sequence (binary values only) with the ASCII code to generate cipher text.
27. Print the Cipher text.

FOR GENERATING RANDOM VARIABLE LENGTH KEY / SPLICED KEY

Step 1: Take the DNA sequence and find 'A'.

Step 2: Whenever 'A' occurs, splice two consecutive letters followed by an 'A'

and store them into another placeholder(key).

Step 3: Print the key.

VI. DECRYPTION ALGORITHM

The steps of decryption algorithm are:

1. Get the bit pattern of the cipher text.
2. Convert the cipher text to DNA code sequence (i.e., m-RNA). (This method is called reverse translation).
3. Perform Full Vigenere Decryption on cipher text so that all the DNA characters of cipher text and random input key are fully exhausted in encryption purpose.
4. Apply mutation to the above m-RNA at the places mentioned by the position of 1 in binary value of random input key.(A & G and C & U are complementary DNA)
5. Apply reverse crossover to M-RNA based on the position of 1 in random key to generate combination of plain text DNA sequence and encrypted spliced key.
6. Identify the encrypted spliced key and Decrypt the spliced key using the input key by Vigenere Table and spliced key decryption technique. Generate the DNA sequence by merging spliced key to m-RNA.
7. Apply transcription by converting 'U' to 'T'.
8. Convert it in binary sequence from DNA sequence
   00-A 01-C 10-G 11-T.
9. Repeat steps 10,11,12,13,14,15,16, 17 and 18 ‘x’ no. of times where ‘x’ is the number of characters in random input key.
10. Store it in 2d array of n*n. n=nearest perfect square lesser than the bit stream. Residue bits in a 1d array.
11. Shift the bits from 1d array into 2d array and same no of bits are shifted from 2d to 1d array.
12. If no. of 1 in Plain text is even then left shift the 2D array by n/2 otherwise by n/4 times.
13. Bit wise up shift.
14. Bit wise left shift.
15. Bit wise reverse diagonal shift.
16. Bit wise down shift.
17. Bit wise right shift.
18. Store the 2d array and Residue bits of 1d array in a 1d array.
19. Shuffle the bit that is exchange the first half with the last half of the bit stream.
20. Perform bitwise XOR on bit 1 and n and substitute in nth position. Leave the first n/2 bit as it is. Repeat this step until all the bits are exhausted.
21. Complement the prime position of the bit stream.
22. Reverse the entire bit pattern
23. Again complement the prime position of the bit stream.
24. Convert this bit pattern to ASCII code to generate plain text
25. Print the Plain Text.

VII. RESULTS

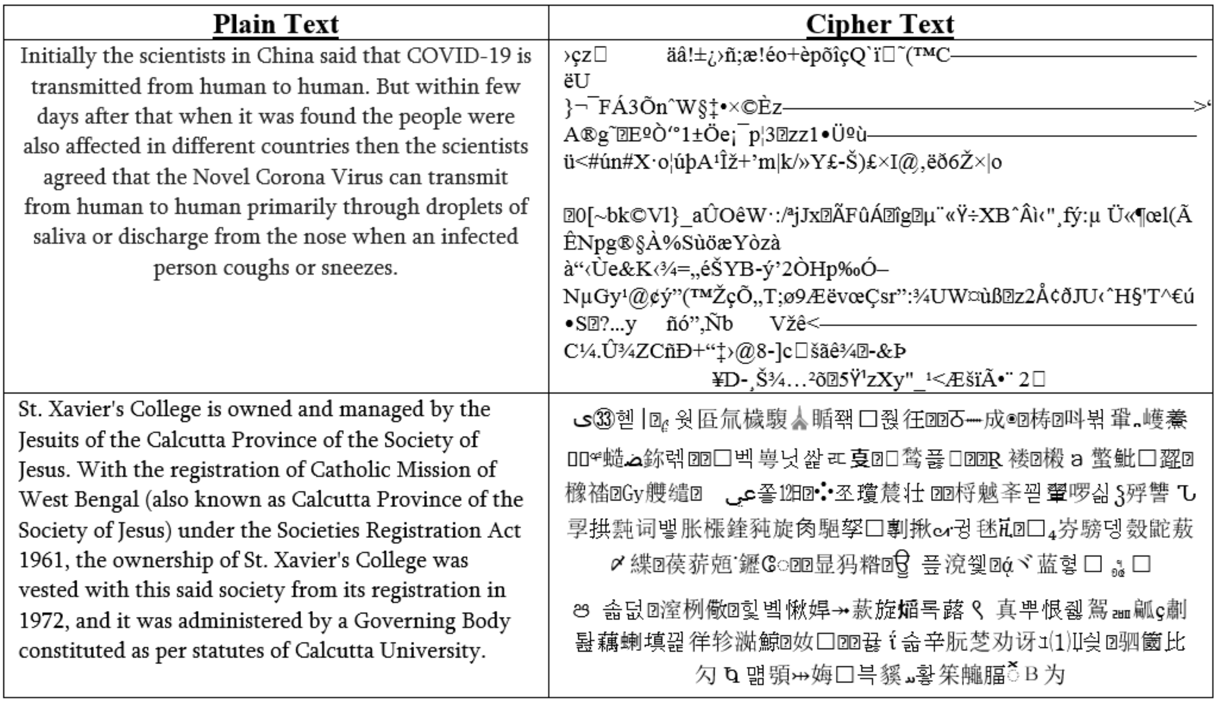
In the table-2 given below some plain texts and the corresponding ASCII value of cipher text are shown. There are many instances where it was observed for the same key, almost similar plain texts, the cipher texts are totally different. So without knowing the secret text-key and the actual decryption process it is quite impossible for the intruder to generate the plain text from the cipher text.

