STM JOURNALS

International Journal of
Bioinformatics and Computational Biology

ISSN: 2583-9977
Volume 3, Issue 2, 2025
July—December
DOI (Journal): 10.37591/IJBCB

https://journals.stmjournals.com/ijbcb

Review IJBCB

Analytical Study on DNA-Based Modern Cryptographic Techniques

Nupoor Singh[1,*], Amit Singhal[2]

Abstract

In the modern digital era, the exponential growth in information generation, storage, and transmission has made information security a critical concern. As data flows through various networks and platforms, ensuring its confidentiality, integrity, and availability has become essential. Traditional cryptographic techniques have been the long backbone of data protection. These include substitution and transposition ciphers, hashing functions, and encryption algorithms, such as Data Encryption Standard (DES), Rivest–Shamir–Adleman (RSA), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and Elliptic Curve Cryptography (ECC). These methods have provided robust security frameworks for decades. However, with the increasing sophistication of cyber threats and advancements in computing technologies, novel approaches, like DNA cryptography, are gaining attention. DNA cryptography leverages the biological characteristics and computational capabilities of deoxyribonucleic acid (DNA) molecules to encode and secure information. Its inherent parallelism, high storage capacity, and randomness offer promising potential for data security applications. Extensive research has been conducted in this domain, exploring how DNA-based systems can complement or enhance traditional cryptographic models. This paper presents a comprehensive review and comparison of these cryptographic techniques, both conventional and emerging, to evaluate their effectiveness in securing digital information against unauthorized access and cyberattacks in the ever-evolving digital landscape.

Keywords: DNA structure, DNA cryptography, DNA techniques, comparison, utilization, deoxyribonucleic acid

INTRODUCTION

Data security and cryptography play a vital role in traditional computing and are likely to be significant for DNA database applications as well. This section introduces fundamental terminology commonly found in various cryptographic methods. The main objective is to securely transmit information from a sender to a receiver in such a way that any third party intercepting the message cannot comprehend its contents [1].

In a cryptographic framework, plaintext refers to a string of characters selected from a limited set of symbols, often forming natural language. Encryption involves converting this plaintext into an unreadable format known as ciphertext by applying a specific algorithm and a confidential key. Decryption is the inverse operation, where the ciphertext is converted back into its original form using the appropriate key [2–4].

Encryption aims to ensure that anyone lacking the secret key cannot decode the message. A

***Author for Correspondence**
Nupoor Singh
E-mail: singh.ghungru@gmail.com

[1]Research Scholar, Department of Computer Science & Applications, Monad University, Hapur, Uttar Pradesh, India
[2]Professor, Department of Computer Science & Applications, Monad University, Hapur, Uttar Pradesh, India

Received Date: November 20, 2024
Accepted Date: April 21, 2025
Published Date: April 28, 2025

Citation: Nupoor Singh, Amit Singhal. Analytical Study on DNA-Based Modern Cryptographic Techniques. International Journal of Bioinformatics and Computational Biology. 2025; 3(2): 7–14p.

cryptosystem is considered unbreakable if no method of cryptanalysis can successfully decode it. One such system is the one-time pad cipher, named because both the sender and receiver have identical pads filled with random data. Each data segment is used a single time to encrypt and decrypt a message and is then discarded permanently. The rest of the paper contains section II, which gives the knowledge of the background of DNA cryptography. Section III introduces various related algorithms or techniques related to DNA cryptosystems. Section IV describes the comparison criteria between various techniques. Section VI describes the conclusion based on the observation of results obtained in the last section.

BACKGROUND

Modern cryptography consists of the interaction between the application of mathematics, computer science and engineering. There are many desktop and web applications which use cryptography. Here the discussion starts with the basics of cryptography to the current techniques.

Cryptography

Cryptography is a way of achieving security by converting or modifying the plaintext message into the ciphertext message, i.e., no one can understand the actual meaning of the original message. In the modern information era, the evolution of e-money and online transactions is on a large scale, which requires more secure and new cryptography techniques. Because the cryptanalysis, which means to analyze and try to break the system proposed by the cryptography techniques, runs parallel with the evolution of the cryptography techniques [2].

