Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of Cryptography using DNA Secret Writing Techniques with OTP

[1]G. Jeevitha, [2]G. Sasikala

[1] Research Scholar, Dept. of Computer Science, [2] Assistant Professor/Dept.of Computer Science
[1, 2] Adhiparasakthi College of Arts and Science (Autonomous), Kalavai,
Vellore, Tamil Nadu, India

Abstract*—In this paper, a brand new scientific discipline technique referred to as polymer cryptography and therefore the already existing ways of recent cryptography area unit studied, enforced and results area unit obtained. Each this scientific discipline method's results area unit compared and analyzed to seek out the higher approach among the 2 ways. The comparison is completed within the main aspects of method period, key size, procedure quality and scientific discipline strength. and therefore the analysis is formed to seek out the ways in which these on top of mentioned parameters area unit enhancing the individual scientific discipline ways and therefore the performance is evaluated The projected system uses the principles of bio molecular computation (BMC) and several other algorithms for polymer (deoxyribonucleic acid) steganography and cryptography: One- Time-Pad (OTP), polymer XOR OTP and polymer chromosomes classification. It represents a synthesis of our add the sector, sustained by former referred publications. Experimental results obtained exploitation Matlab Bioinformatics tool cabinet and conclusions area unit ending the work.

***Index Terms*— Steganography, RNA, DNA, Cryptography, Secret Writing, BMC, PCR**

I. INTRODUCTION

From the traditional days until gift, the key writing techniques area unit practiced to safeguard the info from the adversaries. And among the techniques, cryptography and steganography area unit most typical and wide used ways. Cryptography wills the action of encrypting the info whereas steganography hides the info from the hackers. within the scientific discipline method, bound parameters area unit to be thought of. The cryptography and coding method key generation, encrypted information kind, technique of retrieving the information back from the encrypted data area unit the foremost vital among them.In recent years, encrypted signal process has attracted significant analysis interests. The separate Fourier remodel and reconciling filtering may be enforced within the encrypted domain supported the homomorphy properties of a cryptosystem, and a composite signal illustration technique may be accustomed scale back the dimensions of encrypted information and computation quality. In joint cryptography and information concealing, a vicinity of great information of a lucid signal is encrypted for content protection, and therefore the remaining information area unit accustomed carry buyer–seller protocols, the fingerprint information area unit embedded into Associate in Nursing encrypted version of digital transmission to make sure that the vendor cannot grasp watermarked version whereas the buyer cannot acquire the initial product. variety of works on compression encrypted pictures are additionally bestowed. once a sender encrypts an imaginative image for privacy protection, a channel supplier while not the data of a scientific discipline key and original content could tend to cut back the info quantity because of the restricted channel resource.

Secret writing is that the term used for data protection against adversaries. The foremost wide used techniques of secret writing area unit cryptography and steganography. Cryptography manipulates the data to be misunderstanding for adversaries, whereas steganography is concealing its terribly existence. polymer cryptography and steganography may be a new field bornflomAdleman's analysis in polymer computing and fiomVivianaRisca's project on polymer steganography. the massive benefits that polymer structure offers for economical parallel molecular computation and its huge storage capabilities, made up of this analysis field a awfully promising one for varied applications despite nowadays limitations: expansive or time intense. once a quick introduction on bio molecular technologies the paper investigates a spread of bioinformatics techniques and proposes many algorithms for concealing and encrypting the information: one-time-pad principle and polymer coupling for symmetrical cryptography, polymer chromosomes classification scientific discipline formula, and polymer XOR (Exclusive OR) exploitation tiles for scientific discipline functions.

II. RELETAD WORKS

The presently practiced technique of cryptography that is that the fashionable technique of cryptography is tough to interrupt attributable to the massive mathematical computations and therefore the size of the key concerned in it. additionally this additionally finishes the method in an exceedingly less time. So, it already provides an honest security and takes solely less time for the message to be communicated. And it's tough for the adversaries to hack the info. though an honest theme of security is prevailed and practiced, it's been introduced a brand new technique within the field of cryptography referred to as the 'DNA cryptography' indicating that this technique allows the confidentiality of the info additional high than the trendy ways ,with the utilization of OTP keys and its size. Additionally it's believed that within the polymer cryptography, the key may be generated for a huge length of information compared to the trendy ways during which key area unit generated just for a smaller length of the info. thus it's aforesaid that, the polymer technique offers the confidentiality for a wider vary of information in an exceedingly less time.

