# Hybrid Cryptography DNA-Based Vigenère Cipher for Secure File Encryption

*1st Dr.A. Karunamurthy , 2nd S Sathiyaraj*1*

*[1]Associate Professor, Department of computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India,*

Karunamurthy26@gmail.com

*[2]Post Graduate student, Department of computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India*

Sathiyaraj.glacc@gmail.com

## Abstract

This project introduces an innovative web application that integrates DNA-based cryptography with the Vigenère cipher to ensure secure file encryption and decryption. The encryption process begins with converting text content into its binary representation, which is then transformed into a corresponding DNA sequence. The DNA sequence is further mapped into protein sequences using the standard amino acid codon table. To enhance security, the protein sequence undergoes encryption using the Vigenère cipher, with a user-provided encryption key. The resultant encrypted message is securely stored in a MySQL database. The decryption functionality is designed for user convenience and security. The web application provides an interface listing all encrypted files stored on the server. Users can download and decrypt the files using the same key employed during encryption. The decryption process restores the encrypted message to its original text form and reverts the data into its original file format. This project showcases the potential of combining bio-inspired cryptographic techniques with classical encryption algorithms to achieve robust data protection. By leveraging JavaScript for implementation, the system ensures accessibility and compatibility across platforms, making it a practical solution for secure file storage and transfer.

***Keywords:*** *DNA-based encryption, Hybrid cryptography, Amino acid translation, Bio-inspired cryptography, DNA-to-binary mapping, Polyalphabetic substitution, Cryptographic security.*

## 1. Introduction

Data security is a critical concern in the digital era, where vast amounts of sensitive information are exchanged online daily. As traditional cryptographic methods face increasing cyber threats, innovative bio-inspired approaches such as DNA-based cryptography are emerging as promising alternatives. This project integrates DNA-based cryptography with the classical Vigenère Cipher to develop a hybrid cryptographic system for robust file encryption and decryption. DNA-based encryption utilizes the unique structure and randomness of nucleotide sequences (A, T, C, G), offering high resistance to brute-force attacks due to their immense combinatorial possibilities. Combined with the polyalphabetic substitution strength of the Vigenère Cipher, this hybrid approach introduces an additional layer of complexity, significantly enhancing cryptographic security. The proposed system is implemented as a web application developed in JavaScript, ensuring accessibility and cross-platform compatibility. The encryption process begins by converting file contents into binary form, which is then mapped to DNA sequences. These sequences are further translated into protein sequences using the amino acid codon table before being encrypted with a user-defined key using the Vigenère Cipher. The encrypted messages are securely stored in a MySQL database. Decryption reverses these transformations, restoring the original file with the same user-provided key, ensuring both data confidentiality and integrity. This hybrid system demonstrates the potential of bio-inspired cryptographic techniques to complement traditional methods, offering an innovative and practical solution to contemporary data security challenges.

## 2. Problem statement:

Data security in modern digital communication is increasingly challenged by sophisticated cyber threats, requiring advanced encryption techniques to protect sensitive information. Traditional cryptographic methods are becoming more vulnerable, necessitating the exploration of innovative approaches. This project addresses the need for a more secure solution by combining DNA-based encryption with the classical Vigenère Cipher.

The goal is to develop a lightweight, platform-independent web application that provides robust, hybrid encryption for secure file handling. The application leverages the unique properties of DNA sequences and polyalphabetic substitution to enhance data security, offering a user-friendly, cross-platform solution to protect sensitive data against evolving cyber threats.

