**18CSE381T – Cryptography**

**MINOR PROJECT REPORT**

***Submitted by***

**PRAKHRANSHU SINGH [RA2011030010217]**

**SOORAJ TOMAR [RA2011030010224]**

**MUSTYALA NANDA KISHOR [RA2011030010225]**

**SUSHANT KUMAR SINGH[RA2011030010228]**

**SIVE VISHWA T E[RA2011030010231]**

***Under the Guidance of***

**Dr. Annapurani Panaiyappan**

**Professor & HOD, Department of Networking and Communications**

***In partial satisfaction of the requirements for the degree of***

**BACHELOR OF TECHNOLOGY**

**in**

**COMPUTER SCIENCE AND ENGINEERING**

**with specialization in Cyber Security**

****

**SCHOOL OF COMPUTING**

**COLLEGE OF ENGINEERING AND TECHNOLOGY SRM INSTITUTE OF SCIENCE AND TECHNOLOGY KATTANKULATHUR – 603203**

**A Dynamic DNA Cryptography Using RSA Algorithm and Stronger OTP**

**Abstract**

A Dynamic DNA Cryptography Using RSA Algorithm and OTP is a combination of algorithm like RSA and One Time Pad key generation which is used for Encryption and Decryption of plain text, image, audio and video that are converted from binary numbers into a DNA sequence. The device MAC Address is a unique identification which helps to connect one or more nodes and the information is transmitted from one node to another in a secured fashion. The method of cryptography is used to protect the transmission of confidential information over wireless networks. If the key used in the OTP is randomly generated and not used more than once, then the algorithm is considered to be completely unbreakable. This technique does not provide complete unauthorized data access, only is a stronger method than most.**[1]**

***Keywords****—DNA Cryptography, Encryption, Decryption, Cryptography, One Time Pad.*

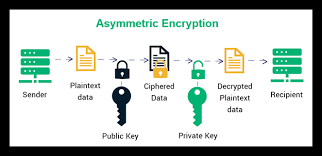


Figure 1: Asymmetric Encryption in Cryptography

**Introduction**

Data is any type of stored digital information. Security is about the protection of assets. Data security or Information Security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, personal databases and websites. To hide any data two techniques are mainly used one is Cryptography and the other is Steganography. In this paper we use Cryptography. Cryptography is the science of protecting data, which provides methods of converting data into unreadable form, so that Valid User can access Information at the Destination. Cryptography is the science of using mathematics to encrypt and decrypt data. **[4]**

In the digital world, cryptography plays an important role in day-to-day life that information security exists since historic times and it is existing in our modern life. The art of cryptography is considered to be born along with the art of writing. The roots of cryptography are found in Roman and Egyptian civilizations. Cryptography offers variety of aspects of data security. The main factors in cryptography are confidentiality, information integrity, authentication & non-repudiation.

The principal objectives of this paper are to more concentrate on the confidentiality phase & it help to discover the approach (ciphers) to make certain privacy via the use of DNA. DNA Cryptography is one of the most essential & promising disciplines in information security. Cryptography is considered as a technique of accomplishing confidentiality or privacy in data or message transmission. Additionally, it is a procedure of transferring the sender's data to a secret layout that is known as the ciphertext that the receiver will get recognize the secret message. The RSA algorithm is regarded as a robust asymmetric encryption algorithm. Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use. RSA has the more security; thus, the algorithm is proved to be cryptographically secure and it is suitable for applications where more than one layer of security is required. OTP is used for key generation purpose. The transferring information from one node to another node by using the MAC address it is very safe and secure as every device has its unique address in its DNA Cryptography Encryption.**[1] [2]**

**Literature Survey**

We started with paper **[6]** to introduce ourselves with the idea and need for Cyber Security. After which, papers **[3]** and **[4]** were followed to give a basic understanding of Cryptographic Techniques, how they work and how is a good and robust Encryption takes place, along with the basics of Ciphers, Symmetric and Asymmetric Algorithms and finally AES, DES and RSA. With the knowledge gained, Papers **[1]**,**[2]** and **[5]** were studied with the sole purpose to find a robust and modern Encryption Technique to provide maximum security. Paper **[1]** forms the main base for this project since there was a vulnerability found in the sense that although the Encryption is extremely secure with RSA and DNA Encryption, however, the Technique does not allow for complete User Authentication and the OTP system used uses a random OTP of **4** digit only which can be easily guessed ad also only a file size of **100 MB** is allowed, leading to limited applications. In this project we shall attempt to rectify these errors by generating truly strong random OTPs and hypothesizing a way to provide larger file support.

