International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.6767
***Article Received**: 14 March 2023 **Revised**: 27 April 2023 **Accepted**: 20 May 2023*

Hybrid Encryption of Cloud Processing With IOT Devices Using DNA And RSA Cryptography

Sohit Agarwal[1], Gagan Joshi[2]
[1]Assistant Professor, Department of Computer Engineering & Information Technology
Suresh Gyan Vihar University
Jaipur, India.
[2]Scholar, Department of Computer Engineering & Information Technology
Suresh Gyan Vihar University
Jaipur, India

Abstract—The research paper titled "Hybrid Data Encryption as well as Decryption Using Hybrid RSA and DNA" develops a hybrid cryptosystem by combining the usefulness of such an asymmetric-key (public-key) cryptosystem with the efficacy of a symmetric-key (private-key) cryptosystem. These two types of cryptosystems use different types of keys. The method addresses concerns regarding the users' right to privacy, authentication, and accuracy by utilizing a data encryption process that is secure in both directions. Both the process of encrypting data and the process of decrypting data, which are both utilized by the system, are two different encryption methods. It has been suggested that a hybrid encryption algorithm, which combines DNA and RSA, be used for file encryption in order to address the issues with efficiency and security. The results of the testing show that the RSA and DNA hybrid encryption algorithm is suitable for use. In this particular research project's hybrid encryption and decoding for cloud processing with IOT devices, the DNA and RSA algorithms were used.

Keywords– Cryptography, Encryption, Decryption, DNA, RSA.

I. Introduction

How people use technology has changed as a result of cloud computing. It suggests a shift away from using computers primarily as tools with cutting-edge applications. However, as technology develops, risks multiply and important data protection has grown more difficult as a result of widespread internet use[1]. New encryption techniques are created daily, and extensive research is done to find a trustworthy cryptographic algorithm. Cryptography is the study of using logical and mathematical operations to encrypt and decrypt data in order to secure information[2]. This method has advanced quickly in terms of securing Internet of Things (IoT) applications, including those related to healthcare, finance, and transportation. Encryption in cryptography is primarily used to shield sensitive data from unauthorized modifications. Data must be encrypted in order to ensure a secure communication; otherwise, even if an eavesdropper effectively intercepts an encrypted message, it will be useless because an unauthorized person is unable to decrypt an encrypted message[3].

The first data encryption engineering principle was created in 1883 by Auguste Kerckhoff. He argued that while encryption methods may be widely known, the encryption key must be understood in order to decrypt encrypted data. Without the key, it is impossible to encrypt or decrypt data, even if the encryption algorithm is known. This is true for both the encoding and decoding processes, respectively. Based on the primary functions of each algorithm, the encryption framework has recently been divided generally into symmetric and asymmetric algorithms. In order to encrypt and decrypt information using the Symmetric Encryption Algorithm (SEA), also known as Secret Key Encryption (SKE), both the sender and the recipient must have their own private keys[4]. The Asymmetric Encryption Algorithm (AES), also known as Public Key Encryption (PKE), necessitates the possession of two keys (public and private key) by both the sender and recipient of an information in order for encryption and decryption operations to be successful on the desired information. The two encryption methods have guaranteed the protection of data from adversaries and weaknesses on insecure communication channels on modern technologies, and they have increased people's confidence in the strength of unbreakable algorithms [5].

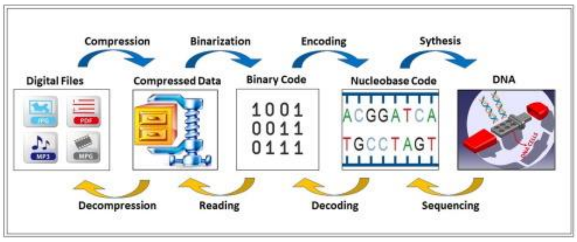


Figure 1. DNA Encryption and Decryption with Binary Sequence.

Techniques for substitution and transposition are available in classical cryptography. In the substitution technique, the plaintext's letters are swapped out for different letters, symbols, or numbers to create a ciphertext. The Caesar cipher, monoalphabetic block cipher, Playfair cipher, monoalphabetic cipher, etc. are a few examples of substitution techniques[5]. Rearranging the bits as well as characters in the data is known as a transposition cipher. The Rail Fence cipher is the most popular Transposition cipher. A key is also utilized in the encryption and decryption processes in modern cryptography. This is referred to as the symmetric or private key. In the symmetric cryptography model, the sender and the receiver share a secret key. The encryption algorithms and this shared key work together to create a ciphertext[6].