Cryptographic Branches

There are some branches of the cryptography which are

a. Cryptographic Engineering [5].
b. Multivariate Cryptography [6].
c. Quantum Cryptography [7].
d. Steganography [8].
e. Visual Cryptography [9].
f. DNA Cryptography [10].

Cryptographic engineering is mainly used for providing confidentiality authenticity to the devices from unauthorized access and provides data integrity from the attacks [11].

Crypto Engineering = Efficient Implementation + Secure Implementation

Multivariate cryptography is also known as asymmetric cryptography. It is based on multivariate polynomial functions over finite fields [12]. Quantum cryptography is mainly used in key distribution mechanisms. It is founded on the Heisenberg uncertainty principle from the field of physics [13].

Steganography is the process of hiding messages such that only intending recipient know about the existence of message [14]. Visual cryptography is the technique in which visual information is encrypted in such a way that the decryption becomes mechanical operation with the help of human, and which does not require any decryption algorithm [15]. The next section describes the DNA cryptography in detail.

DNA CRYPTOGRAPHY

DNA

In the human body, nucleic acids play a crucial role in transferring genetic information between different parts. There are two main types of nucleic acids: DNA and RNA, which carry the instructions required for cells to carry out various functions. DNA is the molecule responsible for storing an organism's genetic code. It determines genetic traits and influences physical appearance and characteristics in both humans and animals [16]. The DNA has a complex structure shaped, like a

twisted ladder with four types of acids, like A (adenine), G (guanine), T (thymine), and C (cytosine), which are used to store and transform information [9]. A strand consists of a series of bases arranged sequences.

The double helix structure is created through hydrogen bonding, where T pairs with C and G pairs with A [17, 18], as illustrated in Figure 1.

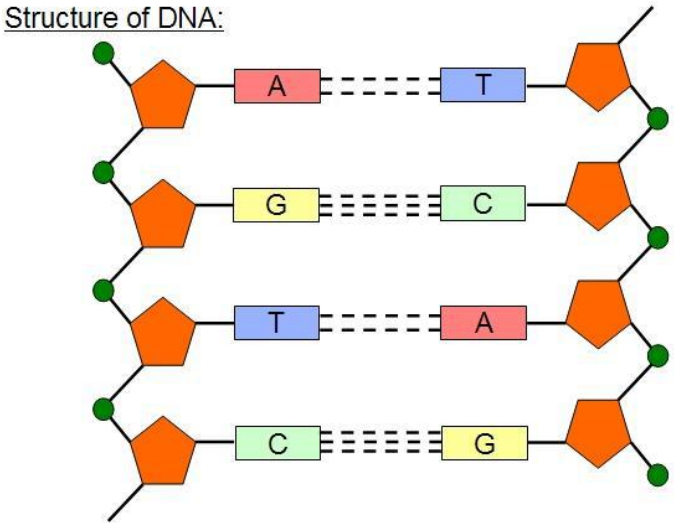

Figure 1. Structure of DNA.

DNA Computing

DNA computing, also known as molecular computing, is a new approach to massively parallel computing. This computing paradigm computes problems using DNA sequence. It is used to resolve the varieties of problems in fractions of a second. It is a type of computing that relies on DNA biochemistry and molecular biology rather than conventional silicon-based computer technology [18].

This computing has brighter potential in all fields, such as steganography, authentication, image encryption, data encryption, visual encryption, one-time pad, etc. [19]. DNA strands store a large amount of data and complex information in the molecules or group of molecules, where 1 gm of DNA can store 10^8 terabytes of data. It is also used to search for possible solutions to the problem simultaneously, which is represented by DNA strands [20]. It is also used for secure communication over the medium without any attack threat, it provides key strength data confidentiality, key strength, key strength, non-repudiation, data integrity [21].

DNA computing is a rapidly evolving field that bridges multiple disciplines. Its research and development are concerned with theory, practical experiments and applications.