TABLE 2. Some Plain Texts and Ascii Code of Encrypted Texts

Srl	**PLAIN TEXT**	**KEY**	**CIPHER TEXT ASCII VALUE**	**CIPHER TEXT**
1	ABAB	St. Xavier’s College	22,102,87,230	fWæ
2	BABA	St. Xavier’s College	166,158,192,10	¦žÀ
3	0000	St. Xavier’s College	221,114,205,190	ÝrÍ¾
4	0001	St. Xavier’s College	54, 122,249,127	6zù•
5	HE IS GOON	st. xavier's college	194,197,100,69,36,216,218,167,67,229	ÂÅdE$ØÚ§Cå
6	HE IS GOOD	st. xavier's college	194,197,100,102,102,47,216,195,205,5	ÂÅdff/ØÃÍ
7	HE IS GOOF	st. xavier's college	194,197,100,70,36,216,218,167,66,229	ÂÅdF$ØÚ§Bå
8	MADAM	A	19,154,95,190,46	š_¾.
9	Aerostat	st. xavier's college	16,155,218,55,159,90,188,59	›Ú7ŸZ¼;
10	Aerrstat	st. xavier's college	83,80,168,73,204,54,208,39	SP¨IÌ6Ð'

In above table the results show that the cipher texts ate totally unpredictable even though the Plain texts contain some trivial patterns. The present method shows cipher texts always different even if input plain contains all characters same. The following table-3 shows a Plain Text file containing a paragraph and its encrypted file encrypted using key ‘AAAA’

TABLE 3. Plain Text file containing paragraph and its encrypted file.