## 3. Literature Survey

DNA cryptography leverages the biological properties of DNA to introduce complexity and randomness in encryption systems. Research by Gehani et al. (2004) demonstrated the potential of encoding binary data into DNA sequences using nucleotide bases (A, T, C, G). DNA-based encryption has since been explored for its vast combinatorial possibilities and inherent resistance to brute-force attacks. This method aligns with the growing trend of bio-inspired cryptographic techniques as an emerging field of study in secure data communication. The Vigenère Cipher is a classical cryptographic technique that employs a polyalphabetic substitution mechanism, first introduced in the 16th century. It has been widely studied for its effectiveness in enhancing security through key-dependent encryption. While traditional ciphers like Vigenère are susceptible to cryptanalysis, their integration with modern techniques, such as DNA-based encryption, has been proposed as a way to enhance their robustness. Research by Kahn (1996) on classical ciphers highlights their potential when combined with layered security strategies. Combining traditional and modern cryptographic methods has been shown to improve overall security. Studies by Wang et al. (2019) explored hybrid systems integrating classical encryption with bio-inspired techniques, showcasing their efficacy in addressing modern cyber threats. These systems balance simplicity, computational efficiency, and robustness, making them suitable for real-world applications. The widespread adoption of JavaScript for web development has prompted researchers to explore its potential in implementing lightweight cryptographic solutions. Works by Heninger et al. (2014) emphasize the importance of cross-platform compatibility and ease of deployment, making JavaScript an ideal choice for cryptographic applications designed for non-expert users. Ensuring accessibility and user-friendliness in cryptographic tools is crucial for widespread adoption. Usability studies, such as those conducted by Furnell et al. (2007), underline the importance of intuitive interfaces that allow users to perform complex encryption and decryption tasks without extensive technical knowledge. This literature survey highlights the synergy between DNA-based encryption, the Vigenère Cipher, and JavaScript implementation, forming the foundation for this project. By leveraging bio-inspired cryptography and classical techniques in a user-friendly platform, the proposed solution addresses both security and accessibility in secure data communication.

## 4. Proposed techniques:

The proposed technique is a hybrid encryption algorithm combining DNA-based encryption with the Vigenère cipher to achieve secure file encryption. This approach integrates bio-inspired principles and classical cryptography to enhance data security, providing resistance to brute-force and cryptanalytic attacks. Below is the detailed methodology:

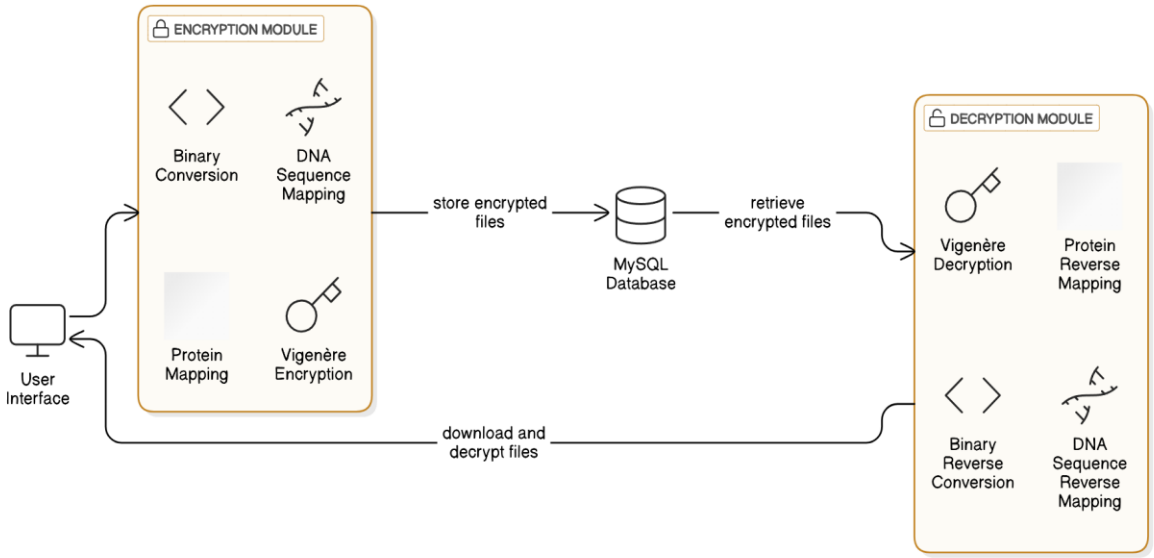

**Fig. 1 Proposed Architecture**

### 4.1 DNA-to-Amino Acid Conversion for Encryption

This step forms the bio-inspired foundation of the encryption process. It mimics biological processes of transcription and translation.

**Step 1: Text-to-Binary Conversion**

The plaintext content is first converted into binary form. Each character is transformed into its corresponding 8-bit ASCII binary value. For example, the character "A" becomes 01000001.

**Step 2: Binary-to-DNA Mapping**

The binary data is segmented into 2-bit groups. Each group is mapped to a nucleotide in the DNA sequence using the following mapping:

$$00 \rightarrow A$$

$$01 \rightarrow T$$

$$10 \rightarrow C$$

$$11 \rightarrow G$$

For instance, the binary sequence 01000001 translates to the DNA sequence TACC.