DNA Cryptography

DNA cryptography offers enhanced data security by converting plain text messages into DNA strands using specific DNA sequences. This cryptographic method was first introduced in 1994 by Dr. Leonard M. Adleman from the University of Southern California, who applied it to solve a complex mathematical problem. He demonstrated the powerful computational capabilities of DNA by successfully solving the NP-complete Hamiltonian Path Problem involving seven vertices [22]. This technique provides dual-layer security through complex computations. It relies on biomolecular methods for both encryption and decryption, leveraging the intricate structure of biomolecules, which are challenging to decode. DNA, consisting of four nucleotides – A, G, T, and C – is encoded during encryption by representing each nucleotide as a binary value: 00, 01, 10, and 11, respectively. These binary representations can then be manipulated or transformed into various binary sequences [23, 24]. DNA cryptography is a temperature-dependent cryptographic method [25] as shown in Figure 2.

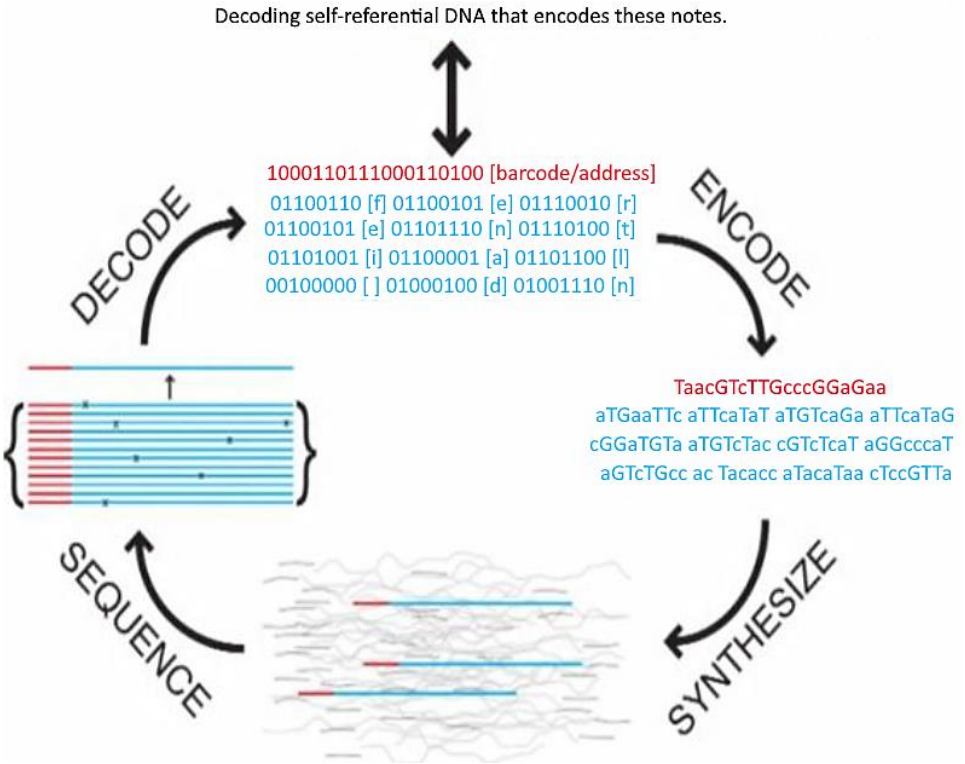

Figure 2. DNA encryption and decryption mechanism.

DNA Techniques

There are various DNA cryptography techniques which have been developed; here some of the DNA techniques which are widely used and recently developed are shown:

DNA Digital Coding Polymers' Chain Reaction PCR

PCR stands for "Polymerize chain reaction". It is highly efficient amplification and quantification process of DNA [26]. DNA amplification is very difficult, to amplify the DNA strands, so PCR method is used. This method was invented by analysis of biological catalysts known as polymerase.

These polymerases are present in a chaining fashion, which represents that the amplification process occurs in various cycles in a chain, one by one, in a cascading manner. By applying PCR, small DNA sequences can be dissolved into samples containing very minute quantities of DNA.