The table below shows the Literature Survey summary of all journals referenced in this project along with their results and limitations.

Table 1: Literature Survey of all the journals read by the team as part of original inspiration for this project

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S. No.** | **Title of Paper** | **Author and Journal Name** | **Objectives of the Paper** | **Methodologies Used** | **Results Obtained** | **Limitations** |
| 1. | “A Dynamic DNA Cryptography Using RSA Algorithm and OTP” | Poojashree Kamble,Firoz Nagarchi,Akshata Akkole,Vanishree Khanapur,Bahubali Akiwate, International Journal of Scientific Research in Computer Science and Engineering | In this approach, the encryption and the decryption take place through RSA Algorithm and the OTP. The use of a combination of DNA with RSA ensures twofold protections in a cloud environment where there are greater probabilities of breaches. | RSA Algorithm DNA Encoding Algorithm  One Time Pad Key Generation | A robust Cryptography Technique using DNA Encryption and OTP System | In future the network can be connected with a greater number of nodes with both IP Address and MAC address with improvement in performance. Proposed File size only up to 100MB.  Only 4-digit OTP, can be guessed easily by a fast-computing machine. |
| 2. | “A Research Paper on Cryptography” | Gurdeep Singh, Prateek Kumar, International Journal for Technological Research in Engineering | Abstract Data Types, Data Encryption, Data Compression, Asymmetric Key Cryptography | Symmetric and Asymmetric Encryption and Decryption | Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. | If the attacker will get the key and sender and receiver is not aware about it, it may harm the CIA triad. So, proper method should be used to Encrypt and Decrypt the data. |
| 3. | “Research Paper on Cyber Security” | Mrs. Ashwini Sheth, Mr. Sachin Bhosale & Mr. Farish Kurupkar, Contemporary Research in India | In the current world of technology, it is crucial to know what Cyber Security is and how to use it effectively. How to Secure Systems, important files, data and other important virtual things. | 1)Symmetric and Asymmetric Encryption 2) Types of Phishing: -Ransomware, Malware. 3)Goals of Cyber Security: Confidentiality, Integrity, Availability. 4)Attacks on IOT | Awareness on Online Attacks, Types of Viruses, Goals of Cyber Security, Advantages and Disadvantages of Cyber Security | Increasing Threats targeting user devices, devices used by employees who are working from home aren't protected well enough from attacks and preventing hackers. |
| 4. | “A Study on Cryptographic Techniques” | Anjali Krishna A, Dr. L C Manikandan, International Journal of Scientific Research in Computer Science, Engineering and Information Technology | Data security using Symmetric and Asymmetric Key Encryption. | Symmetric and Asymmetric Key Encryption | There are different techniques and algorithms researched, and various types of work have been performed. In this paper briefly discussed cryptography and its form of  symmetric key cryptography and algorithms for asymmetric key cryptography. | Key leakage, software bugs, holes in operating systems, side-channel attacks, phishing attacks, and social engineering ttacks. So, it is important to understand and acknowledge that cryptography ≠ security. |