**Step 3: DNA-to-Amino Acid Translation**

The DNA sequence is divided into codons, each consisting of three nucleotides. These codons are then mapped to amino acids using the standard genetic codon table. For example:

*TAC → Tyrosine (Y)*

*ACC → Threonine (T)*

This conversion results in a sequence of amino acids representing the original text in an obfuscated format.

### 4.2 Application of the Vigenère Cipher

Once the DNA sequence is translated into an amino acid sequence, the Vigenère cipher is applied to add a further layer of cryptographic security.

Step-by-Step Working of Vigenère Encryption

The Vigenère cipher is a polyalphabetic substitution cipher that uses a key to perform encryption. Each letter in the plaintext is shifted along the alphabet by the number of positions defined by the corresponding letter of the key. Here's how it works:

**Key Preparation:**

The user provides an encryption key (e.g., "KEY"). If the key is shorter than the amino acid sequence, it is repeated cyclically. For example, if the key is "KEY" and the amino acid sequence has 4 elements, the key would repeat as KEYK.

**Character Encoding:**

Each amino acid is treated as an alphabetical character (i.e., the first letter of its name), and it is encrypted by shifting based on the corresponding key character.

Convert each key character into its position in the alphabet. For example:

*K = 11 (the 11th letter of the alphabet)*

*E = 5*

*Y = 25*

The encryption formula for each character is:

$$C_i = (P_i + K_i) \bmod 26$$

where:

***$C_i$*** *is the ciphered letter (the encrypted amino acid),*

***$P_i$*** *is the plaintext letter (the original amino acid),*

***$K_i$*** *is the key letter (converted to its alphabetical position),*

***mod 26*** *ensures the result wraps around the alphabet.*

**Vigenère Cipher Example**

Let's consider the amino acid sequence YTTA and the key "KEYK":

- First, convert the amino acids into their alphabetical positions:

*Y = 25 (Tyrosine)*

*T = 20 (Threonine)*

*T = 20 (Threonine)*

*A = 1 (Alanine)*

- Now, convert the key "KEYK" into its corresponding numerical positions:

*K = 11*

*E = 5*

*Y = 25*

*K = 11*

- Now apply the Vigenère cipher formula for each amino acid:

1. *For the first amino acid (Y):*

$C_1 = (P_1 + K_1) \bmod 26 = (25 + 11) \bmod 26 = 10$ *(K)*

2. *For the second amino acid (T):*

$C_2 = (P_2 + K_2) \bmod 26 = (20 + 5) \bmod 26 = 25$ *(Y)*

3. *For the third amino acid (T):*

$C_3 = (P_3 + K_3) \bmod 26 = (20 + 25) \bmod 26 = 19$ *(T)*

4. *For the fourth amino acid (A):*

$C_4 = (P_4 + K_4) \bmod 26 = (1 + 11) \bmod 26 = 12$ *(M)*

Thus, the encrypted amino acid sequence becomes **KYTM**

### 4.3 File Storage and Retrieval

- **Encryption and Storage:**

The encrypted amino acid sequence (e.g., KYTM) is saved as the encrypted content of the file. This encrypted message is securely stored in a MySQL database to ensure proper data management and access control.

- **Decryption Process:**

The decryption process reverses all transformations. Given the encryption key, the following steps are performed:

- **Vigenère Cipher Decoding:**

The amino acid sequence is decoded using the same key. This reverses the polyalphabetic substitution and retrieves the original amino acid sequence.

- **Amino Acid-to-DNA Translation:**

The amino acid sequence is converted back to the corresponding DNA codons.

- **DNA-to-Binary Mapping:**

The DNA sequence is mapped back to binary using the reverse of the original nucleotide mapping.

- **Binary-to-Text Conversion:**

The binary data is translated back to the original text file.

