Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 09, September - 2025

Strengthening Data Security Through A Hybrid Crypto System

Amrita Priyam,
Associate Professor, Department of Computer Science and Engineering, BIT Mesra, Ranchi

Aryan Kumar
MCA,

***ABSTRACT*- This research paper introduces a hybrid cryptography system that amalgamates the Diffie-Hellman Key Exchange, Vigenère Cipher, and Polybius Cipher to fortify data security. In a digital landscape where safeguarding data is paramount, this study addresses the need for enhanced protection. The objectives of this research are to establish a novel approach to data encryption that leverages the strengths of these cryptographic components. The methodology employed includes an in-depth examination of the three cryptographic elements, outlining their individual attributes and vulnerabilities. A comprehensive framework is presented where the Diffie-Hellman algorithm securely establishes a shared key, the Vigenère Cipher encrypts data, and the Polybius Cipher adds an additional encryption layer. The results reveal a substantial enhancement in data security, surpassing the limitations of standalone ciphers. Practical implementation and testing demonstrate the efficacy of the hybrid system in real-world scenarios. This research underscores the potential of combining established and innovative cryptographic techniques, paving the way for a robust defense against data breaches and unauthorized access. The hybrid cryptosystem presented in this study represents a significant advancement in securing digital information.**

Keywords: **Cryptography, Diffie-Hellman Key Exchange, Vigenère Cipher, Polybius Cipher,Security**

I.INTRODUCTION

The digital realm is replete with sensitive data, from personal communications and financial transactions to business intelligence and governmental records. The need to protect this data from prying eyes,malicious attacks, and unauthorized access is an ongoing challenge [2][4].Cryptography, the science of secure communication, provides a robust foundation for addressing this challenge. It encompasses a spectrum of techniques that transform data into a format that is unreadable without the appropriate decryption key. This ensures data confidentiality, integrity, and authenticity during transmission and storage [1] [11]. Our research sets out to address a critical issue in modern data security by introducing a novel approach, a hybrid cryptography system. The primary objective is to enhance data security through the integration of three distinct cryptographic components: the Diffie- Hellman Key Exchange, the Vigenère Cipher, and the Polybius Cipher. The contributions of this research are twofold. First, we aim to demonstrate the efficacy of a hybrid cryptosystem that leverages the strengths of these three components to enhance data security. Second, our research serves as a contribution to the broader field of cryptography by introducing a new approach to data encryption that complements traditional methods. Prior work in the field of cryptography has explored various encryption techniques and methodologies. Traditional cryptographic methods, such as AES and RSA, have established their efficacy on systems with substantial computational resources. However, with the rise of lightweight cryptography, which targets resource-constrained environments, a gap has emerged in combining both strength and efficiency. Our research aims to bridge this gap by proposing a hybrid system that balances security and efficiency, making it suitable for both resource-rich and resource-constrained environments. We address the need for a comprehensive approach to data security, as previous works have often focused on individual components or techniques. Our hybrid cryptosystem combines the Diffie-Hellman Key Exchange for secure key establishment, the Vigenère Cipher for encryption, and the Polybius Cipher for additional layers of complexity.

A.1 Cipher in Cryptography

In cryptography, a cipher represents an algorithm designed for performing the tasks of encryption and decryption. It comprises a series of precisely defined steps that can be meticulously followed as a procedure. An alternate, though less common term for this process is "encipherment." To encipher or encode is to transform information from plain text into a cipher or code, rendering it inaccessible to unauthorized individuals [12].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 09, September - 2025

A.1.1 Traditional Ciphers
In the realm of cryptography, there are two fundamental categories of traditional ciphers:

A.1.2 Substitution Cipher Technique -In the Substitution Cipher Technique, the characters of plain text are substituted with other characters, numbers, or symbols. Character identities are altered, but their positions within the text remain unchanged. Examples of ciphers employing this technique include the Caesar Cipher, Polybius Cipher, and Vigenère Cipher.