In public-key cryptography, each party has a unique set of keys—one of which is used as the key while the other serves as the private key—that are kept secret from other parties. Public-key Secrecy as well as authentication services are offered by cryptosystems. Take a look at Figure 2 , where the public key of B (PUb) is used to encrypt the plaintext X. The Public Key can be accessed by A because it is available to everyone. After encryption, a ciphertext Y is created. B obtains the plaintext X at the destination by using its private key to decrypt Y. (PRb). The confidentiality offered by this. Below are examples of plaintext and ciphertext decryption and encryption[7].

Y = E (X, PUb) (1)

X = D (Y, PRb) (2)

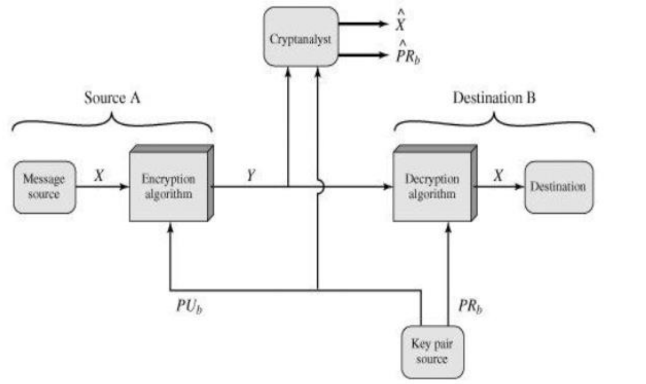


Figure 2. Secrecy with Public-Key Cryptosystem

A key must be delivered to both the sender and the receiver as part of the Key Distribution Technique in order to transmit the message. It is extremely challenging to share the key if encryption occurs at the application level and a key is required for each user pair involved in communication[8]. The receiver has no signature indicating that the message is from the specific sender, which is the second issue with the authentication mechanism. Digital signatures are required to address this problem. Whitfield Diffie and Martin Hellman created the concept of public-key cryptography in 1976 to address the aforementioned issues and offer a safe and secure cryptographic system. Public-key To transfer the Message M, cryptography, also referred to as asymmetric cryptography, needs two keys for encryption (Ek) and decryption (Dk). This was a revolutionary development in the field of cryptography. The primary property of public-key cryptosystems is that the decryption key cannot be computationally determined from the encryption key and cryptographic algorithm alone.

Take a look at Figure 3, which shows how public keys are used for authentication [4]. Here, the plaintext X is encrypted with the help of A's private key (PRa). After that, the ciphertext Y is sent to B, who uses A's public key (PUa) to decrypt it and produce the plaintext X. It is evident that the message was sent by A because the encryption was performed using A's private key. Here, the encrypted message serves as the digital signature. Furthermore, the message can only be changed with A's private key. As a result, it also ensures the integrity of the data and the source's authentication.

Y = E (X, PRa) (3)

X = D (Y, PUa) (4)

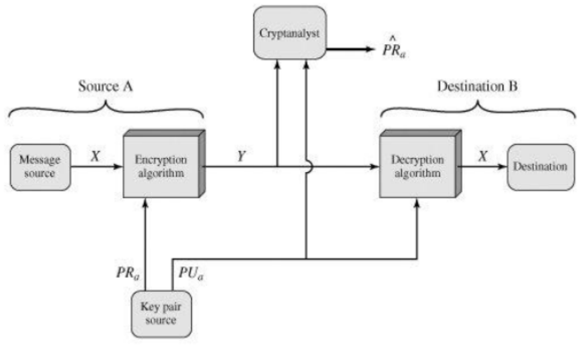


Figure 3. Public-Key Cryptosystem

Additionally, by using public-key cryptography, authentication as well as confidentiality can both be enabled. In this instance, the plaintext is encrypted once more using B's public key and A's private key (Digital Signature). The destination receives the obtained cipher text Z. Now, this message is decrypted using both B's private key and A's public key (Confidentiality). Figure 4 shows an illustration of this.