The objective of this paper is to check the trendy ways of formula and therefore the polymer formula by comparison the parameters like cryptography and coding period, key size, mathematical expressions concerned in the algorithm, scientific discipline strength, procedure quality, memory, cost, and information length.

III. IMPLEMENTATION

CRYPTOGRAPHY REVIEW

Cryptography is that the science of encrypting and decrypting the info therefore on keep the info additional secured. it's capable of keeping the info secretly whereas saving the data or passing it over the unsafe networks, like net. This can be tired order to safeguard the info from the hackers and create it comprehendible solely to the meant receiver.

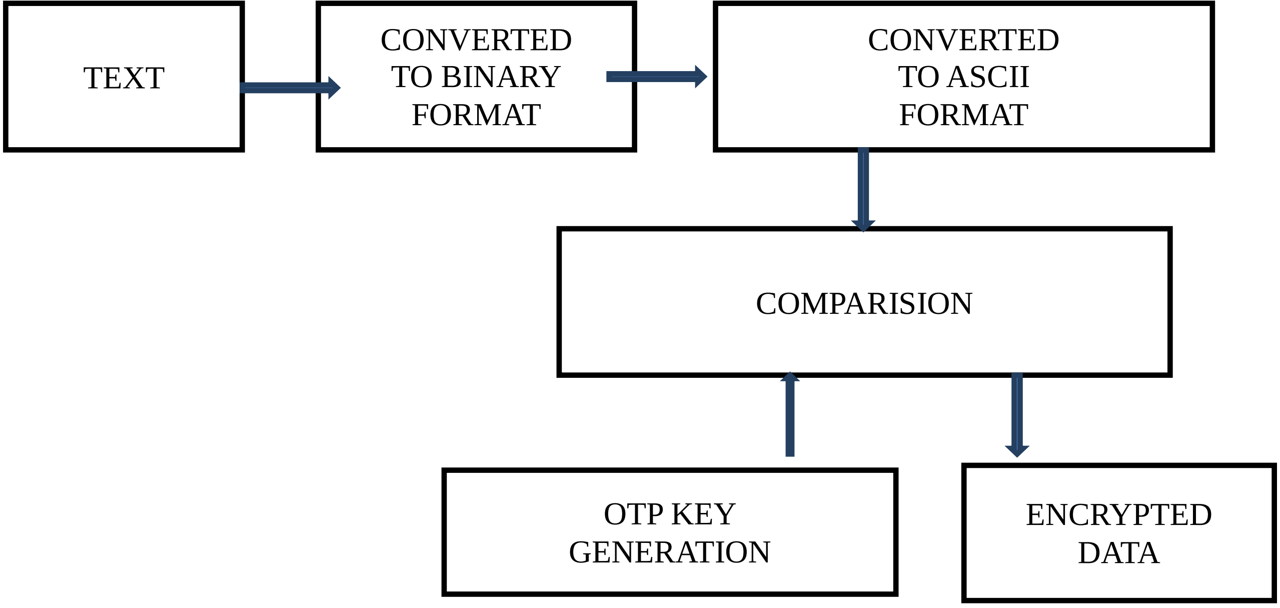


FIG 1: BLOCK DIAGRAM OF PROPOSED SYSTEM TRANSMITTER SIDE

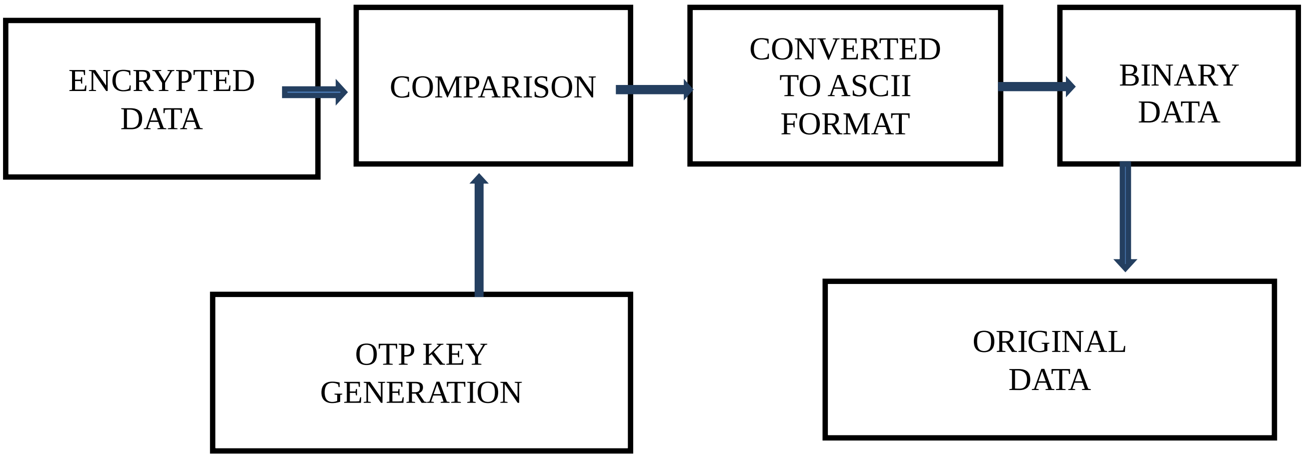


FIG 2: BLOCK DIAGRAM OF PROPOSED SYSTEM RECEIVER SIDE

PROJECT DESCRIPTION

DNA, the key support of genetic data (genetic blueprint) of any organism within the part, consists of 2 long strands of nucleotides, every containing one among fourbases (A – A, G – purine, C – pyrimidine, T – thymine), a carbohydrate sugar and a phosphate cluster. The polymer strands have chemical polarity, which means that on every finish of a molecule there area unit totally different teams (5' – prime finish and 3' – bottom end) [3]. A polymer molecule has double-stranded structure obtained by 2 fibre polymer chains, secure along by gas bonds: A = T covalent bond and C ≡ G triple bond. The helix structure is designed by 2 single parallel strands . The polymer strands that bond one another through A-T and C-G bonds area unit called complementary strands.

The polymer strands may be with chemicals synthesized employing a machine, called polymer synthesizer. The fibre chains obtained unnaturally with the polymer synthesizer area unit named oligonucleotides having sometimes 50-100 nucleotides long. within the gift paper the individual strands are going to be documented as fibre polymer (ssDNA), and therefore the helix as double-stranded polymer (dsDNA). Individual ssDNA will, below bound conditions, kind dsDNA with different complementary ssDNA. This method is named coupling, as a result of the double-stranded molecules area unit hybrids of strands returning from totally different sources.

Elements of Bio Molecular Computation (BMC)