Plain Text	**Cipher Text**
Initially the scientists in China said that COVID-19 is transmitted from human to human. But within few days after that when it was found the people were also affected in different countries then the scientists agreed that the Novel Corona Virus can transmit from human to human primarily through droplets of saliva or discharge from the nose when an infected person coughs or sneezes.	›çz□ ää!±¿›ñ;æ!éo+èpõîçQ`ï□˜(™C ëU }¬¯FÁ3ÕnˆW§‡•×©Èz >‘ A®g˜□EºÒ‘°1±Öe¡¯p¦3□zz1•Üºù ü<#ún#X·o¦úþA¹Îž+’m|k/»Y£-Š)£×I@,ëð6Ž×|o □0[~bk©Vl}_aÛOêW·:/ªjJx□ÃFûÁ□îg□µ¨«Ÿ÷XBˆÂì‹",fý:µ Ü«¶œl(Ã ÊNpg®§À%SùöæYòzà à“‹Ùe&K‹¾=„éŠYB-ý’2ÒHp‰Ó– NµGy¹@¢ý”(™ŽçÕ„T;ø9ÆëvœÇsr”:¾UW¤ùß□z2Å¢ðJU‹ˆH§'T^€ú •S□?...y ñó”,Ñb Vžê< C¼.Û¾ZCñÐ+“‡›@8-]c□šãê¾□-&Þ ¥D-¸Š¾…²õ□5Ÿ¹zXy"_¹<ÆšïÃ•¨ 2□
St. Xavier's College is owned and managed by the Jesuits of the Calcutta Province of the Society of Jesus. With the registration of Catholic Mission of West Bengal (also known as Calcutta Province of the Society of Jesus) under the Societies Registration Act 1961, the ownership of St. Xavier's College was vested with this said society from its registration in 1972, and it was administered by a Governing Body constituted as per statutes of Calcutta University.	ى㉝헬 |□ 윓 叵 氚 檨 駿 晒 잭 □ 졣 徍□□ㆁ 成□梼□믜 봒 翬 嶁 鮝 □□ 螠 ض 鉥 렉 □□□ 벡 塆 넛 쐁 ㄹ 叓□□ 鸄 픎 □□□R 褛□檓 ə 螿 魮 □ 翿□ 橼 褡□Gy 艘 缮□ عي 졽 12ㅂ□ ⁘ 丕 瓆 蕽 壮 □□梣 魆 夆 꾇 翚 啰 싦 ʒ 殍 髻 Ꭴ 孠 拱 瓡 词 뻴 胀 棖 鏲 豘 旋 肏 駔 挐 □ 剸 揪 ര 귕 毬 ň□□₄ 岺 驁 뎅 瞉 龅 蔽 〆 緤□葔 菥 殖 鑩 ℭ○□□ 显 犸 糌□ 믐 浣 쮤□ q ヾ 蓝 혛 □ □ ඡ 숨 딦□滏 栵 儆□힟 볭 愀 婥 ↣ 蔌 旋 婿 록 蕗 ᠺ 真 뿌 恨 쥥 駕 ₂₈₈ 颩 ç 劏 홢 藕 蝲 填 꿆 徉 轸 滶 鯨□妏 □□□ 꿆 í 숩 辛 朊 楚 劝 讶 ɿ⑴ ꟷ 싍 □驷 籄 比 勺 ᥰ 맵 頨 ↠ 娒 □ 븍 豯 ᵕ 횡 笨 艫 腷 B 为

In Figures 3 to 12 the encrypted data and also plain text data are shown while in fig-13 the graph of first paragraph and encrypted plain text is shown. The results show that the Cipher texts patterns are totally unpredictable. The hackers will not be able apply any kind of brute force method to find Plain Text without knowing secret key. The present may be used to encrypt confidential message such as password, key etc. Following are the graphical representation of mapping of plain text vs. cipher text to show the unpredictability

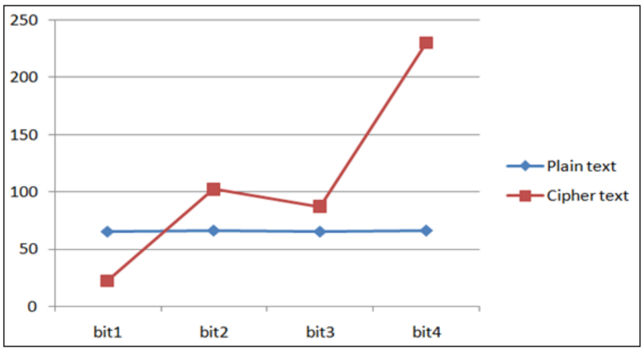


Figure 3. Graph between 'ABAB' and its cipher text with key as 'St. Xavier's College'

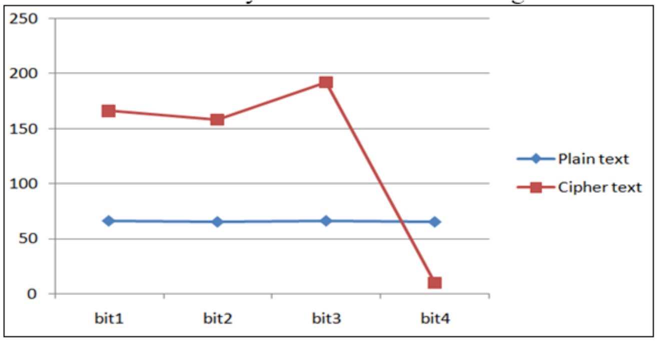


Figure 4. Graph between 'BABA' and its cipher text with key as 'St. Xavier's College'

