ARUNAI PUBLICATIONS

Asian Journal of Applied Research

DOI: http://dx.doi.org/10.20468/ajar.2018.02.02

Research Article

DNA Based Cryptography Using Encryption Scheme for Data Security

P. V. Kumaraguru, V. J. Chakravarthy

Department of MCA, Guru Nanak College, Velachery, Chennai, Tamil Nadu, India

Address for correspondence:
V. J. Chakravarthy,
Department of MCA, Guru Nanak College, Chennai,
Tamil Nadu, India.
E-mail: chakku_vjc@yahoo.co.in

ABSTRACT

The important issues in the analysis of cryptography are security. These are considered the evolvement of cryptography in the fields of upcoming research. Cryptography is concerned with converting a plain text into cipher text which is storing and transmitting data in a particular form so that only those who are intended can read and process it. DNA cryptography plays a key role is closely related to field of biotechnology. In terms of DNA cryptography are not traditional cryptography which is completely repulse and to construct the possible hybrid model of cryptography. Using the concept of DNA cryptography, traditional based cryptographic systems are now vulnerable to attacks the possible technology that takes advancing a new hope for unbreakable algorithms. This paper present encryption scheme using polymerase chain reaction (PCR) technology is termed as PCR and is the most prominent cryptographic technique used in DNA cryptography that utilizes a biological method for encryption and decryption process.

Keywords: DNA Cryptography, Encryption, Decryption and data security

Received: 02nd December 2017
Accepted: 20th December 2017
Published: 05th February 2018

INTRODUCTION

The new field of technology is DNA cryptography for encoding any sort of message. In recent days, scientists are concentrating on various DNA technologies. Based on the DNA technology there are two approaches to realize, i.e., conventional cryptography and DNA computing. DNA computing uses molecular biology which consists of DNA hybridization, DNA fragmentation and micro biology. DNA computation is mainly used to solve the problem of Hamiltonian path.[1] In DNA cryptography, DNA base pairs are used as the information carrier. Big processing power of DNA chips makes it more advanced technique as compared to other techniques which are being used. Therefore, DNA chips carry forward to the present silicon chips which are new hope for overriding in future which may improve personal computer (PC) information handling in a tremendous manner. There are many cryptographic algorithms such as RSA and DES which are already destroyed by many attackers; hence, to require more and secure techniques of cryptography have emerged. The issues of cryptography based on DNA computing algorithm have been already proposed. Many of the algorithms have been designed by the use of symmetric and asymmetric keys which are based on DNA cryptography for hiding the data . The benefit of DNA cryptography is low power utilization for computing, storage capacity of DNA is excellent, and the processing time is high with extraordinary performance. DNA cryptographic strategies by considering traits including security which is provided by the method, to process for time taken the technique, the capacity of storage medium which is utilized to store the information in the system, the capacity limit of the storage medium utilized and the outcomes of the stability for the specific procedure.

Security based traditional cryptography is relies on only computational difficulties that can be referred to be one fold. The efficient cryptographic algorithm is time taken by few seconds that involve DNA chip and polymerase chain reaction (PCR) technology based DNA cryptographic techniques can take time to complete the whole process. Conventional cryptography keeps running on PCs over the system, so the capacity mediums are silicon chips of the PCs, though DNA cryptography manages the DNA strands which are controlled by biological methods. If DNA is considered as the storage medium compared to the equal measure of silicon chips, as it has got the high capacity of storage. This property of information makes DNA computing and DNA cryptography extremely enticing and beneficial field of research. In this paper proposes PCR technology and DNA digital coding which is designed using the DNA synthesis of technologies based on encryption scheme. To get the entirely different ciphertext from the same plaintext by means of preprocesses operation, which can adequately keep attacker from a conceivable word as PCR primers.