Adleman projected this Bio Molecular Computation technique so as to resolve the combinatorial search issues. it had been done by exploitation the parallel combinatorial search with the massive solutions created by the polymer strands. there have been additionally proposals to destroy the DES (Data cryptography Standard) by exploitation the BMC ways. Excluding the combinatorial search, there area unit several different smart uses in BMC attributable to the exceptional saving capability of polymer. Actually, there area unit regarding 108 terra-bytes of information in an exceedingly gram of polymer. thus for a giant category of information, polymer may be an honest storage info medium.

DNA OTP generation in 2 main ways:

- Conversion of binary information to polymer format and contrariwise
- DNA tiles
- DNA XOR with tiles

DNA based mostly Cryptography

With the study of polymer computing, there was found a new emerged technique referred to as polymer cryptography. during this technique the biological technical data is employed as implementation suggests that whereveras the polymer is employed because the carrier information. the large denseness and therefore the vast uniformity within the polymer molecules area unit examined for the authentication, encryption, signatures and connected scientific discipline functions. during this literature, the biological terms associated with polymer cryptography and its computing principles followed with the development of key problems concerned within the same technique's analysis field is explained. beside it, polymer cryptography's tendency and its security, standing and application area unitas are analyzed thereupon of the quantum cryptography and therefore the fashionable cryptography.

IV. RESULTS

DNA coupling TECHNIQUE

As altogether the scientific discipline ways, the polymer coupling technique additionally involves the cryptography and coding processes in changing the plaintext into the cipher text and so retrieving back the initial message.

Encryption

Plain text:

The original message that is to be transmitted to the receiver is taken as plain text.
Let us think about the plain text to be 'HELLO'.

Conversion of Plain text to Binary Form:

The plain text is at the start reborn to the computer code code. And second, it's once more reborn to the binary message.
The corresponding ACII code.

7269767679

Into Binary kind the subsequent

0100100001000101010011000100110001001111

The computer code code is additional reborn to its equivalent binary variety of the info.