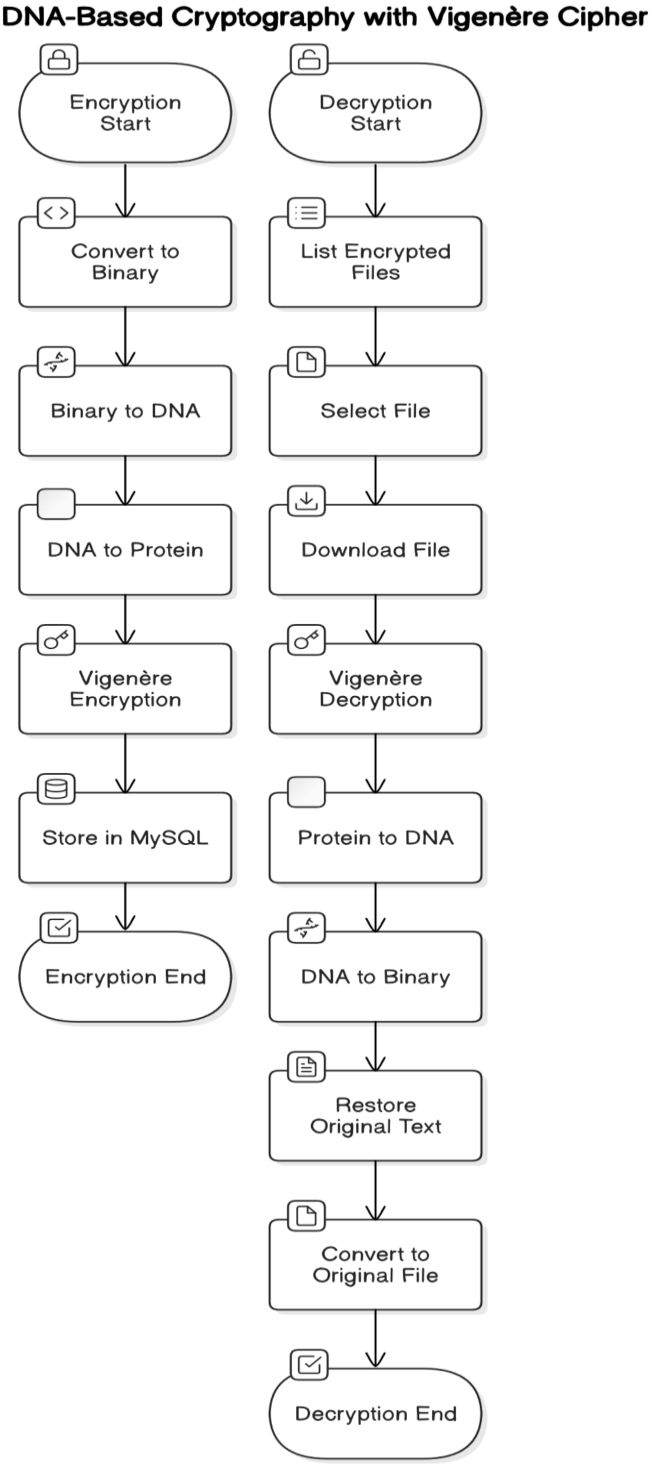

**Fig. 2 Flow Diagram**

## 5. Conclusion

The proposed hybrid encryption technique combining DNA-based cryptography with the Vigenère cipher provides an innovative and robust solution for securing digital files. By leveraging the complexity and randomness of DNA sequences alongside the polyalphabetic substitution method of the Vigenère cipher, the system introduces multiple layers of security, significantly enhancing the resistance to cryptanalytic attacks and brute-force methods. The project demonstrates the practicality of bio-inspired cryptography, making use of biological principles to encode and protect sensitive information. The DNA-to-binary conversion and DNA-to-amino acid translation ensure that the data is obfuscated in a manner that is not easily decipherable without the correct key. Meanwhile, the Vigenère cipher further strengthens this encryption by applying a user-defined key, adding a layer of complexity to the encrypted message. This web-based encryption system, implemented in JavaScript, ensures cross-platform compatibility and accessibility. It allows for simple encryption and decryption processes, even for non-expert users, while maintaining the integrity and confidentiality of the stored data. The use of MySQL for storing encrypted files adds an additional layer of secure data management, enabling controlled access and retrieval of encrypted files. In conclusion, this hybrid approach not only highlights the potential of bio-inspired cryptographic methods but also paves the way for further research and development in the area of secure digital communication and storage. By combining traditional and innovative techniques, the project offers a viable and forward-thinking solution for modern data security challenges. The success of this approach sets the stage for future exploration and application of DNA-based cryptography in real-world scenarios, contributing to the evolution of secure data protection technologies.