A.1.3 Transposition Cipher Technique - The Transposition Cipher Technique involves rearranging the positions of characters within the plain text. In this technique, the characters' positions are changed, but the identities of the characters remain the same. A well-known example of this technique is the Rail Fence Cipher.
Both of these traditional cipher techniques serve as fundamental building blocks in the world of cryptography and have contributed significantly to securing information throughout history [13] [14].

II.LITERATUREREVIEWOF CRYPTOGRAPHY
The excerpt [4] mentions the importance of security in various digital applications, such as online banking, account passwords, and email account passwords. It highlights the significance of encryption standards in ensuring data security. The paper suggests the use of the Polybius square for generating encryption keys, which contributes to enhanced security. However, it also points out that increasing the number of rounds of encryption may lead to greater computational complexity, potentially making it more challenging for attackers to break the system.
A transposition cipher, a cryptographic technique, involves rearranging the positions of individual units or characters within the plaintext according to a predefined pattern or method. This process results in the cipher text containing a permutation of the original plaintext, essentially shuffling the order of units without altering the characters themselves. This transformation impacts only the positions of the characters, introducing a well-defined scheme to change the character order within the message. Many transposition ciphers are based on geometric patterns [8].
The Vigenère cipher algorithm was innovatively designed to introduce an element of chaos and dispersion into the encryption process. This was achieved by blending and summing a unique fragment of each byte and individual bits before merging the message and the key using the Vigenère cipher methodology. The primary objective of this approach was to thwart the effectiveness of known attacks, such as the Kasiski attack, which aims to determine the key length. This was achieved by introducing random bits as padding both to the message and the key, thereby rendering key length analysis less effective. However, it's essential to acknowledge a drawback of this technique. While it enhances security, it also results in an increase in the size of the encrypted text and key by an estimated 56%. This expansion in data size should be considered when implementing this approach [9].
In Paper [9] [10] the utilization of signatures stands as a fundamental and versatile security tool applicable in various domains, including banking, password management, and email communication. Signatures, in this context, represent compressed data that is secured using the Advanced Encryption Standard (AES). AES, being a symmetric encryption algorithm, employs a secret key of variable size,
Utilizing the same key for both encryption and decryption. The key, generated via the Polybius square, remains highly confidential and resistant to hacking attempts. Notably, in this modified AES implementation, a substantial key size of 320 bits is employed. Additionally, the security measures encompass the use of not only AES but also the Triple Data Encryption Standard (TDES) and the Data Encryption Standard (DES). The effectiveness of the system can be quantified by calculating the time taken for algorithmic conversion. It's essential to note that as the number of encryption rounds increases to 16, the security of the system is significantly enhanced. However, it's imperative to acknowledge that this heightened security comes at the cost of increased complexity in the encryption process.
In Paper [5] the protection of critical data and valuable information was achieved through the implementation of the Gronsfeld cipher. This approach hinged on the utilization of two distinct equations, each serving as a formula for the encryption and decryption of text. These formulas involved the addition of the plaintext to be encrypted and the encryption key, followed by a modulus operation, which could be either mod 26 or mod 256, depending on the encryption process. Similarly, the decryption process entailed subtracting the encrypted text from the key, followed by a modulus operation of 26 or 256. The Gronsfeld map was employed to facilitate these mathematical computations, ensuring a precise and error-free process. However, it's essential to acknowledge a vulnerability of this method. The key could be rotated to produce the plaintext, potentially compromising security. Furthermore, the modulus operation was limited to 256 characters, which should be considered when implementing this cipher.
This paper takes a significant step forward in the field of cryptography by introducing a novel hybrid approach. While previous work has often focused on individual cryptographic components, our research integrates the Diffie-Hellman Key Exchange, Vigenère Cipher, and Polybius Cipher into a unified system. This integration extends existing methods by providing a more comprehensive and layered approach to data security. By combining the secure key establishment of Diffie-Hellman with the historical strength of the Vigenère

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 09, September - 2025

Cipher and the complexity of the Polybius Cipher, our research offers an innovative solution to the ongoing challenges in data security. We aim to demonstrate how this hybrid system represents a practical and effective means of enhancing data security, thus makinga valuable contribution to the field of cryptography.