Z = E (PUb, E (PRa, X)) (5)

X = D (PUa, D (PRb, Z)) (6)

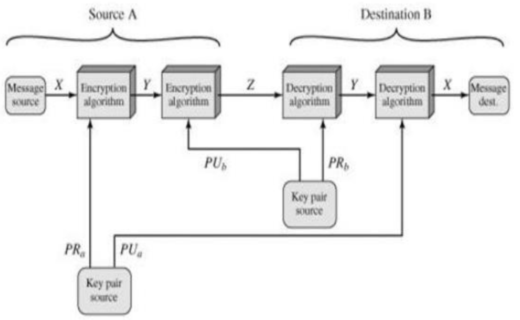


Figure 4. Public-key Cryptosystem: Privacy and Authentication.

This work proposed a hybrid asymmetric algorithm to secure cloud data in an Internet of Things environment using DNA and RSA algorithms[9][10]. The algorithm is based on sequence cryptography self-compression and the decomposition mechanism of text strings into DNA sequence. Finally, encrypted DNA encode was generated using RSA to improve the robustness of the algorithm[11].

II. Literature Review

Elamir et al. 2022 [12] The cloud facilitates data sharing between various infrastructure components. Unauthorized users of such systems and networks require a reliable cryptographic method of protection. There is a serious issue with the safety of the information and communication resources that are shared over the internet. This study proposes a cryptosystem that uses DNA cryptography and DNA mixing to keep this level of security. This study's findings suggest a cryptosystem based on the RSA algorithm and DNA cryptography concepts, with the added innovation of using mixed DNA strands encoded from medical images and reports to bolster the safety of IoT networks. The resulting image reconstructions were both precise and of high quality, thanks to this system. With 18 seconds gone by, there was already 92% overlap between the original as well as restored data. For E-health care via IoT system to aid medical teams in safely handling patient data between hospitals, the proposed cryptosystem proved the feasibility of protecting information in network security. These findings backed RSA's claims that it is a secure and efficient cryptographic tool.

Rashid 2021 et. al [13] used for such reasons. However, in order to improve data security, a new term, DNA, was brought into cryptography. The DNA can be readily used for transferring and storing data, so it becomes an efficient procedure for such purposes and is used to implement computation. A new cryptography method is suggested, which consists of two phases: encryption and decryption. The encryption phase consists of six stages, beginning with converting plaintext to their equivalent ASCII values afterwards to binary values. Following that, the binary values are changed to DNA characters, which are then converted to their complementary DNA sequences. These DNA sequences are then translated into RNA strands. Finally, the RNA sequences are translated into amino acids. The decryption phase includes six steps that are identical to the encryption steps but are performed in opposite order. It begins by converting amino acids to RNA sequences, and then to DNA sequences, and finally to their complimentary complementary DNA. Following that, DNA sequences transform to binary numbers and their ASCII equivalents. The concluding stage is to convert ASCII values into plaintext alphabet characters. Six text files of varying sizes were used as test material for evaluation reasons. The encryption and decryption times are used to determine performance.

Pavithran et. al 2021 [14] method utilized to ensure privacy of stored information. The main purpose of cryptography is to ensure that the content of a message is safe from being retrieved by an eavesdropper during transmission. This paper proposes a new cryptosystem using ideas from DNA cryptography and the theory of infinite automata. The gadget has a key pair generator, a transmitter, and a receiver. The DNA-based secret key is 256 bits in length and is generated by the sender based on information about the recipient. The DNA sequence is then encrypted using a Mealy machine that generates random numbers, further strengthening the ciphertext. It is possible that the proposed scheme will protect the system from brute force, known plaintext, differential cryptanalysis, cipher text only, man in the middle, and phishing attacks. The outcomes and discussions indicate that the proposed scheme is superior to existing schemes in terms of effectiveness and safety.

Vidhya et. al 2020 [15] The suggested effort aims to improve the DNA algorithm's critical strength. The mix of the genetic algorithm or the Diffie-Hellman key exchange method improves key strength. The Shannon entropy quantifies data compression, whereas the critical entropy quantifies key security.

Chirakkarottu et. al 2020 [16] Advised for use in diagnostic imaging. The purpose of this study is to suggest a novel, efficient, and highly secure method of encrypting medical images. It can be added to any medical image, regardless of the medium on which it is stored. The proposed method involves randomly rearranging the image's pixels using a generator of random numbers premised on a two-dimensional Zaslavski map. The image permutation is encrypted using DNA encryption. Analyses of quality and security, as well as methods of visual analysis and correlation evaluation, are used to verify the method's efficacy.