PCR amplification can be used for DNA cloning and clustering, i.e., it has the nature of duplicating the DNA [27]. In summary, the PCR process can be divided into two main phases.

i. In the first phase, the two DNA chromosomes, are merged into target DNA.
ii. In the second phase the polymerase amplification process is applied for forming the target DNA.

PCR amplification is a highly sensitive technique that can be influenced by temperature fluctuations.

DNA Based Bimolecular Cryptographic Design

A bimolecular cryptographic system scrambles the data into DNA code by using oligonucleotide sequences [28]. It uses the one-time pad (OTP) technique of cryptography, which is based on the principle of unbreakable [29]. The actual experiment of cryptographic schemes follows OTP, which has limitations in transmission over conventional electronic media because of the size of the OTP. DNA strands are very neat in design as storage media, and a small amount of DNA is enough for a large amount of OTP [30].

We use one-time pad encryption, which uses a codebook to scramble the part of a small segment of plaintext message to cipher text message. The codebook used here is a random code book, i.e., One secret code is used only once for encryption and decryption, not repeatedly. The OTP of the plaintext message is distributed to both sender and receiver in advance [31]. DNA based bimolecular cryptographic encryption has the following schemes:

1. *Substitution:* In the substitution method, the pair mapping is performed between the libraries of various pads, which are randomly generated. In this method, encryption is both random and reversible, transforming plaintext into cipher strands while eliminating the original plaintext strands. Later, the DNA substitution uses long DNA pads that contain various parts, and each part has a cipher word followed by a plain text word. Here the cipher word is attached to the plaintext word to form word-pairs. It also acts as a hybridization site for the binding of primer. Word pairs generated for DNA strands serve as a reference table for converting plaintext into ciphertext during the scrambling process.
2. *XOR mapping:* This XOR mapping uses molecular computation and index random key strings. Information technology maps DNA strands in a random, reversible manner, where the original data is transformed into encrypted strands, and the original plaintext strands are eliminated.

Symmetric Key Crypto System Using DNA

The symmetric system uses the same key for the encryption and decryption process [22]. These are extremely fast and widely used for processing huge amounts of data. It is having some threat of attack while transmitting over the communication media, for example, man in the middle.

These are accessible by the external. In this method the plain text is converted DNA sequence in which DNA strands are used as the unique key for encryption and decryption [12].

Asymmetric Key Crypto System Using DNA

The Asymmetric system uses two different keys for the encryption and decryption process [22]. We can also be called DNA-public key cryptography. These are extremely fast and widely used for process amounts of data because it is much more secure as compared to the symmetric key encryption process.

External users may find it difficult to access. In this method the plain text is converted DNA sequence in which DNA strands are used as the unique key for encryption and decryption [14].

DNA STEGANOGRAPHY

Steganography is the technique of hiding secret messages apart from the sender and receiver. DNA steganography can be said to be the supplement of classical DNA cryptography. The DNA steganography has a constraint that this method is open to attack [9]. In this process the original message is covered by DNA samples to a microdot size.

In the DNA steganography encryption process, the original message is converted to DNA strands, and those strands are combined with the other DNA strands to generate a dummy DNA strand of equal length and size. However, encryption is not of primary importance in steganography; therefore, a simple substitution cipher can be encoded to characters in DNA triplets.

In the decryption process, the secret key and the dummy DNA strands are amplified by applying the PCR process. The cipher message will be converted into original message only by the intended recipient who knows the PCR primer or key or PCR strand sequence.

PSEUDO DNA CRYPTOGRAPHY METHOD

Pseudo DNA cryptography varies from DNA cryptography. This method depends on the function of DNA, not on the DNA strands. In this method the scrambling and unscrambling process is based on the

flow of genetic information within biological system [15]. The sender converts the mRNA data into proteins based on the genetic code chart. The keys are sent to the receiver on a security channel as shown in Figure 3.