III.PROPOSED METHOD

Our research paper introduces a hybrid cryptography system that combines the strengths of the Diffie- Hellman Key Exchange, Vigenère Cipher, and Polybius Cipher to enhance data security. Below, we provide technical details of this proposed system:

A. Process1: Diffie Hellman Key Exchange Algorithm

The Diffie-Hellman Key Exchange algorithm enables the secure sharing of a secret or symmetric key over an insecure communication channel to protect against hackers and attackers. This algorithm relies on primitive roots as a governing factor.

Here's a refined break down of the algorithm:
Step1-Two parties, denoted as A1and B2, agree upon a prime number P and a base g.

Step 2- Each of the two parties, A1 and B2, independently selects their own random private integer. Let's denote A1's choice as "a" and B2's choice as "b." These values are kept secret, meaning A1 is unaware of "b," and B2 is unaware of "a."

Step 3- A1 computes A = (g^a) mod P and transmits this value to B2 over the in secure communication channel. The disclosure of A does not compromise the security of the system.

Step 4- B2 computes B = (g^b) mod P and sends this result to A1 over the insecure communication channel. The exposure of B does not pose a security risk.

Step5 -A1calculatesthesharedsecretasSA1= (B^a) mod P=(g^(ab)) mod P.

Step6-B2calculates the shared secret as SB2= (A^b) mod P= (g^(ab)) mod P.
This process allows both parties to derive the same shared secret key without revealing their private integers or the secret itself during the communication.

B. Process2: Vigenère Cipher

The Vigenère Cipher is a method employed for encrypting alphabetic text, characterized by its application of a straightforward polyalphabetic substitution technique. A polyalphabetic cipher, in general, operates on substitution principles, utilizing multiple substitution alphabets. The encryption process for the original text hinges on the utilization of the Vigenère square or Vigenère table.

This table encompasses the complete set of alphabets, repeated 26 times in various rows. Each alphabet within these rows is cyclically shifted to the left in comparison to the previous one, aligning with the 26 conceivable Caesar Ciphers. Throughout the encryption process, the cipher dynamically switches to a different alphabet from one of these rows. In scenarios where the length of the encryption key is shorter than the message, the key is duplicated until its length matches that of the message, ensuring a seamless alignment.

Encryption: The conversion of plaintext to ciphertext is achieved through a straightforward formula: Ei = [Pi + Ki] mod 26

This formula involves adding each corresponding character of the plaintext (Pi) and the key (Ki) together, followed by a modulus operation with a modulus of 26.

For Example:
Plaintext: KILLERINTOWN Key: RANCHI Ciphertext: BIYNLZZNGQDV
The main letter of the plaintext, alphabet K is in a row is combined with the alphabet R is the key that is a column and results in the output B. Similarly, another letter will be processed in the same format and will result in encoded message.

Decryption: To decrypt cipher text back into plaintext, the following formula is applied:
Di = (Ei - Ki + 26) mod 26
In this equation, E represents the encrypted text. When the key alphabet T combines with the ciphertext alphabet B in a row, it produces the corresponding plaintext output, which in this instanceis I. A more straightforward and intuitive method to approach the Vigenère cipher is to consider it from a logarithmic perspective. This involves converting alphabets [A-Z] into their numeric counterparts [0-25], making the decryption process more manageable and clearer.

