DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5860

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

BIT BASED SYMMETRIC ENCRYPTION METHOD USING DNA SEQUENCE AND QUANTUM TECHNIQUE TO GENERATE ENCRYPTED KEY

Ratnakumari Challa
Dept. of CSE, APIIIT (RGUKT)
Andhra Pradesh, India

N.Srilatha
Dept. of CSE, APIIIT (RGUKT)
Andhra Pradesh, India

kanusu Srinivasa Rao
Dept. of Computer Applications
Yogi Vemana University
Andhra Pradesh, India

Abstract: Now a day everyone wants to provide security to their data. Present days many methods are available for doing the Cryptography. DNA sequence key based cryptography became popular because of its more security features. In the paper, encryption technique proposed is based on using two methods: Quantum key distribution for generating a key corresponding to the bit of the plain text and DNA sequence based encryption for encryption of the plain text. Sender first performs complement and LBP operation on the data. Instead of sending the processed plain text bits, sender sends the complement of the key if the processed plain text bit is 0 otherwise sends the swapped key sequence. DNA Complement method on the key which is generated by the Quantum key generation method is done based on BB84 protocol. Two step encryption and decryption technique using DNA based encryption is proposed and practically implemented. The performance of the proposed technique is analysed and compared with other related techniques.

Keywords: DNA Cryptography, Quantum Key Distribution, Binary Bit;

1. INTRODUCTION

Cryptography is the science of encrypting and decrypting the data so as to keep the data more secured. It is capable of keeping the data in secret while saving the information or passing it over the unsafe networks, like internet. This is done in order to safeguard the data from the hackers and make it understandable only to the intended receiver. Because of its security base cryptography is one of the most vastly used and the most important fields. Even though it is a very ancient field, its need and significance has much improved in the modern times because of the rapid growth in the use of internet. And moreover, in the recent times the protection systems, shopping systems, banking systems and many other manual systems has been made into the practice of utilizing the website advantages. For all these applications of manual systems, the most confidential data involved in it is being transmitted over the internet and it is much susceptible to strikes or outbreaks like teardrop, IP spoofing, man in the middle attack and so on. So inorder to protect our data in our systems and website applications, it is highly necessary to rely on the strength of the cryptography. There exists a similar other area called cryptanalysis. It is executed analogous to the field cryptography. The main job in cryptanalysis is to break the security technique envisioned by the obedience of cryptography by analyzing it. Thus in a nut shell it can be said that 'Stronger the Cryptography, weaker the Cryptanalysis'. A big challenging work in designing and achieving the greater level of data confidentiality has been performed both in cryptography and cryptanalysis. The general process of cryptography involving both encryption and decryption is illustrated below in the Figure 1.

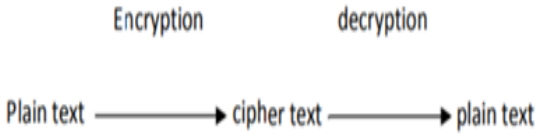


Fig. 1 Flow diagram of Cryptography

- **Plain text:** The original data which is to be transmitted is considered as plain text.
- **Encryption:** The method of obtaining the cipher text from plain text is known as encryption.
- **Cipher text:** The confused or the distorted data obtained as a result of encryption process is known as cipher text.
- **Decryption:** Decryption is the reverse process of encryption. The original message or the plain text is obtained as a result of this process.

In the proposed work, bit based symmetric key encryption using Quantum Key Distribution and DNA Sequence based encryption is implemented and experimented.

A. Quantum key Distribution Technique

In Quantum Cryptography, a Quantum Key Distribution is used for providing secure transmission. In 1984 Charles Bennett and Gilles Brassard published the first QKD protocol [1]. It was based on Heisenberg's Uncertainty Principle and is simply known as theBB84 protocol[2]. The basic model for QKD protocols involves two parties, referred to as Alice and Bob, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. Table shows how a bit can be encoded in the polarization state of a Photon in BB84.

Everybody has secrets, from military intelligence and banking transactions to rendezvous notes. Suppose Alice (sender) wishes to send a private message, or plaintext, to Bob (receiver), amidst. Attempts by a nosy Eve (eavesdropper) to covertly uncover the message. Alice could then encrypt the message using a secret code, or key, such as to render it unintelligible to Eve, provided of course the encryption/decryption algorithm" is known only to Alice and Bob.