LITERATURE REVIEW

DNA cryptographic techniques are developed widely in many advanced encryption data security nowadays to use DNA sequence as an information carrier. Here, in this process, the plaintext is encrypted to DNA digital coding.[2,3] The exploration of DNA cryptography is still at the underlying stage, and there are numerous issues to be illuminated. The new conceived DNA cryptography[4,5] which is far from develop both in realization and theory and this may be the motivation behind why just few examples of DNA cryptography were proposed. The current DNA cryptography focuses the period of laboratory exploration is still in experiments, while there is not general hypothesis about applying DNA atoms in cryptography.[6,7] In DNA research, some of the key technologies are PCR, digital coding of DNA, and DNA synthesis that only have been developed and accepted well in recent years.[8] PCR is quick DNA enhancement technology based on the complementary of Watson-crick. To amplify the encoded message sequence, it would even now be extremely hard without knowing the correct pairs of two primers. The modern biological techniques as tools are used to implement DNA cryptography and the main security premise as biological hard problems to completely apply the exceptional point of interest. As explained above by applying the special function of two primer pairs which could be used as the correct key to PCR amplification. Then again, the security-based traditional cryptography is depends on the tough mathematical problems, which develop both in realization and theory. There are numerous powerful cryptosystems of traditional cryptography, for example, RSA, DES, and AES were invented. In this manner, DNA cryptography does not completely repulse the traditional cryptography, and it is conceivable to develop the hybrid cryptography of them.

Primers are used as a key to encrypt and decrypt data which will result in a DNA template. The technology used in this scheme is PCR which is a DNA digital coding technique.[9] Data are first transformed into its equivalent hexadecimal code and then into its binary code. These binary digits are then converted into DNA sequence which is used as the DNA pattern. The forward primer[10] is used to perform the PCR. Now that the DNA sequence has been changed, it will be completely dissimilar from the original data. To decrypt the encoded data, reverse primer is used to convert the PCR DNA sequence to the original data. This is then converted into its equivalent binary which is then altered to the original information. This technique has both technical and mathematical difficulties which will prevent an adversary to identify the original information.

METHODOLOGY OF DNA CRYPTOGRAPHY UTILIZES BIOLOGICAL METHODS

PCR technology

PCR is known as PCR which it is based on the rapid amplification of DNA on PCR technology. Because the manipulation of DNA on a small amount of PCR technology is very difficult and typically used to amplifying the DNA which has been determined. In practice, cloning is the techniques of DNA amplification. The efficiency of PCR amplification is extremely high and can increase a large number of selected DNA in a small time period. Moreover, PCR will achieve the amplification using natural nucleotide molecules. To attain the amplification of PCR technology, the experimenter required to know the sequence of the chosen DNA chain, and use it to design primers for amplification. The PCR process can be categories into two stages.

- At the beginning and end, of the two primers which are distinctly loaded onto the target DNA.
- Under the action of the polymerase to the finding of the target DNA and its amplification.

DNA encoding scheme

In the field of information science, the most basic encoding method is binary encoding. This is because everything can be encoded by the two states of 0 and 1. Table 1 shows the DNA has categories into 4 units[11]:

Table 2 shows the easiest way to encode is to represent these four units as four figures [11]:

Obviously, by these encoding rules, there are 4! = 24 possible encoding methods.

DNA encoding, it is necessary to reflect the biological characteristics and pairing principles of the four nucleotides. Based on this principle, we know that:

A(0) – 00 and G(3) – 11 make pairs,

T(1) – 01 and C(2) – 10 make pairs.

A total of 24 possible encoding programs , from there only 8 programs.

0123 – CTAG, 0123 – CATG, 0123 – GTAC, 0123 – GATC, 0123 –TCGA, 0123 – TGCA, 0123 – ACGT.

0123 – AGCT matched pair of DNA is the basis of complementary principle. 0123 – CTAG is finest encoding scheme. This coding scheme should be reliable with the weight of the molecular chain.