**Architecture Diagram**

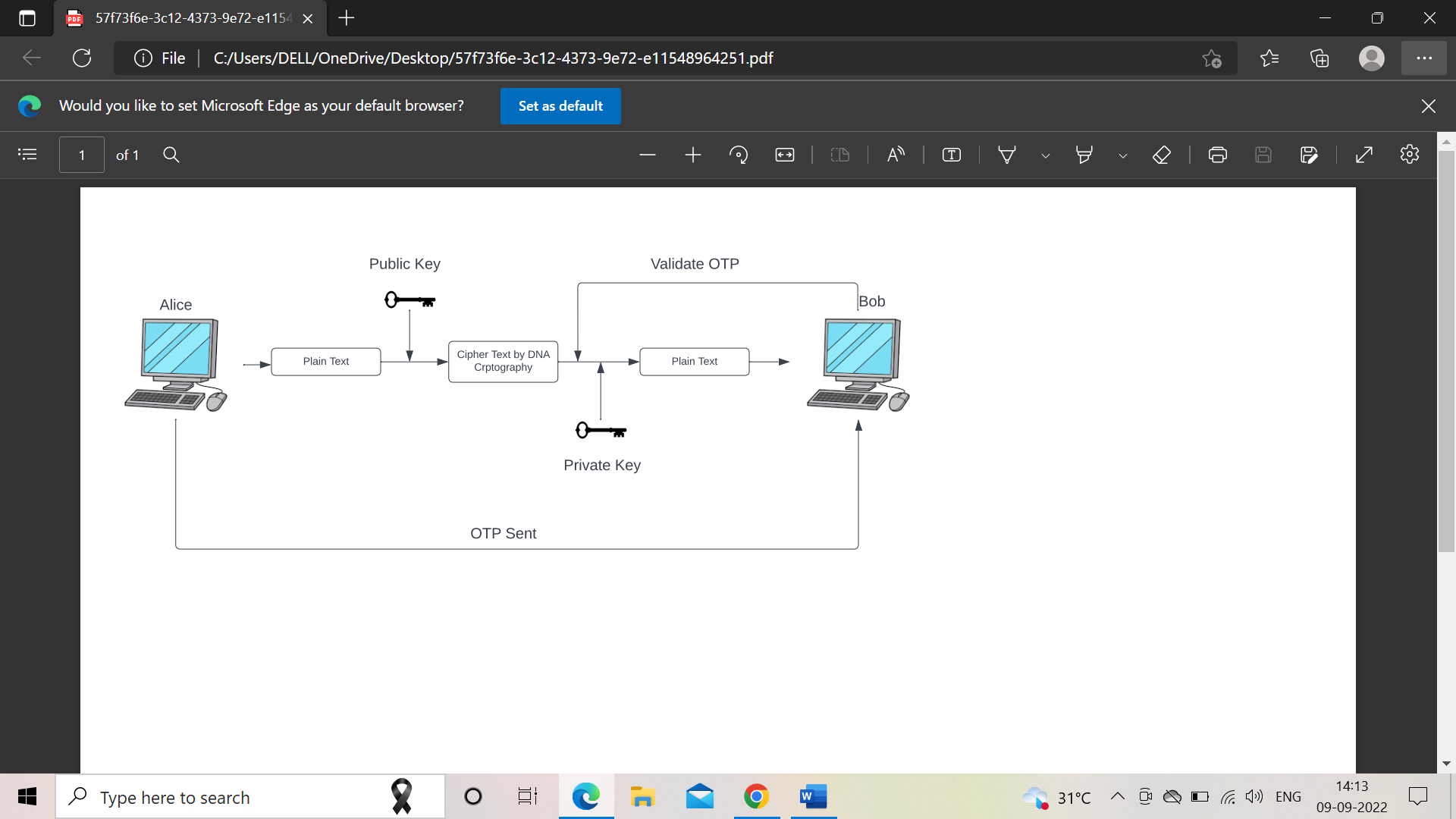


Figure 2: Architecture Diagram for the Encryption and Decryption Process between Communicators