OTP KEY:

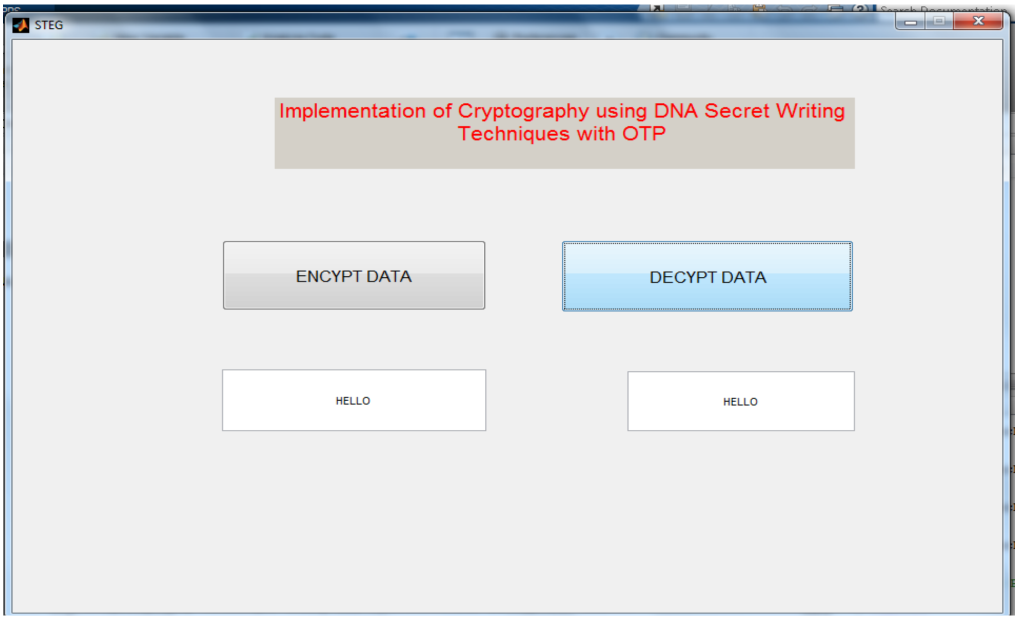
The OTP is generated by combining the random oligonucleotides (ssDNA) strands beside facilitate of a brief polymer fragment as model.
The first digit of the binary bit is one. This binary bit one is compared with the last ten bases of the OTP key and therefore the complementary information of the polymer kind is created because the encrypted message. The complementary information of the polymer sequences is that the oligonucleotide sequence.
CAGCGGGAACGGCTGTGCAGTCACACCGCTGTGTAGCGGACAGTCTGAGCTACCCTCTCAAGCACGAGATC
TACAGGGCGGGGTAGAAGCCGTCGCTTCGGGTCCATGCGGGGGGTAAAACCCTGTTTAAGAGGTCCGGGC
AGCATACGCGCGGCACCCATCTCTCTTCATTCGCTTATTGTGAACGTTCGAAAGCACAATGTGGTTTATGTG
CTACTGTGGAGAGGGTTTGTGAATCTAGGAGCACAAAAAAGCGGCGCACTTCAGGCATAAAAGGATGGAT
TTTTGACAATCCCCGATGTCCAAGCTATGGTCCCTTAACAGCAATGCTAGGGAGCAATAAACATAACCATC
CACAGTGAATTGATCCGAAGGGGGTCGGCATCGGAAGCTTGAAATT

Decryption

It is famous that in the cryptography method, the comparison was done from the reverse. So, within the coding method, the primary ten bits of the encrypted message is compared with the last ten bits of the OTP key, is that they area unit found to be complementary then a binary '1' is made. If the complementary matches aren't found, it's merely replaced with a zero, '0'.

Message Recovery

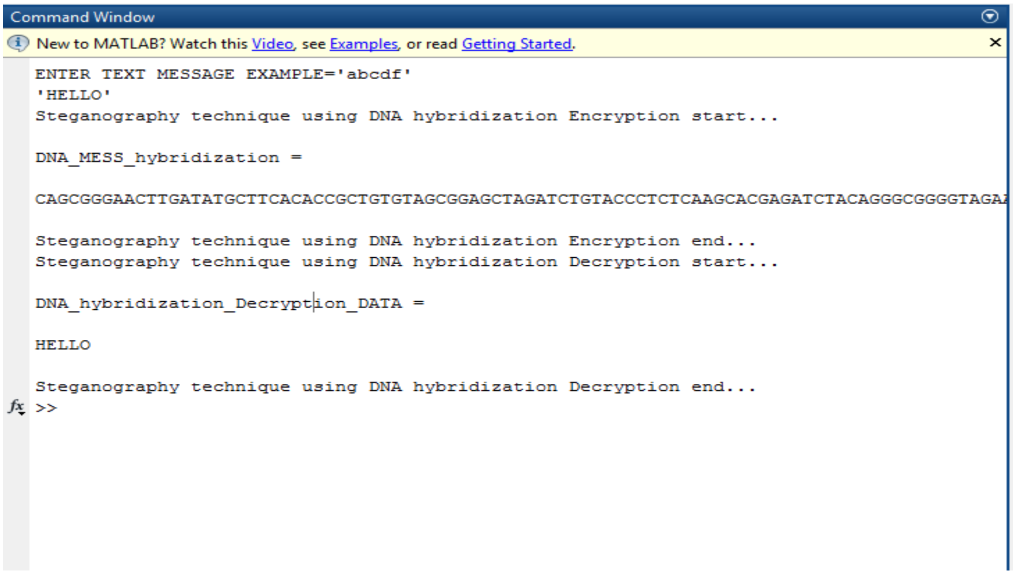
The original message that is to be received from the transmitter is get as plain text.
'HELLO'