Encryption and decryption process

If the encrypted wants to encrypt the plaintext, first needs to transform the plaintext using the code rules. Next get the sequence of DNA which is represented as the special meaning of the base sequence according to DNA and then uses the biotechnology artificially synthesize the DNA chain as the target DNA. After this, design the appropriate primers as the key. When the sender has the key, loads them onto the target DNA for its strand and end according to the sequence synthesis primers of the primer. On this basis, we use DNA technology to cut and splice, and implant this DNA into a long DNA chain. Finally, adds an interfered DNA chain, explicitly the common DNA chain. The arrangement of these chains does not comprise any significant information. To decrypt the encoded data, reverse primer is used to convert the PCR DNA sequence to the original data. This is then converted into its equivalent binary which is then altered to the original information. This technique has both technical and mathematical difficulties which will prevent an adversary to identify the original information.

Table 1: Categories of DNA

Nucleotide	Strands
A	Adenine
T	Thymine
C	Cytosine
G	Guanine

Table 2: Nucleotide bases

Nucleotide used	Binary Sequence
A (0)	00
T (1)	01
C (2)	10
G (3)	11

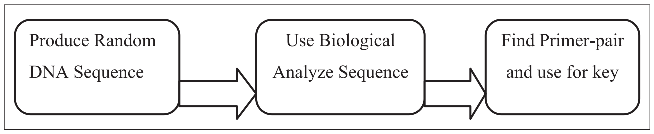
Produce Random DNA Sequence
Use Biological Analyze Sequence
Find Primer-pair and use for key

Figure 1: Key preparation processes

DESIGN OF CRYPTOGRAPHIC ALGORITHMS ON PCR-BASED AMPLIFICATION TECHNOLOGY OF DNA

Key generation

In this encryption system, we use the united keys instead of a single key. Figure 1 show the Key preparation processes [11]. The key is divided into two parts: The first part is a PCR technique used in the primers, with the primer sequences as a key - Key A. The second part concerns the initial conditions and parameters which are used in the chaotic system, and the system is called Key B. The password system is the most important which relies on bio-security. As such, the DNA code of the key has the requirement of high quality. However, in the united key, key Key Bis-related with the DNA code. For the generation of Key A, Key A is a string of bases of the DNA sequence, which is used for the PCR amplification primers. Password security and systems can be realized, which is determined by the success of the primer design system. Accordingly, the design of this key is very important. If the key is designed strictly according to the design principles of the design primer, it will cause limited limitation of primer shortage space. Therefore, the primer design of the encryption system is designed by software Premier 5.0, which is used in the biological simulation.

Encryption process

The message sender is also called the encrypter: After implementation of the key design, it starts to encrypt the plaintext and creates a ciphertext. Figure 2 shows the encryption process [11].

- The process which is converted into binary code.
- Then, the binary code is used for the DNA encoding rule for chaos.
- Transporting Key B into a chaotic system which is used to produce the chaotic Pseudo-random number sequence.
- Sequences of operating and plaintext which are equivalent to binary using XOR so as attain the processed binary data sequence.

This binary sequence is divided into n sub-sequences, and the specific number is decided by the length of the ciphertext. The pair sequence is numbered l_1, l_2,… ln and is followed by the following operations:

$l_1 \oplus l_2 = s_2,$

$s_2 \oplus l_3 = s_3$

…

$s_{n-1} \oplus l_n = s_n$

Get s_2, s_3,…,s_n n-1 orders and then l_1, s_2, s_3,…, s_n, and its subscript number of these

sequences. The sequences were added to each sequence at the beginning.

Next, the sequence was converted into a DNA base sequence allowing for DNA coding. The coding rules are 0123 - CTAG. Afterward, select the stand-n-primer from that attained in the preceding primer sequence step that added to the front of the sequence. The ciphertext arrangement circulated successfully.