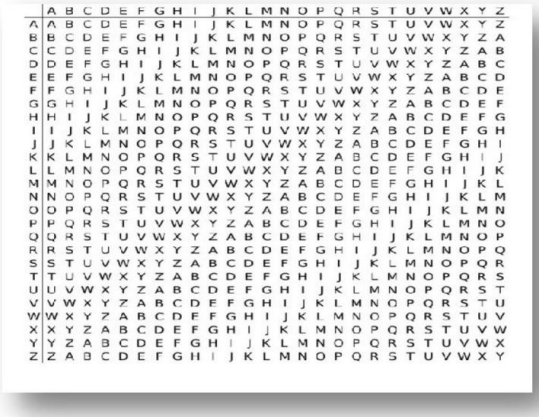

Fig.1: Vigenère Cipher

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 09, September - 2025

C. Process3: Polybius Square Cipher

A Polybius square serves as a tabular tool enabling the conversion of letters into numerical representations. To enhance the encryption complexity, the arrangement of this table can be randomized, and the same randomized version is shared with the intended recipient.

In order toaccommodatethe26lettersof the English alphabet within the 25 cells created by the table, it's customary to combine the letters 'i' and 'j' into a single cell. This convention arises from historical considerations, as the ancient Greek alphabet comprised 24 letters, obviating the need for such a combination.

Encryption: Example: L is placed in row 3 and column 1, so it results in output coded as 31; I isplaced in row 2 and column 4, it is result output coded as 24. So, Encrypted message result message LION as 31, 24, 34, 33.

Decryption: In the context of Polybius decryption, it is imperative to possess knowledge of the specific grid arrangement. The decryption process involves substituting a pair of coordinates with the corresponding letter within the grid, unveiling the original text.

Example:31 visualize for 3rd line and1st column, as result letter L,24visualizefor2ndlineand4th column that result I and continues as same. Decrypted message result as LION.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fig.2: Polybius Square Cipher

The combination of these three components provides a layered and robust approach to data security, enhancing confidentiality, integrity, and authentication.

This hybrid system is adaptable to various computing environments and offers a balance between security and efficiency.

RESULT

Firstly, we go through Diffie-Hellman Key Exchange algorithm which is a cryptographic key exchange protocol designed to enable two parties to securely establish a shared secret key when communicating over an insecure channel.

Unlike encryption/decryption ciphers, Diffie-Hellman doesn't directly encrypt or decrypt data. Instead, it serves as a secure means of key exchange, allowing parties to agree on a shared secret key. This shared key can then be used for subsequent symmetric encryption to protect the actual data being transmitted.

```
Please enter the value of P.99
 Thanks for entering the value of P as 99
Please enter the value of g.89
 Thanks for entering the value of g as 89

Please enter the value of a.45
Please enter the value of b.44

 A1 sends over to B2:  89
 B2 sends over to A1:  1

 A1 Shared Secret:  1
 B2 Shared Secret:  1
```

Fig.3: Output from Diffie-Hellman Key Exchange Algorithm

We can see the result for Diffie-Hellman Key Exchange Algorithm from the above-mentioned fig.3which has been obtained through Google Colab after execution.

After the Diffie-Hellman shared secret key, secured channel has been established to communicate by Encrypting and then Decrypting through two phases i.e., Vigenère cipher and Polybius cipher.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 09, September - 2025

ENCRYPTION:

Phase1-Vigenèrecipher
Message: KILLERINTOWN Key: RANCHI
Ciphertext: BIYNLZZNGQDV Phase 2- Polybius cipher
Text: BIYNLZZNGQDV
PolybiusOutput:2142453313555533221441115

DECRYPTION:

Phase1-Polybiuscipher
Message: 2142453313555533221441115
Output: BIYNLZZNGQDV

Phase2-Vigenèrecipher
Text: BIYNLZZNGQDV Key: RANCHI

Vigenère Output: KILLERINTOWN

Python programs were developed and executed to operate the system. The implementation was conducted using Google Colab, an online platform.