III. Proposed Methodology

The proposed method uses DNA and RSA algorithms to encrypt and decrypt data at multiple stages. You can see how the proposed method works in the diagram below; the first steps are those that produce a DNA sequence using the four nucleotides (Adenine, Cytosine, Thymine, and Guanine)[17]. Together, these bases form a double helix. Codons in DNA are triplets of nucleotide bases.

A. Pre-processing Stage

This data can only be prepared after reading classified information. In the case of a text file, the ASCII values are converted. Arrange them in a binary representation of 8 bits. Two adjacent bits are copied to one of the four DNA bases—adenine (A), cytosine (C), guanine (G), or thymine (T). To give

DOI: https://doi.org/10.17762/ijritcc.v11i6.6767
***Article Received**: 14 March 2023 **Revised**: 27 April 2023 **Accepted**: 20 May 2023*

one concrete example, consider Table 1. Whenever information from text files is converted to 8-bit binary format. Adenine (A), cytosine (C), guanine (G), and thymine (T) are the four bases in DNA that receive one of the two adjacent bits.

Table 1. Coding in DNA and Digital Representation

Bits	00	01	10	11
DNA	A	C	G	T

Information can take on any shape, including a binary form (message, image, video, or signal). The binary information is partitioned into 8-bit categories. The DNA building blocks (A, C, G, and T) are shifted to the two adjacent bits. For ease of understanding, let's pretend that some secret information is a binary bit file. Break up the binary data into a collection of bytes of any length.

B. Encryption stage

The two main types of cryptographic algorithms are those that use symmetric keys and those that use asymmetric keys. In the Symmetric Scheme, the sender and the receiver share a key. Public and private keys in asymmetric schemes are mathematically related to one another. The main benefit of the symmetric cryptographic algorithm is that it can encrypt large amounts of data quickly due to advances in cryptography technology. The proposed method employs the symmetric key in a DNA-based cryptographic algorithm.

Use the key to encrypt the binary data that was sequenced from DNA. The solution may be a DNA sequence or a binary string. The key's lifespan is adjustable. An exclusive OR operation is carried out on the elements of the DNA sequence that correspond to the key data and then the DNA sequence is converted back to its original form.

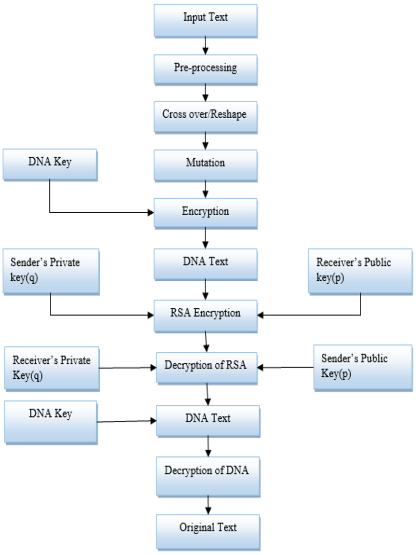


Figure 4. Flow chart of proposed methodology.

C. Reshaping Stage

After encryption, the only remaining operators in a basic genetic algorithm are replication, crossover, and mutation. The reshaping procedure yields the chromosome population that advances to the next stage of the process. The first count and size of individual chromosomes are calculated at this stage. These numbers can remain the same or change from round to round. The chromosomes (chromosome population) of parents with a specified length can be remodeled by aligning the DNA sequence into rows.

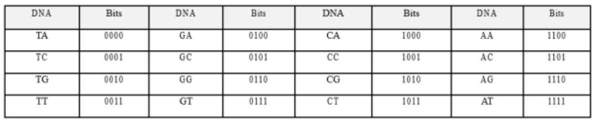
D. Crossover Stage

Crossover is the next step after constructing the parental chromosomes. There are two varieties of crossover. The techniques can be used in a series or rounds. Parents are selected in the first scenario, which takes place in a mating pool. To create two new individuals by switching the heads of parents 1 and 2, a single crossover point is selected between the first and last bits of chromosomes. Crossover occurs in two ways: by aligning the DNA sequence into rows for chromosome construction, and by rotation. Adjusting the degree of rotation left or right by a fixed amount.

E. Mutation Stage

After a crossover event, the chromosomes are vulnerable to mutation. Mutation refers to the alteration of string components. It employs a dual-mutation strategy. In the first, the data is converted to a binary vector, and two mutation points are defined between the first and last bits; bits in between are then complemented, so that a mutation at a single point can change from 1 to 0 and vice versa. Mutation type 2 involves changing each of the four bits into two DNA bases, for instance, 1010 CG (see Table 2 for an example). Shift the DNA bases to each other after converting to a vector of DNA bases and finding two points midway between the first and last bases. (i.e., C->G).