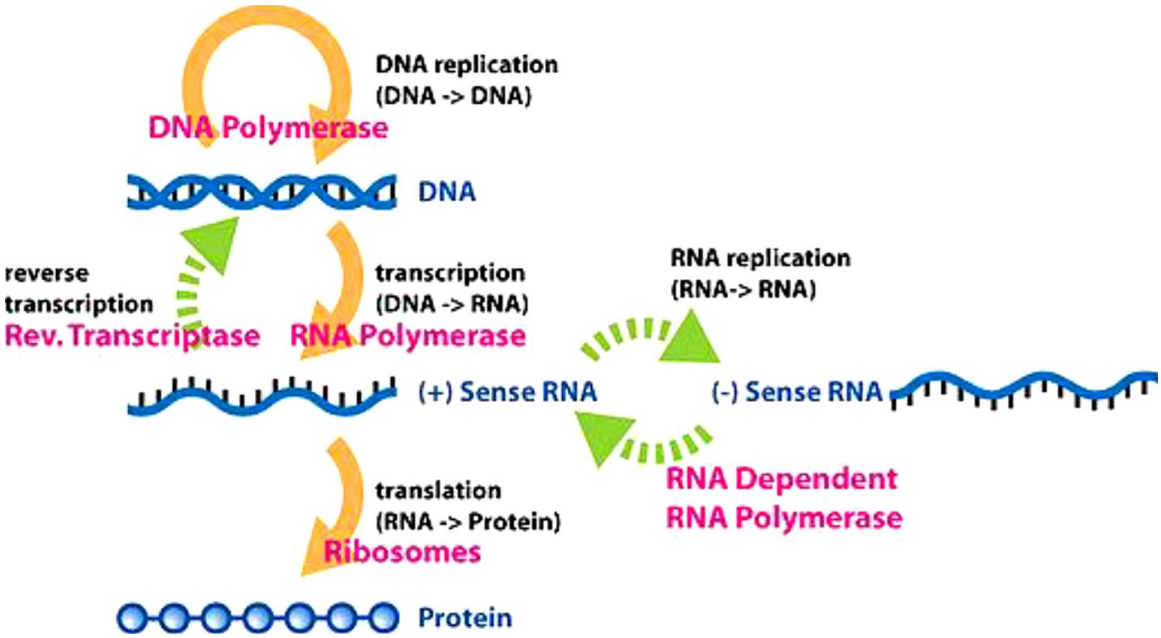

Figure 3. Diagram of flow of genetic information.

DNA Chip Based Technologies

DNA chip technology uses micro arrays of molecules which are restricted over the solid surface for biochemical analysis. DNA Chips are useful in manipulating the large amount of data from genome sequencing and to find parallel expressions of various genes [5].

A DNA chip consists of an array of DNA sequence molecules, known as probes. The encryption and decryption process in DNA chips are not stable as the property of nucleotides changes with the climatic or surrounding conditions [17].

Chaotic Coding

Chaos encoding is the behavioral study of the dynamic systems which are very much dependent on the initial condition. Chaos means the state of disorder. We should follow the following properties.

1. It must be dependent on initial condition.
2. It must be topologically mixed.
3. It must have dense periodic orbits

Cycling chaos is used for encoding image pixels positions and rearranging the pixels grey value by using DNA sequencing masking. When a random process is occurring in a non-liner dynamic system, it is said to be chaos. Chaotic systems are mainly used for dynamic systems [21]. This method is vilely used in image encryption. DNA primers store the encoded image pixels in the form of a matrix.

Image encryption is done by:

$ak + 1 = \mu * ak (1 – ak)$,

where a0 is initial condition, it varies between 0 and 1 μ is the control parameter having value between $0.3 < \mu < 4$ [26].

COMPARISON OF VARIOUS TECHNIQUES

Table 1 here shows the comparison working of different techniques of DNA cryptography. The different parameters, like design, method, coding, technology, and efficiency, are used for the comparison.

Table 1. Comparison between various techniques.