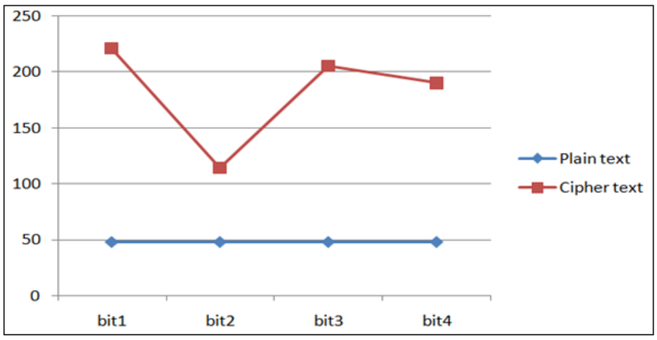


Figure 5. Graph between '0000' and its cipher text with key as 'St. Xavier's College'

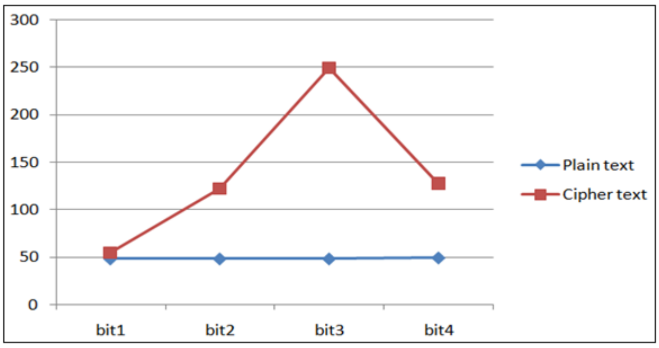


Figure 6. Graph between '0001' and its cipher text with key as 'St. Xavier's College'

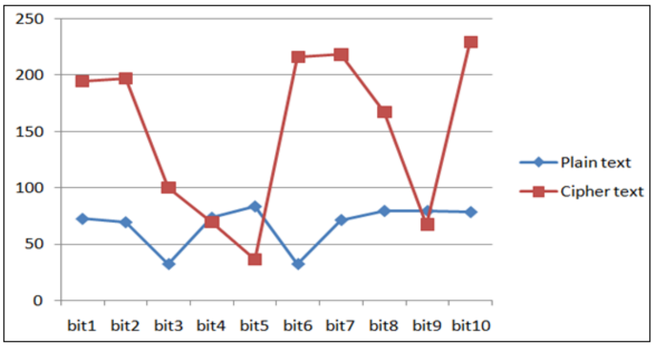


Figure 7. Graph between 'HE IS GOON' and its cipher text with key as 'st. xavier's college'

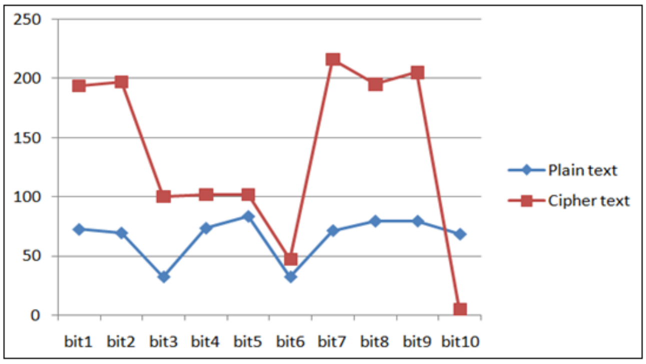


Figure 8. Graph between 'HE IS GOOD' and its cipher text with key as 'st. xavier's college'

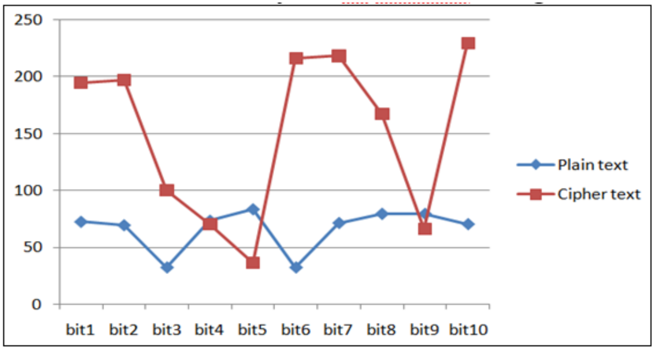


Figure 9. Graph between 'HE IS GOOF' and its cipher text with key as 'st. xavier's college'