B. DNA Sequence Based Encryption

Owing to the growth of science and study in the field of network, it is responsibility to secure our image, data from the third parties. For DNA cryptography, it gives a new path to the information in more secured manner. In DNA based cryptograph, DNA sequences are used to encrypt the data more powerful manner. Each DNA sequence is composed of three groups of components: i) sugar group ii) nitrogen group and iii) phosphate group. Mainly DNA based cryptography focuses on the nitrogen groups. As nitrogen groups are important to decide the physical appearance to the human being, In cryptography, the nitrogen group nucleic acids called adenine (A), thymine (T), Cytosine (C), guanine (G) are giving the proper appearances to the cryptographic algorithm. Generally the adenine acid always pairs with thymine acid as same as the guanine nucleic acid will always pairs with cytosine nucleic acids. It is also known as Watson-crick rule [3]. For example, in binary system if the adenine component is 00 means thymine component will be 11 similarly if the cytosine component is 10 means surely the guanine will be 01. From this we can able to know that the pairing nucleic acid always complementary to each other. DNA cryptography is the science of providing security to the data stored in the form of DNA sequence.

Table 1: DNA Sequence rule

Alphabets	Binary representation
A	00
B	01
G	10
T	11

2. BACKGROUND WORK

In Symmetric key the single key is used at the both encryption and decryption of the cryptography [4]. Symmetric key is provide the security for the possible attacks but it does not work for the brute force attack on secret key, by using the DES algorithm we can solve this problem [5][6]. Quantum Key Distribution is used for providing secure transmission. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt the plain text [7]. A unique property of Quantum Cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key [8]. This quantum cryptography enables the transfer of data through quits which have the special property that they change their states if they are copied [8][9]. In simulation, quantum key exchange and authentication followed by DNA based encryption algorithm for secure message exchange was implemented. Various protocols that implement quantum key distribution are BB84, B92, Ekert protocols [10].

Generally, the BB84 protocol coding scheme uses four non-orthogonal polarization states where as B92 protocol uses only two orthogonal states that will polarize each of the photon which will be transmitted. In this protocol, sender and receiver have to communicate within two channels, Quantum channel and public channel to share a secret key. Ekert protocol is a 3-state protocol that uses three non-orthogonal polarization states that will polarize each of the photon. In [11] DNA-based Cryptography DNA sequences are used for secure communication and key distribution, and the chemical information of biological alphabets are used for steganography – Information Hiding. Pseudo DNA cryptography is used to overcome the limits of using the DNA cryptography [12]. DNA computing methods are implemented based on DNA-based signature scheme [13], a protocol for playing mental poker on the wetware, and an RNA-based zero-knowledge proof system based on solving the Sudoku problem.

Providing primitives of classical cryptography since it provides a variety of advantages over conventional silicon-based computing paradigms. PCR-based amplification technology of DNA, in order to solve the key space-constrained problem that the PCR amplification technology of DNA has, the authors used a method for building a chaotic system [13, 14]. This system includes a logistic chaotic map and a Henon chaotic map. Generate a chaotic pseudo-random sequence which could handle the plaintext for eliminating the statistical rules in it with the two maps. Improving security and the key space, and it provides an operational test of it. It is defined a one-time pad cryptosystem using DNA self-assembly and showed that self-assembly is more efficient than PCR for generating the DNA sequences needed by our system [14].

3. PROPOSED WORK

In the proposed system, input data can be taken in any form (audio, video, image or a text file). Data is encrypted using DNA based encryption method. The process of encryption and decryption is processed through binary conversion, Quantum key Distribution Technique and DNA based encryption ad decryption. The entire process of key generation, encryption and decryption is presented in the following figure 2.

A. Binary Conversion

Every data has some ASCII value and it is unique. In binary conversion process, ASCII value of the input data is converted into 7 bit binary data. Converted binary value is used as the plaintext in the encryption and decryption algorithm.

B. Quantum key Distribution Technique

For every data bit of the plain text key is computed using BB84 protocol. In BB84 protocol, only four directions are used for generating the key. Key is now is translated into the DNA sequence based on the plain text. Each binary bit of plain text has four DNA Sequence letter and is mapped to a key. For every data bit of the plain text key is computed.