S. N.	DNA Cryptographic Technique	Working
1	DNA Digital Coding Polymers' Chain Reaction PCR	This technique uses POLYMERIZE chain reaction for the amplification for the DNA Strands [25].
2	DNA Based Bimolecular Cryptographic Design	This cryptographic method uses one time pad (OTP) and dynamic code book [9].
3	Symmetric Key Crypto System Using DNA	This technique uses a single DNA strand key for encryption and decryption process. Fabrication and hybridization are done for encryption and decryption process respectively [12].
4	Asymmetric Key Crypto System Using DNA	This method employs a pair of DNA strands as keys – one designated for encryption and the other for the decryption process [14].
5	Pseudo DNA Cryptography Method	This technique is based on the functioning of DNA. It uses mRNA form to generate Cipher text according to genetic code table [15].
6	DNA Chip Based Technologies	It utilizes the genetic sequence of a molecular array. It contains series of blots, which can bind nucleotide by which data is electronically calculated based on binding probe in each blot [20–27].
7	Chaotic coding	This coding uses pseudo-randomness and determination which are two features of chaotic systems. Also, it is dependent on the initial condition [19–26].

CONCLUSIONS

The DNA cryptography is the art of securing data using the DNA sequences. This process uses various techniques as all the techniques mentioned above in the paper. Each method employs distinct algorithms for encrypting and decrypting data. This paper represents detailed study and comparison between the various techniques and algorithms used for DNA cryptography.

REFERENCES

1. Adleman LM. Molecular computation of solutions to combinatorial problems. Science. 1994 Nov 11;266(5187):1021–4. doi:10.1126/science.7973651.
2. Cui GZ, Liu Y, Zhang X. New direction of data storage: DNA molecular storage technology. Comput Eng Appl. 2006;42(26):29–32.
3. Chen J. A DNA-based, biomolecular cryptography design. In: Proceedings of the 2003 IEEE International Symposium on Circuits and Systems (ISCAS); 2003 May 25; Bangkok, Thailand. IEEE; 2003. p. III–III. doi:10.1109/ISCAS.2003.1205473.
4. Cui G, Qin L, Wang Y, Zhang X. An encryption scheme using DNA technology. In: 2008 3rd International Conference on Bio-Inspired Computing: Theories and applications; 2008 Sep 28–30; Wuhan, China. IEEE; 2008. p. 37–42. doi:10.1109/BICTA.2008.4656701.
5. Lu MX, Lai XJ, Xiao GZ, Qin L. Symmetric-key cryptosystem with DNA technology. Sci China Ser F Inf Sci. 2007 Jun;50(3):324–33. doi:10.1007/s11432-007-0025-6.
6. National Center for Biomedical Communications. Handbook on Genetic Cells and DNA. Bethesda (MD): National Library of Medicine, National Institutes of Health, Department of Health and Human Services. 2020.
7. Tanaka K, Okamoto A, Saito I. Public-key system using DNA as a one-way function for key distribution. Biosystems. 2005 Jul 1;81(1):25–9. doi:10.1016/j.biosystems.2005.01.001.
8. Fuscoe JC, Branham WS, Melvin CL, Desai VG, Moland CL, Han T, et al. Technical issues involved in obtaining reliable data from microarray experiments. Regul Res Perspect. 2016;6(1):1–22.