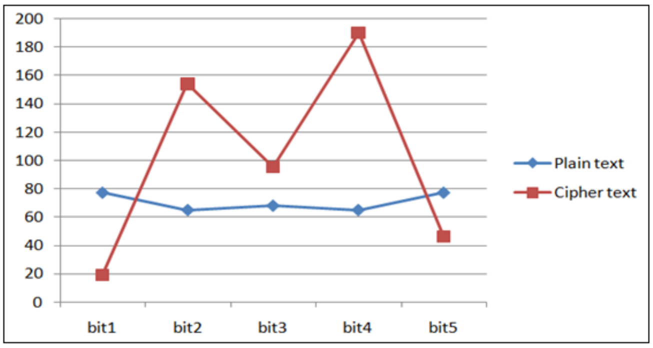


Figure 10. Graph between 'MADAM' and its cipher text with key as 'A' where key size is less than plain text

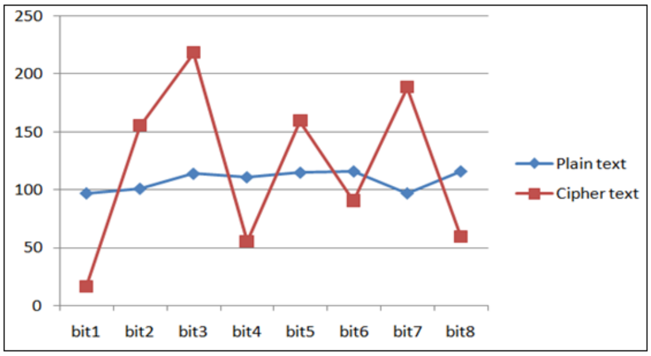


Figure 11. Graph between 'aerostat' and its cipher text with key as 'st. xavier's college'

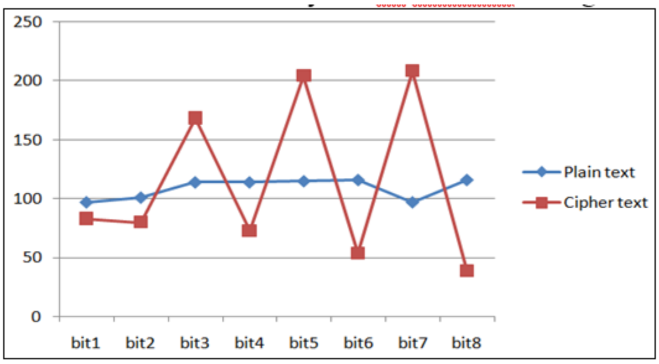


Figure 12. Graph between 'aerrstat' and its cipher text with key as 'st. xavier's college'

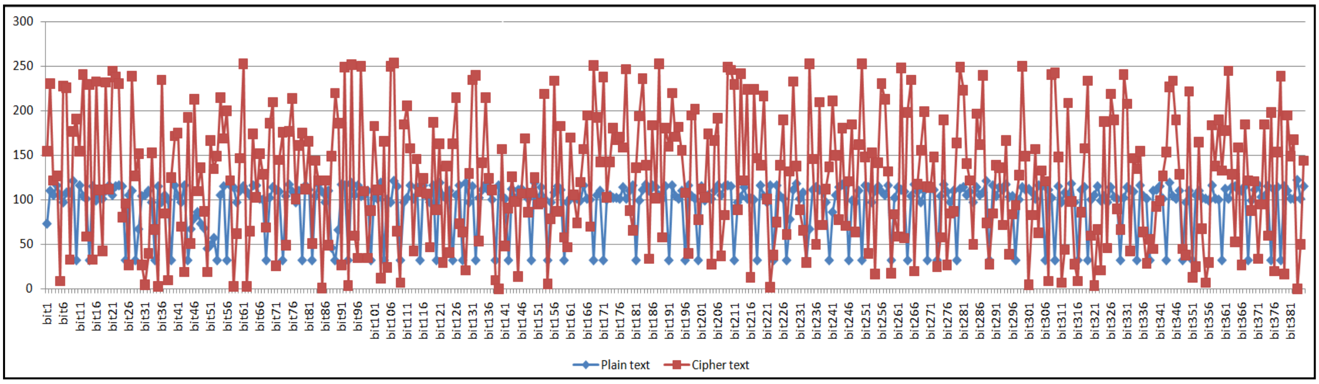


Figure 13. Graph between paragraph 1 and its cipher text with key as 'AAAA'