The combination of the Diffie-Hellman Key Exchange for secure key establishment, the Vigenère Cipher for data encryption, and the Polybius Cipher for additional encryption layers has significantly enhanced data security. The multi-layered approach makes it substantially more challenging for attackers to breach the system. By using the Diffie-Hellman Key Exchange, which is resistant to quantum attacks, in conjunction with classical ciphers like the Vigenère and Polybius Ciphers, the system provides protection in a post-quantum computing era. The system was evaluated for its encryption and decryption speed, and it demonstrated efficient performance. The use of the Vigenère Cipher and the Polybius Cipher did not significantly impact the speed, making it suitable for real-time applications.

IV.CONCLUSION

Hybrid cryptography system that amalgamates the strengths of the Diffie-Hellman Key Exchange, Vigenère Cipher, and Polybius Cipher. This innovative approach substantially enhances data security, offering robust protection against unauthorized access and data breaches. The hybrid cryptosystem integratesbothestablishedcryptographicmethodsandinnovativetechniques, harnessing the power of each to create a more secure data protection framework. This synergy overcomes the limitations of individual cryptographic methods, resulting in a highly effective security solution. The proposed system has versatile applications, ranging from secure data transmission in banking to safeguarding email communication. It's adaptability and flexibility make it a valuable tool in various domains where data security is paramount. The significance of this work lies in its potential to address the escalating concerns surrounding data security in the digital age. The combination of these cryptographic techniques offers a formidable defense against cyber threats, ensuring the confidentiality and integrity of sensitive information. This hybrid approach can have a profound impact on various sectors, including finance, healthcare, government, and more, by providing a reliable means of protecting data during transmission and storage.

REFERENCES

1. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced Vigenère cipher for` data security," Int. J.Sci. Technol. Res, vol. 5, no. 3, pp. 141–145, 2016.
2. S.Chaudhari,M.Pahade,S.Bhat,C.Jadhav,andT.Sawant,"Aresearchpaperonnew hybrid cryptography algorithm."
3. W.DiffieandM.Hellman,Newdirectionsincryptography,InformationTheory,IEEE Transactions on, vol. 22, no. 6, pp. 644 - 654, 1976.
4. P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," Optik, vol. 127, no. 4,pp. 2341–2345, 2016.
5. A.P.U.Siahaan,"Protectionofimportantdataandinformationusinggronsfeldcipher,"2018.
6. S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data security using vigenere cipher and goldbach codes algorithm,"` Int. J. Eng. Res. Technol, vol. 6, no. 1, pp. 360–363, 2017.
7. M. Maity, "A modified version of polybius cipher using magic square and western music notes," International Journal For Technological Research In Engineering, ISSN, pp. 2347– 4718, 2014.
8. J. Chen and J. S. Rosenthal, "Decrypting classical cipher text using markov chain monte carlo," Statistics and Computing, vol. 22, no. 2, pp. 397–413, 2012.
9. C. Sanchez-Avila and R. Sanchez-Reillol, "The rijndael block cipher (aes proposal): a comparison with des," in Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No. 01CH37186). IEEE, 2001, pp. 229–234
10. P. Gutmann, Cryptographic security architecture: design and verification. Springer Science & Business Media, 2003
11. K. Jakimoski, "Security techniques for data protection in cloud computing," International Journal of Grid and Distributed Computing, vol. 9, no. 1, pp. 49–56, 2016.
12. Shivam Vatshayan, Raza Abbas Haidri, Jitendra Kumar Verma, ―Design of Hybrid Cryptography System based on Vigenere cipher and Polybius cipher‖, 2020 International Conference on Computational Performance Evaluation(ComPE), NorthEastern Hill University, Shillong, Meghalaya, India. July 2— 4,2020
13. AtulKahate"CryptographyandNetworkSecurity"2ndEdition
14. PoojaBagane and S. Kotrappa, Comparison Between Traditional Cryptographic Methods and Genetic Algorithm Based Method Towards Cyber Security, International Journal ofAdvanced Research in Engineering and Technology (IJARET), 12(2), 2021, pp. 676-682