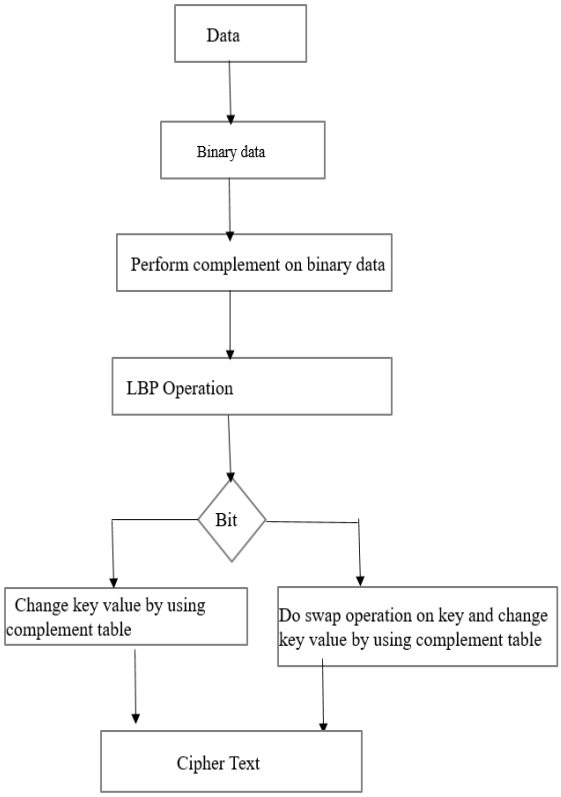


Figure 2: Proposed Encryption process

C. DNA based Technique

In DNA Technique, Getting the key which is generated by the Quantum key Distribution. This key is translated as a DNA Sequence by using the DNA sequence table2 and Perform the Encryption operation by using Key on the Binary bit and Complement of the DNA Sequence using complement rules as given in table 3.

Table 2: BB84 Protocol

Direction	→	↑	↖	↗
Symbols	H	V	L	R
Bits	0	1	0	1

D. Encryption

The third step of the proposed technique is the encryption of the data. In this proposed technique, the actual data is never send through the unsecured or open channel. Here send the DNA Sequence key which is generated by the quantum key distribution after performing the complement operation based on the binary bit.

1. Take the plain text which is the result of Binary Conversion
2. Perform the Complement operation
3. Perform the LBP operation on the complemented bits
4. Perform Encryption on the individual bit by using the Quantum key and DNA Complement table
   if bit is 0
   change the key value by using the Complement table
   else bit is 1
   do the Swap operation on the Key and then perform the complement Using DNA Complement table.

Table 3: DNA Complement Rules

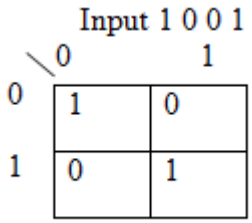
S. No	DNA Sequence	Complement
1	AA	AC
2	AT	TA
3	AG	GT
4	AC	CG
5	TA	TC
6	TT	AT
7	TG	CA
8	TC	GA
9	GA	GT
10	GT	CC
11	GG	AA
12	GC	TG
13	CA	CT
14	CT	GC
15	CG	TT
16	CC	AG

E. Decryption

1. Take the cipher text
2. Do the reverse complement operation by using the DNA Complement rule
   if
   result is equal to the key then the bit is or plain text is 0
   else
   perform the swap operation on the key then the key is equal to result then the plain text is 1.

Example:

1. Binary bits or plain text is 0 1 1 0
2. Complement of the bits are 1 0 0 1
3. LBP operation:



Here the bits are arranged in the row format but retrieve in the diagonal format that is result is index of matrix: 00, 11, 01,10. So the output of the bits are 1 1 0 0.

4. Generate the Quantum Key in the following way:

i. Take the Alice and Bob patterns as s1 and s2 strings. Alice string
Generate the actual key of Alice and Bob patterns by using BB84 protocol.

key1=01101010110100101111001101100011
key2=01001011011100101011000001000000

ii. Compare the key1 and key2 bits for generating key3. If key1 bit equal to key2 bit then key3 value is 1. Otherwise 0. Based on the BB84 Protocol

key3=11011110 01011111 10111100 11011100

iii. Convert this bits to the DNA Sequence using DNA Sequence table.