VIII. DISCUSSIONS

1. If we can follow the above mentioned table, we can see that if we change a single character in a plain text, the whole cipher text gets changed too. For example, cipher text of the plain text '0000' is 'ÝrÍ¾ ', where the key is 'St. Xavier's College' and in the next case, cipher text of the plain text '0001' is '6zù', which is totally different from the previous case.

2. Change of the key will give us different cipher text of the same plain text. For example if we use the key 'St. Xavier's College' in the method of encryption, the cipher text of the plain text 'AAAA' will be '¹l}' and if we change the key, that is, if we use 'st. xavier's college' we can get a totally different cipher text of plain text 'AAAA' that is 'Ö̩?'.

3. The results show that the cipher texts ate totally unpredictable even though the Plain texts contain some trivial patterns. The present method shows cipher texts always different even if input plain contains all characters same.

4. The hackers will not be able apply any kind of brute force method to find Plain Text without knowing secret key.

5. The length of secret key is variable as it can be greater than the length of plain text or even lesser than the length of plain text. Guessing the length of key is very difficult as DNA Vigenere cipher, crossover, mutation are applied to the DNA characters.

6. Avalanche Effect[12]

In cryptography, the avalanche effect is used to quantify the effect on cipher-text when a slight modification takes place in the plain text or the key. A slight modification of the plain text or the key means changing or flipping a bit in the text.

The formula to calculate the avalanche effect -

Avalanche effect =(Number of bits changed in ciphertext / Number of total bits in ciphertext) X 100%.

The following is the calculation of the avalanche effect to various cryptographic techniques.

Plaintext1: aerostat
Plaintext2: aerrstat
Key: eggplant

a. Caesar Cipher

Ciphertext1:011001100110101001110111011101 00 0111100001111001011001100111100

Ciphertext2:011001100110101001110111011101 11 0111100001111001011001100111100 1

b. Playfair Technique

Ciphertext1:01100111011000010111001101110001 0111000101100011011101000110100 0

Ciphertext2:01100111011000010111100101111001 0111000101100011011101000110100 0

c. Vigenere Cipher

Ciphertext1:01100101011010110111100001100100 0110010001110100011011100110110 1

Ciphertext2:01100101011010110111100001100111 0110010001110100011011100110110 1

d. ASKCA VER-1.0

Ciphertext1:01101110101010000101001010000101110010011010001001111011110101 00

Ciphertext2:01011010101010000101001010000101110011011010001001111011111111 00

The following table shows the comparison results of various crypto algorithms and the proposed algorithm :

TABLE 4
Comparison results of Avalanche Effect for strings "aerostat" and "arrstat" Comparison in avalanche effect

Name of the Algorithm	**Number Of bits flipped**	**%**
Ceaser Cipher	2	3.125
Playfair	3	4.69
Vigenere Cipher	2	3.125
ASKCA VER-1.0	6	9.375

The result of the avalanche effect of the proposed algorithm is slightly better than the result of the avalanche effect of other mentioned crypto algorithms.

IX. FUTURE SCOPE

1. Every application has its merits and demerits. The project has covered almost all requirements. Further requirements and improvements can easily be done since coding is mainly structured or modular in nature.
2. By implementing another layer into the transposition method we can extend this algorithm to 4 dimensions.
3. The present algorithm can be applied to files like .txt, .png, .jpg, .dll, .exe etc. But the authors have implemented the method in basic text files and the results were quite satisfactory.
4. Currently it is not feasible to use this method for large files as execution time is high.

This method can also be modified to send only the DNA stream as output of the plain text which will reduce the transfer file size to half of the original.