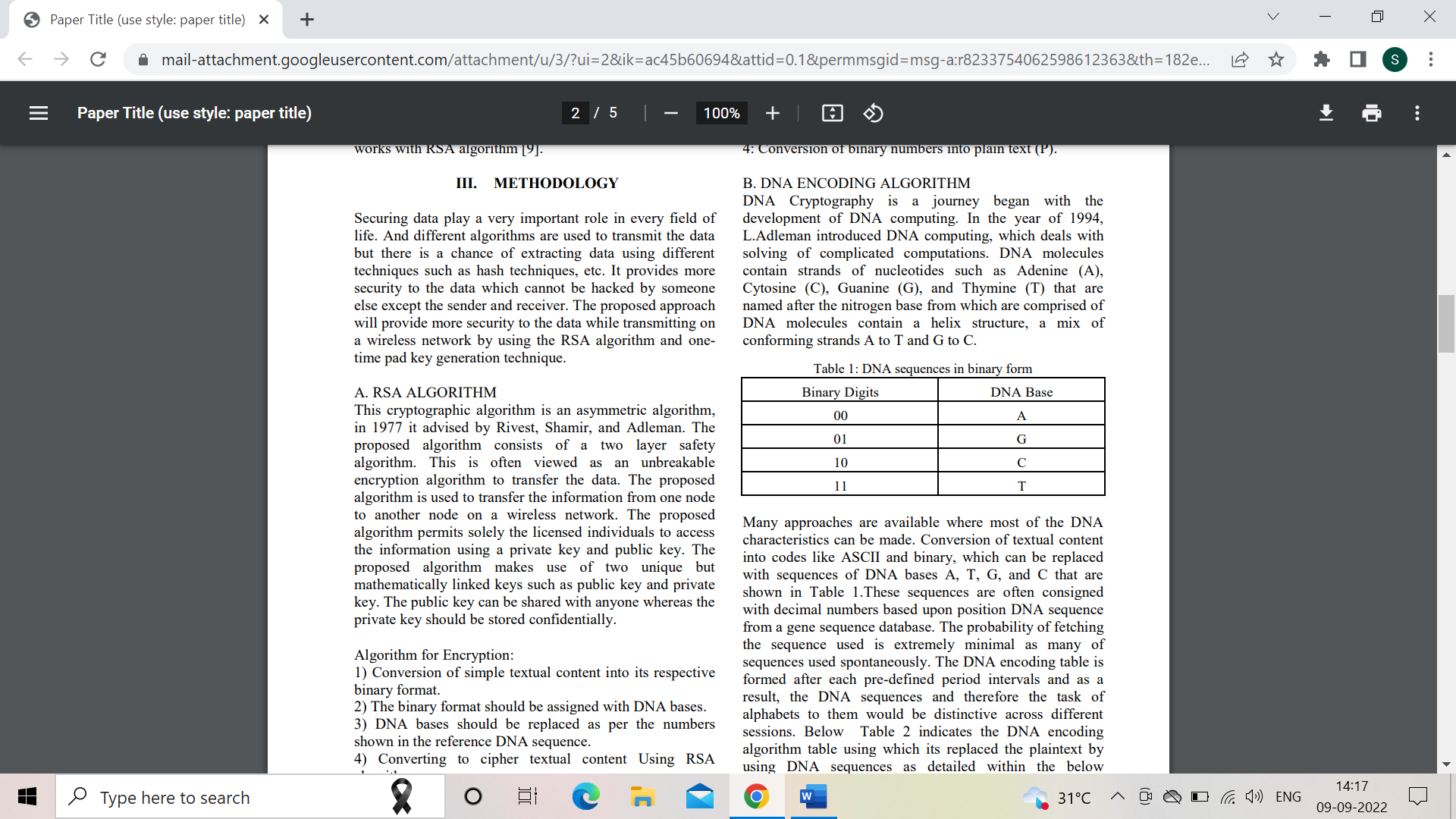


Figure 3: DNA Encoding as per binary digits

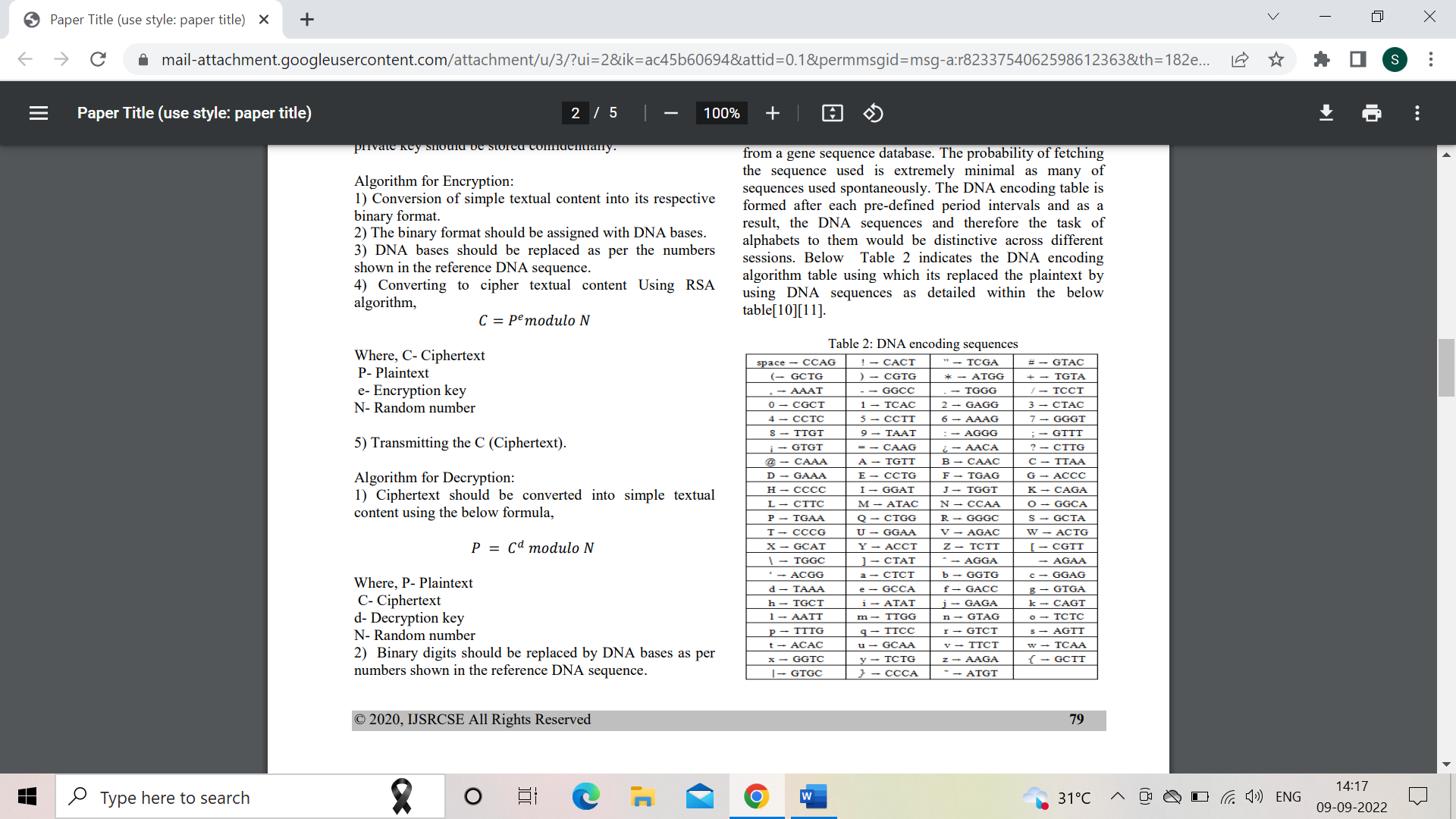


Figure 4: DNA Encoding Sequences - Example

**References**

**[1]** Poojashree Kamble,Firoz Nagarchi,Akshata Akkole,Vanishree Khanapur,Bahubali Akiwate, “A Dynamic DNA Cryptography Using RSA Algorithm and OTP”, International Journal of Scientific Research in Computer Science and Engineering Vol.8, Issue.4, pp.78-82, August (2020).

**[2]** Mahbuba Begum, Jannatul Ferdush, Md. Golam Moazzam, “A Hybrid Cryptosystem using DNA, OTP and RSA,” International Journal of Computer Applications (0975 – 8887), Volume 172 – No.8, August 2017. (As extra reference, not part of Literature Survey)

**[3]** Anjali Krishna A, Dr. L C Manikandan, “A Study on Cryptographic Techniques”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 6, Issue 4, pg. 321-327, July-August 2020.

**[4]** Gurdeep Singh, Prateek Kumar, “A Research paper on cryptography”, International Journal for Technological Research in Engineering, Volume 7, Issue 4, December-2019.

**[5]** Hamza Hammami, Hanen Brahmi, Sadok Ben Yahia, “Secured Outsourcing Towards a Cloud Computing Environment Based on DNA Cryptography,” IEEE, pp. 31-36, 2018. (As extra reference, not part of Literature Survey)

**[6]** Mrs. Ashwini Sheth, Mr. Sachin Bhosale & Mr. Farish Kurupkar, “Research Paper on Cyber Security”, Contemporary Research in India, Special Issue: April, 2021.