Decryption process

First, the cracker has to get Key A using key information that is obtained from safe prior sources and then carry out PCR amplification. For the second step, the DNA to be amplified will be selected using electrophorus, and these DNA have the information we need. For the third step, through the sequencing of the DNA chain, we can draw the corresponding DNA sequence. For the fourth step, the DNA sequence was restored to a binary sequence by the DNA encoding. At this time, the obtained binary sequence is l_1, s_2, s_3, …, s_n in the encrypted process. After sorting it is then calculated:

$s_{n-1} \oplus s_n = l_n$ ……

$s_2 \oplus s_3 = l_3$

$l_1 \oplus s_2 = l_2$

We can get l_1, l_2…l_n. For the fifth step, the binary sequences are spliced together, and we can get a sequence that is a clear binary sequence after the sequence of the pre-treated. For the sixth step - the building of the chaotic system - we bring the parameters of Key B into the chaotic system. Figure 3 shows the Decryption process [11].

After these operations, we can obtain a binary sequence corresponding to the plaintext. For the seventh step, through transcending and the restoration of the character data, we can get clear. Now, the information transmission process is over. When the sender sends a successful message, the receiver will get safe information, and they will get plaintext.

CONCLUSION

This paper analyzing the encryption algorithm for the amplification of PCR based DNA technologies is improving

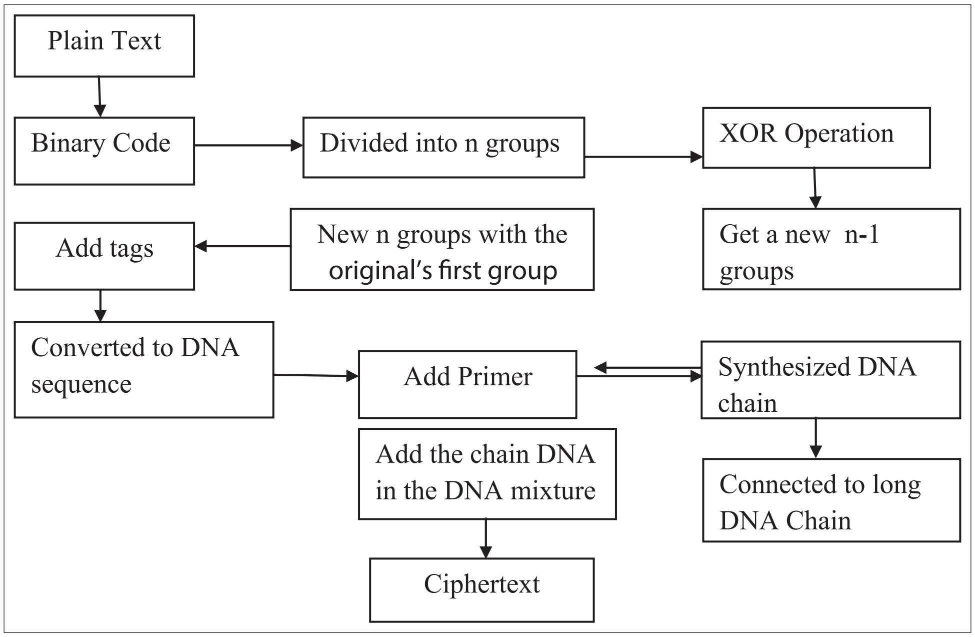
Plain Text
Binary Code
Divided into n groups
XOR Operation
Get a new n-1 groups
New n groups with the original's first group
Add tags
Converted to DNA sequence
Add Primer
Synthesized DNA chain
Add the chain DNA in the DNA mixture
Connected to long DNA Chain
Ciphertext