X. CONCLUSION

In this era of technology, any kind of information is a valuable asset. So protection of the information should be at the top of the priority list. Not only we store this information but also we pass the information from one end to another ends. Since the information is being shared through the internet, the vulnerabilities to the integrity of that information will increase too. To avoid this kind of scenario we need to protect the vital information from the people who can use them for their benefits or bring harm to others. We can prevent this kind of scenario by using this algorithm so that no one can hack it easily. This encryption and decryption method can be applied to various types of files such as .txt, .doc, etc. Hacker cannot decrypt the encrypted plain text without the spliced key since the spliced key is generated from the plain text itself only.

XI. ACKNOWLEDGMENT

We are very much grateful to the Department of Computer Science to give us this opportunity to work on symmetric key Cryptography. One of the authors (AN) sincerely expresses his gratitude to Rev. Dr. Dominic Savio, S.J., Principal of St. Xavier's College (Autonomous) for giving constant encouragement in doing research in cryptography.

XII.REFERENCES

[1]. L.M. Adleman, Molecular Computation of solutions to combinatorial problems, 'Science', 266:10211024, November 1994

[2]. Behnam Bazli, Mustafa Anil Tuncel and David Llewellyn-Jones," DATA ENCRYPTION USING BIO MOLECULAR INFORMATION", International Journal on Cryptography and Information Security (IJCIS), Vol. 4, No. 3, pp.21-33, September 2014

[3]. A. Gehani, T. Labean, and J. Reif, "DNA-Based Cryptography," pp. 1–17, 2000.

[4]. Asoke Nath, Madhumita Santra, Supriya Maji and Kanij Fatema Aleya,"3-Dimensional Bit Level Encryption Algorithm Ver-1(3DBLEA-1)", International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 4, pp. 8611-8618 Issue 5, MAY 2016.

[5]. Asoke Nath, Ayan Ghosh, Enakshi Ghoshand Jayisha Saha,"3-Dimensional Bit Level Encryption Algorithm Ver-2(3DBLEA-2)", International Journal of Advanced Research in Computer Science and Management Studies (IJARCSMS), Vol. 5, pp. 30-37 Issue 7, JULY 2017

[6]. Behrouz A. Forouzan, "Cryptography and Network Security", Special Indian edition 2007, Tata McGraw Hill publishing company limited, pages - 2-13and 56-58

[7]. Nath, Asoke & Ray, Soumyadip & Dhara, Salil & Hazra, Sourav. (2018). 3-DIMENSIONAL BIT LEVEL ENCRYPTION ALGORITHM VERSION-3 (3DBLEA-3).10. 10.21172/1.102.55.

[8]. E. Suresh Babu, C. Naga Raju, and Munaga HM Krishna Prasad, "Inspired Pseudo Biotic DNA Based Cryptographic Mechanism Against Adaptive Cryptographic Attacks", International Journal of Network Security, Vol.18, No.2, PP.291-303, Mar. 2016

[9]. Mohammadreza Najaftorkaman and Nazanin Sadat Kazazi," A Method to Encrypt Information with DNA-Based Cryptography", International Journal of Cyber-Security and Digital Forensics (IJCSDF), the Society of Digital Information and Wireless Communications, 2015 (ISSN: 2305-0012), pp. 417-426

[10]. Ashish Kumar Kaundal and A.K Verma,"DNA Based Cryptography: A Review", International

Journal of Information& Computer Technology, Vol. 4, pp. 693-698 Issue 7,2014

[11]. Hamdy M. Mousa, “DNA-Genetic Encryption Technique”, Computer Network And Information Security, pp. 1-9, Issue 7,2016

[12]. P.Bharti Devi and Dr. R Kiran Kumar,”Inspired Fiestel DNA Based Crypto System Using D-Box”, International Journal of Applied Engineering Research (ISSN: 0973-4562), Vol. 13, pp. 2847-2856, Issue57,2018

Cite this article as :

Asoke Nath, Ankita Kedia, Sunanda Pal, Moumita Sen, "Advanced Symmetric Key Cryptography Algorithm: Application of Pseudo Biotic DNA Method(ASKCA VER-1.0) ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.884-895, May-June-2020. Available at
doi : https://doi.org/10.32628/CSEIT2063210
Journal URL : http://ijsrcseit.com/CSEIT2063210