Table 2. DNA bases and Representation of bits



DNA	Bits	DNA	Bits	DNA	Bits	DNA	Bits
TA	0000	GA	0100	CA	1000	AA	1100
TC	0001	GC	0101	CC	1001	AC	1101
TG	0010	GG	0110	CG	1010	AG	1110
TT	0011	GT	0111	CT	1011	AT	1111

Crossover and mutation operations have a 100% chance frequency. Encrypt and reformat information to be submitted. A fixed number of iterations determines the total number of rounds. Send the encrypted file (text/image) to the recipient. Binaries at the receiving end reshape, decrypt, crossover, mutate, reshape, and restore data to its original format based on DNA sequencing.

F. Encryption of Text using DNA sequence.

```
Input: Read text
Output: Encoded DNA+RSA = Hybrid File
Generate Binary for data
Reshare Binary data
Grouping the adjacent two bits
While (Roundoff != 0):
    Encode Binary 2nd data with generated key
    Reshape Binary data 2nd
Perform Crossover and Mutation
Reshape Binary data 2nd
Generate Public Key RSA (p)
Generate Private Key RSA (q)
Encrypt DNA sequence with public key of Receiver
```

The pre-processing stage is confounded in the previous description of the D-GET technique. This means that for each kind of information file and format, it is wide-ranging among converting to ASCII values, trying to read text, separating components or letters, and having the text file properties as described above in order to solve this issue and generalize the DNA_RSA technique. In other words, the pre-processing stage is complicated. The same DNA_RSA steps are used in the generalization technique, but in place of the read and preprocessing phase of the data, a straightforward read binary file (fread) command is used instead. This command makes use of an 8-bit unsigned integer (uint8) as well as specific parameters that define the format of the hidden data[18].

G. Encryption of Encoded DNA sequence with RSA

After receiving DNA-encrypted data with a binary key, the information will be encrypted using the public key of the receiver[19][20]. The DNA code will then be converted into ASCAII-coded strings, which will contain the encoded DNA sequence of the actual text as well as the key to decrypt it. After applying the reverse process of the RSA algorithm with the public key of the sender and the private key of the receiver for the decryption process, applying the decryption process of DNA sequencing with the given key, and then getting the original data decrypted, the process was complete.

```
Input: Encode Hybrid File
Output: Decoded Original text
Decrypt Hybrid file with (q) key
Get DNA sequence
Binarize text
Reshape Binaries
While (Roundoff != 0):do
    Mutation
    Crossover
Reshape Binaries
Decrypt Binaries
Reshape Binaries
Output original text
```

IV. Results and Discussion

This work was accomplished with the assistance of an Intel i7-1100k processor running at 4.9 GHz, 16 gigabytes of random-access memory (RAM), the Windows 10 64-bit operating system, and the Python programming language with a Jupyter notebook. In order to determine whether or not the suggested method is effective, we put it through its paces using data sets of varying lengths of text.

Cryptanalysts will attack any encrypted data in an effort to decipher its contents by employing a wide variety of cryptanalytic, mathematical, and brute-force attacks. Robustness is essential for a successful encryption technique to use against them. Therefore, there are some characteristics that have to be accomplished. Here there is no connection whatsoever between the sensitive data values that existed before encryption and the encrypted data values that exist after encryption. The various components of the hidden data should be encrypted, and then the encryption should be blended around those components so that nothing is presented in its original position.

Table 3. Performance of proposed approach with execution time comparison.

Original Letters Length	Encrypted text length of DNA	Key length of DNA Sequence	Encrypted text length of RSA	Encryption Time (sec)	Decryption Time (sec)
50	200	128	256	0.015	0.021
69	276	128	506	0.017	0.014
22	88	128	256	0.016	0.002

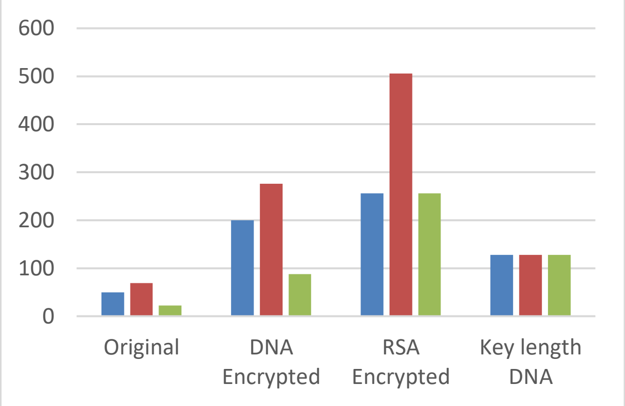


Figure 5. text length comparison of original vs encrypted data

.