Figure 2: Encryption process

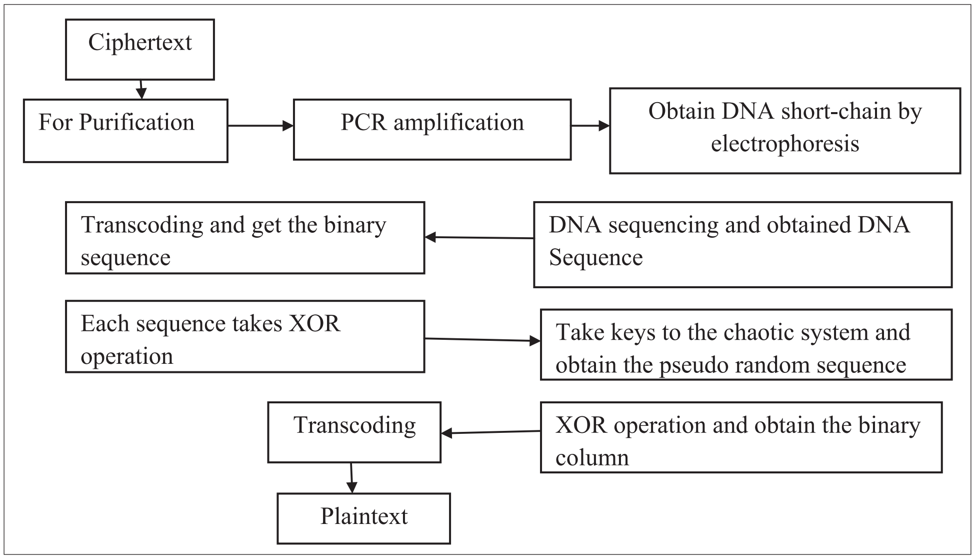
Ciphertext
For Purification
PCR amplification
Obtain DNA short-chain by electrophoresis
Transcoding and get the binary sequence
DNA sequencing and obtained DNA Sequence
Each sequence takes XOR operation
Take keys to the chaotic system and obtain the pseudo random sequence
Transcoding
XOR operation and obtain the binary column
Plaintext

Figure 3: Decryption process

the security. This is mainly used for increasing the security of encryption scheme using DNA cryptography. On the other hand, DNA digital coding and traditional encryption process are used to preprocess the data to be plaintext. Through this preprocess operation we can get entirely dissimilar ciphertext from the similar plaintext, which can successfully prevent an attack from a possible word as PCR primers. The complexity of biological difficult problems and cryptography computing problems offer a double security safeguards for the scheme. However, it has some particular advantages and meets cryptography principles. Most importantly, DNA cryptography specifies that biological molecules can be used for cryptographic purposes and have irreplaceable properties.

REFERENCES

1. Ad Leman LM. Molecular computation of solution to combinatorial problems. Science 1994;266:1021-4.
2. Javheri S, Kulkarni R. Secure data communication and cryptography based on DNA based message encoding. Int J Comput Appl 2014;98:35-40.
3. Kaundal AK, Verma AK. DNA based cryptography: A review. Int J Inf Comput Technol 2014;4:693-8.
4. Cui GZ, Qin LM, Wang YF, Zhang XC. Information Security Technology based on DNA Computing. 2007 IEEE International Workshop on Anti-Counterfeiting Security, Identifying; 2007. p. 288-91.
5. Leier A, Richter C, Banzhaf W. Cryptography with DNA binary strands. Biosystems 2000;57:13-22.
6. Lu MX. Symmetric-Key crptosystem with DNA technology. Sci

China Ser F Inf Sci 2007;3:324-33.

7. Gehani A, Labean TH, Reif JH. DNA-based cryptography, DNA based computers V. Provid Am Math Soc 2000;54:233-49.
8. Kazuo T, Akimitsu O, Isao S. Public-key system using DNA as a one way fuction for key distribution. Biosystems 2005;81:25-9.
9. Cui G, Wang Y, Zhang X. An Encryption Scheme Using DNA Technology; 2008.
10. Clelland T. Hiding messages in DNA Microdots. Nat Magaz 1999;399:533-4.

Cite this article: Chakravarthy VJ. DNA Based Cryptography using Encryption Scheme for Data Security. Asian J Appl Res 2018;4(3):16-20.

Source of Support: Nil, **Conflict of Interest:** None declared.