1101	1110	0101	1111	1011	1100	1101	1100
TC	TG	CC	TT	GT	TA	TC	TA

DNA Sequence key for plain text bit after performing the LBP

Bit	Key
1	TCTG
1	CCTT
1	GTTA
2	TCTA

iv. Perform the encryption by using DNA Complement on the DNA Sequence key Based on the binary bit.

Table 4: Example

S. No	Binary bit	Key	Encryption	Decryption	Binary bit
1	1	TCTG	CAGA	TCTG	1
2	0	CCTT	AGAT	CCTT	0
3	0	GTTA	CCTC	GTTA	0
4	1	TCTA	TCGA	TCTA	1

4. CONCLUSION

In the proposed method, the information can be transmitted securely through the open medium. Instead of transmitting the actual key information through the medium, the complement of key is sent. Receiver will recover the plaintext bits 0 or 1 based on the received patterns. Key is chosen / generated by quantum key distribution method and translates it in to DNA sequence by using sequence rule. Each plain text bit has four DNA sequence key. The encryption process involved with many levels of processing will increase the security. In the first level, complement is performed on the bits, at the second level LBP operation is performed on the bits and at the third level 16 complementary rules are performed. So, this method is more secured and it require very less computations compared to other existing methods.

REFERENCES

[1] Gilles Brassard “Brief History of Quantum Cryptography: A Personal Perspective” in the Proceedings of the IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Awaji Island, Japan, 17 October 2005.
[2] Richard J. Hughes, George L. Morgan and C. Glen Peterson “Practical quantum key distribution over a 48-km optical fiber network” Physics Division Los Alamos National Laboratory, Los Alamos, NM 87545, LA-UR-99-1593.
[3] N.Srilatha G.Murali “Fast Three Level DNA Cryptographic Technique to Provide Better Security” 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) 978 -1-5090-2399-8/16/$31.00 ©2016 IEEE Pno:428-432.
[4] E Suresh Babu, C Nagaraju, MHM Krishna Prasad “Analysis of SecureRouting Protocol for Wireless Adhoc Networks Using Efficient DNA Based Cryptographic Mechanism” published in Procedia Computer Science dec-. Vol-70Pno:341-347 , 2015.
[5] Lelde Lace, Oksana Scegulnaja-Dubrovska, RamunsUsovs, AgneseZalcmane, “Quantum Cryptographic Key Distribution Protocols”, the European Social Fund (ESF), 2008.
[6] R Pradeep Kumar Reddy, C Nagaraju, N Subramanyam ”Text encryption through level based privacy using dna steganography” published in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 2014,vol:3 issue:3
[7] Lin, H.S., Cryptography and Public Policy, Journal of Government Information, PP135–148 . April1998.
[8] Alia, M.A., Yahya,A., Public–Key Steganography Based on Matching Method, European Journal of Scientific Research PP223-231 Aug (2010).
[9] G. Cui, L. Qin, Y. Wang and X. Zhang, “An encryption scheme using DNA technology”, Bio Inspired Computing: Theories and Applications, pp. 37-42, 2008.
[10] Z. Chen and J. Xu, "One-time-pads encryption in the tile assembly model," Bio-Inspired Computing: Theories andApplications, 2008, pp.23-30.
[11] Z. Chen and J. Xu, "One-time-pads encryption in the tile assembly model," Bio-Inspired Computing: Theories andApplications, 2008, pp.23-30.
[12] Biological Alphabets and DNA-based Cryptography Qinghai Gao Department of Security Systems, Farmingdale State College, SUNY
[13] Implementing Modern Cryptographic Protocols Using DNA and RNA Information Processing ArashKarimi Iran University of Science and Technology (IUST), Narmak, Tehran, Iran, VOL.11 No.11, November 2011.
[14] auday h. saeed al-wattar, ramlan mahmod, zuriatiahmadzukarnain & nurizuraudzir university putramalaysia, faculty of computer science & information technolgy, selangor-serdang, Malaysia