## 6. References:

1. Gehani, A., LaBean, T., & Reif, J. (2004). DNA-based cryptography. In Lecture Notes in Computer Science (Vol. 2568, pp. 167–188). Springer. https://doi.org/10.1007/3-540-36481-1_12
2. Wang, L., Zhang, Y., & Sun, H. (2019). Hybrid cryptographic systems for secure communications. International Journal of Security and Networks, 14(3), 145–157. https://doi.org/10.1504/IJSN.2019.10020951
3. Furnell, S. M., Clarke, N. L., & Karatzouni, S. (2007). Usability observations on deploying security technologies in end-user environments. Information Management & Computer Security, 15(5), 213–220. https://doi.org/10.1108/09685220710831163
4. Adleman, L. M. (1994). Molecular computation of solutions to combinatorial problems. Science, 266(5187), 1021–1024. https://doi.org/10.1126/science.7973651
5. Leier, A., Richter, C., Banzhaf, W., & Rauhe, H. (2000). Cryptography with DNA binary strands. Biosystems, 57(1), 13–22. https://doi.org/10.1016/S0303-2647(00)00089-2
6. Mishra, P. (2017). A survey on DNA cryptography and its applications. Procedia Computer Science, 125, 427–432. https://doi.org/10.1016/j.procs.2017.12.056
7. Singh, S., & Kaur, P. (2019). Review on bio-inspired cryptographic algorithms. Journal of Network and Computer Applications, 133, 50–64. https://doi.org/10.1016/j.jnca.2019.01.007
8. Qi, X., Wei, X., & Zhang, Y. (2011). A new DNA cryptography method based on dynamic key and encryption. Optik, 122(21), 1961–1965. https://doi.org/10.1016/j.ijleo.2011.01.001
9. Patidar, S., & Jain, V. (2017). Hybrid cryptography: New frontier of secure communication. Journal of Emerging Technologies in Web Intelligence, 9(3), 117–123. https://doi.org/10.12720/jetwi.9.3.117-123
10. Sharma, A., & Kumar, R. (2015). A secure data communication using DNA

cryptography. Procedia Computer Science, 48, 119–124. https://doi.org/10.1016/j.procs.2015.04.163

11. Bashash, M., & Sadkhan, S. (2020). Bio-inspired computing in cryptography: A comprehensive review. Journal of Information Security, 11(2), 67–80. https://doi.org/10.4236/jis.2020.112005
12. Lin, Y., Zhang, Q., & Song, J. (2021). DNA-based cryptographic algorithms: A state-of-the-art review. Journal of Computational Biology, 28(3), 311–327. https://doi.org/10.1089/cmb.2020.0512
13. Alghazzawi, D. M., & Rassam, M. A. (2020). DNA-based encryption techniques: A systematic review. Journal of King Saud University – Computer and Information Sciences, 32(5), 552–562. https://doi.org/10.1016/j.jksuci.2018.09.007
14. Amodio, A., Quarta, G., & Re, C. (2020). Hybrid DNA encryption: Combining modern cryptographic approaches with DNA storage techniques. Biosystems, 199, 104274. https://doi.org/10.1016/j.biosystems.2020.104274
15. Al Hasani, H., & Hammad, M. (2021). A DNA cryptography-based approach for secure image transmission. Journal of Information Security and Applications, 58, 102811. https://doi.org/10.1016/j.jisa.2020.102811
16. Heider, D., & Barnekow, A. (2007). DNA-based watermarks using the DNA-Crypt algorithm. BMC Bioinformatics, 8, 176. https://doi.org/10.1186/1471-2105-8-176
17. Tsiatsis, V., & Stojmenovic, I. (2005). Secure hybrid cryptographic techniques for networks. Wireless Communications and Mobile Computing, 5(3), 269–279. https://doi.org/10.1002/wcm.318
18. Garg, D., & Kumar, R. (2019). An efficient image encryption scheme using DNA cryptography and chaos. Multimedia Tools and Applications, 78(1), 1039–1065. https://doi.org/10.1007/s11042-018-6235-z
19. Amiri, M., & Zarei, S. (2020). DNA steganography: Hiding digital data in DNA sequences. Expert Systems with Applications, 140, 112897. https://doi.org/10.1016/j.eswa.2019.112897
20. Liu, X., Luo, Z., & Qian, X. (2016). Image encryption based on DNA sequence operation and chaotic systems. Multimedia Tools and Applications, 75(23), 16069–16085. https://doi.org/10.1007/s11042-015-2807-5
21. Clark, D., & Essex, A. (2011). Cryptographic DNA sequences: Theoretical foundations and practical applications. Future Generation Computer Systems, 27(1), 118–129. https://doi.org/10.1016/j.future.2010.06.012