9. Gehani A, LaBean TH, Reif JH. DNA-based cryptography. In: Jonoska N, Păun G, Rozenberg G, editors. Aspects of Molecular Computing. Berlin: Springer-Verlag; 2004. p. 167–88. (Lecture Notes in Computer Science; vol. 2950). doi:10.1007/978-3-540-24635-0_12.
10. Amosa M, Paun G, Rozenberg G. Topics in the theory of DNA computing. Theor Comput Sci. 2002;287:3–38.
11. Xiao GZ, Lu MX, Qin L, Lai XJ. New field of cryptography: DNA cryptography. Chin Sci Bull. 2006 Jun;51(12):1413–20. doi:10.1007/s11434-006-2012-5.
12. Lu M. Symmetric key cryptosystem with DNA technology. Sci China. 2017 Jun;324–223.
13. Chen J. A DNA-based, biomolecular cryptography design. In: Proceedings of the 2003 IEEE International Symposium on Circuits and Systems (ISCAS); 2003 May 25–28; Bangkok, Thailand. IEEE; 2003. p. III-822–5.
14. Lai XJ, Lu MX, Qin L, Han JS, Fang XW. Asymmetric encryption and signature method with DNA technology. Sci China Inf Sci. 2010 Mar;53(3):506–14. doi:10.1007/s11432-010-0063-3.
15. Kang N. A pseudo DNA cryptography method. arXiv. 2009 Mar 16. Available from: https://arxiv.org/abs/0903.2693
16. Borda M, Tornea O. DNA secret writing techniques. In: 8th International Conference on Communications (COMM); 2010 Jun 10–12; Bucharest, Romania. IEEE; 2010. p. 451–6. doi:10.1109/COMM.2010.5515484.
17. Shyam VMM, Kiran N. A novel encryption scheme based on DNA computing. In: 14th IEEE International Conference on Information Technology: Research and Education (ITRE). Tia, India; 2007 Dec 13–15.
18. Gehani A, LaBean T, Reif J. DNA based cryptography. In: Aspects of Molecular Computing. Berlin: Springer-Verlag; 2004.
19. Singh K, Kaur K. Image encryption using chaotic maps and DNA addition: Operation and noise effects on it. Int J Comput Appl. 2011 Jun;23(6):17–24. doi:10.5120/3779-2892.
20. Gabig M, Wegrzyn G. An introduction to DNA chips: Principles, technology, applications and analysis. Acta Biochim Pol. 2001;48(3):615–22. Available from: https://doi.org/10.18388/abp.2001_3896
21. Ricsa VI. DNA-based steganography. Cryptologia. 2001;25(1):37–49.
22. Kahate A. Cryptography and network security. 3rd ed. New Delhi: McGraw-Hill Education; 2013. 501 p. ISBN: 9781259029882.
23. Stallings W. Cryptography and network security: Principles and practice. 3rd ed. Upper saddle river (NJ): Prentice Hall; 2002. 696 p. ISBN: 9780130914293.
24. Elliott C. Quantum cryptography. IEEE Secur Priv. 2004;2(4):57–61. doi:10.1109/MSP.2004.54.
25. Zhang Y, Zhou D, He L, Karanafil YH, Fu B. A new DNA cryptogram scheme based on PCR technology. J Adv Technol Inf Technol. 2012 Nov 15;45:1–6.
26. Soni A, Acharya AK. A novel image encryption approach using an index based chaos and DNA encoding and its performance analysis. Int J Comput Appl. 2012 Jun;47(23):1–6. doi:10.5120/7493-9944.
27. Zhan J, Cabrera L, Osman G, Shah R. Using private matching for securely querying genomic sequences. In: Proceedings of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and IEEE Third International Conference on Social Computing (SocialCom); 2011 Oct 9–11; Boston, MA, USA. IEEE; 2011. p. 1163–8. doi:10.1109/PASSAT/SocialCom.2011.170
28. Jena D, Jena SK. A novel visual cryptography scheme. In: Proceedings of the 2009 International Conference on Advanced Computer Control (ICACC); 2009 Jan 22–24; Singapore. IEEE; 2009. p. 207–11. doi:10.1109/ICACC.2009.109.
29. Gligoroski D, Samardjiska S. The multivariate probabilistic encryption scheme MQQ-ENC. Cryptology e-Print Archive. 2012;2012:328. Available from: https://eprint.iacr.org/2012/328
30. Paar C. Crypto engineering: some history and some case studies. In: Clavier C, Gaj K, editors. Cryptographic Hardware and Embedded Systems – CHES 2009. Berlin: Springer; 2009. p. 220–4. (Lecture Notes in Computer Science; vol. 5747). doi:10.1007/978-3-642-04138-9_13.

31. Watson JD, Crick FHC. A structure for deoxyribose nucleic acid. Nature. 1953;171(4356):737–8.