DOI: https://doi.org/10.17762/ijritcc.v11i6.6767
***Article Received**: 14 March 2023 **Revised**: 27 April 2023 **Accepted**: 20 May 2023*

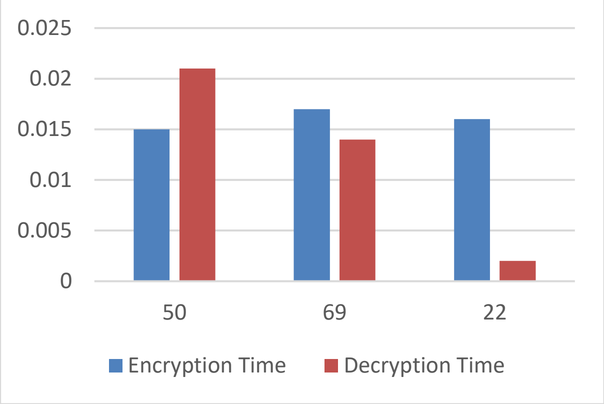


Figure 5. Execution time of text lengths for 50, 69, 22

Table 3 depicts the final results of the proposed method in terms of execution time with text letters length generation. In this table, we can see that the DNA encrypted file make range around from 200 to 300 or letters of genomes, while the key of DNA contains only 128 letters among all of the results. The encryption average time of this proposed work is approximately 0.015 seconds, while the average decryption time is approximately 0.01 seconds.

V. Conclusion

The research paper titled "Hybrid Data Encryption and Decryption using Hybrid RSA and DNA" develops a hybrid cryptosystem by combining the advantages of an asymmetric-key (public-key) cryptosystem with the efficacy of a symmetric-key (private-key) cryptosystem. This results in the hybrid system having both the benefits of an asymmetric-key cryptosystem and the benefits of a symmetric-key cryptosystem. A two-way secured data encryption procedure is utilized in the method in order to address concerns regarding the user's right to privacy, the authenticity of the user, and the precision of the data. The encryption and decryption processes used by the system each make use of a different form of the system's two distinct encryption methods. In order to solve the issues with efficiency and safety that have been brought up in relation to file encryption, a hybrid encryption algorithm that combines DNA and RSA has been proposed. The findings of the tests indicate that the hybrid encryption method utilizing RSA and DNA is superior. During the course of this study, the DNA and RSA algorithms were utilized in order to perform hybrid encryption and decoding for cloud processing with IOT devices.

References

[1] M. A. Iliyasu, O. A. Abisoye, S. A. Bashir, and J. A. Ojeniyi, “A review of DNA cryptograhic approaches,” Proc. 2020 IEEE 2nd Int. Conf. Cyberspace, CYBER Niger. 2020, pp. 66–72, 2021, doi: 10.1109/CYBERNIGERIA51635.2021.9428855.

[2] T. Mandge and V. Choudhary, “A DNA encryption technique based on matrix manipulation and secure key generation scheme,” 2013 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2013, pp. 47–52, 2013, doi: 10.1109/ICICES.2013.6508181.

[3] G. Bhoi, R. Bhavsar, P. Prajapati, and P. Shah, “A review of recent trends on DNA based cryptography,” Proc. 3rd Int. Conf. Intell. Sustain. Syst. ICISS 2020, pp. 815–822, 2020, doi: 10.1109/ICISS49785.2020.9316013.

[4] X. Zhou and X. Tang, “Research and implementation of RSA algorithm for encryption and decryption,” Proc. 6th Int. Forum Strateg. Technol. IFOST 2011, vol. 2, pp. 1118–1121, 2011, doi: 10.1109/IFOST.2011.6021216.

[5] D. A. Zebari, H. Haron, S. R. M. Zeebaree, and D. Qader Zeebaree, “Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations,” ICOASE 2018 - Int. Conf. Adv. Sci. Eng., pp. 312–317, 2018, doi: 10.1109/ICOASE.2018.8548824.