STEG
Implementation of Cryptography using DNA Secret Writing Techniques with OTP
ENCYPT DATA
DECYPT DATA

HELLO

HELLO

FIG 3: FINAL graphical user interface OF THIS PROJECT


Command Window
New to MATLAB? Watch this Video, see Examples, or read Getting Started.

```
ENTER TEXT MESSAGE EXAMPLE='abcdf'
'HELLO'
Steganography technique using DNA hybridization Encryption start...

DNA_MESS_hybridization =

CAGCGGGAACTTGATATGCTTCACACCGCTGTGTAGCGGAGCTAGATCTGTACCCTCTCAAGCACGAGATCTACAGGGCGGGGTAGAA

Steganography technique using DNA hybridization Encryption end...
Steganography technique using DNA hybridization Decryption start...

DNA_hybridization_Decryption_DATA =

HELLO

Steganography technique using DNA hybridization Decryption end...
>>
```

FIG 4: MATLAB WINDOW AND space

V. CONCLUSION

Thus, the polymer cryptosystems containing the polymer coupling technique, the polymer classification technique and therefore the OTP approach area unit studied, explained, enforced and therefore the corresponding results area unit taken from MATLAB. The analysis of all the protection parameters associated with every technique is completed and compared and so, the performance is evaluated.Taking under consideration the massive advance in polymer technology, particularly in microarray, the nowadays bio-processor obeying Moore's law, we have a tendency to should expect a quicker repetition of microchip evolution and at larger scale. Options and benefits of the polymer cryptography area unit acknowledged on the presentation, however the molecular laboratory experiments can finally validate the benefits and limitation during this field.

REFERENCES

[1] L. M. Adleman, “Molecular computation of answer to combinatorialproblems”, Science, vol. 266, pp. 1021-1024, Nov 1994.

[2] C. Taylor, V. Risca, and C. Bancroft, “Hiding messages in DNAmicrodots”, Nature, vol. 399, pp. 533-534, 1999.

[3] M. Schena, “Microarray Analysis”, Wiley-Liss, July 2003.

[4] Arizona Board of Regents and Center for Image process inEducation, “Gel action Notes what's it and the way will it work”,1999.

[5] B. Schneier, “Applied Cryptography: Protocols, Algorithms, and SourceCode in C”, John Wiley &amp; Sons, Inc, 1996.

[6] A. Gehani, T. LaBean, and J. Reif, “DNA-Based Cryptography”,Lecture Notes in engineering science, Springer. 2004.

[7] H. Wang, “Proving theorems by pattern recognition”, Bell SystemsTechnical Journal forty, pp. 1-42. 1961.

[8] S. Roweis, E. Winfree, R. Burgoyne, et all, “A sticker based mostly architecturefor polymer computation”, vol. forty four of DIMACS: Series in DiscreteMathematics and Theoretical engineering science, pp. 1-30. 1996.

[9] M. E. Borda, O. Tornea, T. Hodorogea, “Secret Writing by DNAHybridization”, ActaTehnicaNapocensis, vol. 50, pp. 21-24, 2009.

[10] S. T. Amin, M. Saeb, S. El-Gindi, “A DNA-based Implementation ofYAEA cryptography Algorithm”, IASTED, pp. 120-125, 2006.

[11] M. E. Borda, O. Tornea, T. Hodorogea, M. Vaida, “Encryption Systemwith classification polymer Chromosomes scientific discipline formula ”, IASTEDProceedings, pp. 12 – 15, 2010.

[12] http://www.ncbi.nlm.nih.gov

[13] O. Tornea, M. E. Borda, „DNA scientific discipline Algorithms”, MediTechCluj-Napoca, vol. 26, pp. 223-226, 2009.

[14] T. Bajenescu, M. E. Borda, “Securitate in informaticasitelecomunicatii”,Dacia,2002.