[6] B. B. Raj and V. Ceronmani Sharmila, “An survey on DNA based cryptography,” 2018 Int. Conf. Emerg. Trends Innov. Eng. Technol. Res. ICETIETR 2018, pp. 1–3, 2018, doi: 10.1109/ICETIETR.2018.8529075.

[7] F. J. Aufa, Endroyono, and A. Affandi, “Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm,” Proc. - 2018 4th Int. Conf. Sci. Technol. ICST 2018, vol. 1, pp. 1–5, 2018, doi: 10.1109/ICSTC.2018.8528584.

[8] K. A. Fasila, “Automated DNA encryption algorithm based on UNICODE and colors,” Proc. 2017 2nd IEEE Int. Conf. Electr. Comput. Commun. Technol. ICECCT 2017, pp. 6–9, 2017, doi: 10.1109/ICECCT.2017.8117907.

[9] S. Arunpandian and S. S. Dhenakaran, “DNA based Computing Encryption Scheme Blending Color and Gray Images,” Proc. 2020 IEEE Int. Conf. Commun. Signal Process. ICCSP 2020, pp. 966–970, 2020, doi: 10.1109/ICCSP48568.2020.9182195.

[10] F. H. M. S. Al-Kadei, H. A. Mardan, and N. A. Minas, “Speed Up Image Encryption by Using RSA Algorithm,” 2020 6th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2020, pp. 1302–1307, 2020, doi: 10.1109/ICACCS48705.2020.9074430.

[11] K. S. Sajisha and S. Mathew, “An encryption based on DNA cryptography and steganography,” Proc. Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2017, vol. 2017-January, pp. 162–167, 2017, doi: 10.1109/ICECA.2017.8212786.

[12] M. M. Elamir, M. S. Mabrouk, and S. Y. marzouk, “Secure framework for IoT technology based on RSA and DNA cryptography,” Egypt. J. Med. Hum. Genet., vol. 23, no. 1, 2022, doi: 10.1186/s43042-022-00326-5.

[13] R. Ahmad, S. Naz, M. Afzal, S. Rashid, M. Liwicki, and A. Dengel, “A Deep Learning based Arabic Script Recognition System : Benchmark on KHAT,” vol. 17, no. 3, pp. 299–305, 2020.

[14] P. Pavithran, S. Mathew, S. Namasudra, and P. Lorenz, “A novel cryptosystem based on DNA cryptography and randomly generated mealy machine,” Comput. Secur., vol. 104, p. 102160, 2021, doi: 10.1016/j.cose.2020.102160.

[15] E. Vidhya and R. Rathipriya, “Key Generation for DNA Cryptography Using Genetic Operators and Diffie-Hellman

***Article Received**: 14 March 2023 **Revised**: 27 April 2023 **Accepted**: 20 May 2023*

Key Exchange Algorithm," Int. J. Math. Comput. Sci., vol. 15, no. 4, pp. 1109–1115, 2020.

[16] S. Chirakkarottu and S. Mathew, "A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography," SN Appl. Sci., vol. 2, no. 1, pp. 1–10, 2020, doi: 10.1007/s42452-019-1685-8.

[17] R. Soni, A. Johar, and V. Soni, "An encryption and decryption algorithm for image based on DNA," Proc. - 2013 Int. Conf. Commun. Syst. Netw. Technol. CSNT 2013, pp. 478–481, 2013, doi: 10.1109/CSNT.2013.105.

[18] L. K. Galla, V. S. Koganti, and N. Nuthalapati, "Implementation of RSA," 2016 Int. Conf. Control Instrum. Commun. Comput. Technol. ICCICCT 2016, pp. 81–87, 2017, doi: 10.1109/ICCICCT.2016.7987922.

[19] M. Sabry, M. Hashem, T. Nazmy, and M. E. Khalifa, "Design of DNA-based Advanced Encryption Standard (AES)," 2015 IEEE 7th Int. Conf. Intell. Comput. Inf. Syst. ICICIS 2015, pp. 390–397, 2016, doi: 10.1109/IntelCIS.2015.7397250.

[20] A. Jain and N. Rajpal, "Adaptive key length based encryption algorithm using DNA approach," Proc. - 2013 Int. Conf. Mach. Intell. Res. Adv. ICMIRA 2013, no. 3, pp. 140–144, 2014, doi: 10.1109/ICMIRA.2013.34.