Cipher X: Design of a Hybrid Cryptography System based on Vigenère and Polybius Ciphers

Preetham K V[1], Anshu Tripathi[2], and Balaram M[3]

[1]Preetham K V, U G Student, BMS College of Commerce and Management

[2]Anshu Tripathi U G Student, BMS College of Commerce and Management

[3]Balaram M, Assistant Professor dept of BCA, BMS College of Commerce and Management

***Abstract*— Cryptography, originating from a Greek word meaning the art of securing information by transforming it into a complex and unreadable format, blends mathematics with computer science. The explosive growth of the Internet has heightened awareness of security vulnerabilities. Despite increasing concerns over internet security, many applications have been developed without adequately addressing fundamental goals of data security: confidentiality, authentication, and integrity.**

As our daily activities increasingly rely on data networks, understanding these security issues becomes increasingly crucial. Cryptography is essential to prevent unauthorized access to data. This paper introduces a novel hybrid security cipher by combining two of the most significant ciphers, namely the Polybius Cipher and the Vigenère Cipher. This hybrid encryption approach offers enhanced security compared to traditional ciphers.

***Index Terms*—Encryption, Cryptography, Polybius Ciphers, Vigene`re Ciphers**

I. INTRODUCTION

In today's global landscape, technological advancements have reached a point where most people prefer using the internet as the primary means to transmit data worldwide. There are numerous ways to communicate information over the internet, such as through emails, chats, and other platforms. The internet enables data exchange to be rapid, efficient, and precise. However, one of the significant challenges associated with transmitting data over the internet is the inherent security risks, including the potential for interception or hacking of sensitive or personal information. Therefore, ensuring data security becomes crucial, as it is paramount during the data transfer process.

Security is a critical concern in open systems, and cryptography plays a significant role in addressing this challenge. Cryptography, an ancient and secure method of information protection in public networks, aims not only to provide confidentiality but also solutions for ensuring data integrity, authentication, and non-repudiation. It encompasses techniques and procedures designed to securely transmit meaningful data and information in such a way that only the intended recipient can access it.

Cryptography systematically hides data and information over communication channels, functioning as an art to conceal information from unauthorized parties. As technology advances daily, the demand for secure data transmission over communication channels intensifies.

Encryption is the systematic process of converting plain text messages into ciphertext. This process requires an automated encryption algorithm and a key to convert the plain text into cipher text. In cryptography, encryption occurs at the sender's end before transmitting the message to the receiver.

Decryption is the reverse systematic process of encryption, transforming encrypted ciphertext back into plaintext. In cryptography, decryption occurs at the receiver's end and involves steps such as a decryption algorithm and a key.

Cryptography is broadly categorized into two classes based on the key used to convert original text into encrypted text: asymmetric key encryption and symmetric key encryption. Symmetric key encryption uses the same key for both encryption and decryption processes. While this approach is simple and powerful, key distribution remains a significant challenge. Asymmetric key encryption, on the other hand, employs two mathematically related keys: a public key and a private key for encryption. The public key is accessible to everyone, but data encrypted using a public key can only be decrypted by the corresponding private key possessed by the specific user, whether as sender or receiver."

This version maintains the technical details while enhancing clarity and readability. Adjustments can be made based on the specific focus and requirements of your research paper.

II. LITERATURE SURVEY

In the realm of web banking security, safeguarding account passwords, email credentials, and other sensitive information necessitates digital media encryption. This underscores the importance of data security and the evolution towards stronger encryption standards. Increasing the number of encryption rounds enhances security against both active and passive attacks by hackers and intruders.

The Caesar cipher, also known as a shift cipher, is one of the simplest and most well-known classical encryption systems. It operates as a substitution cipher where each letter in the plaintext is shifted. For example, with a shift of 2, A becomes C, B becomes D, and so forth. While the Caesar cipher is straightforward, it falls short in modern applications such as the ROT13 and paraphrase systems, lacking robust security and privacy. Named after Julius Caesar, who used it to communicate with his officials, this encryption method requires a numerical value known as a shift, indicating the number of positions each letter in the text is shifted.

The transposition cipher rearranges units of plaintext based on a predefined pattern, altering their position to form the ciphertext. This method involves reordering the sequence of characters or elements within the plaintext, thereby obscuring the original message.

In, an enhanced version of the Vigenère cipher algorithm involves adding a random component to each byte and bit before encryption, which thwarts Kasiski attacks attempting to determine the key length by introducing irregular bits. However, a drawback of this method is that it increases the size of the encrypted text and string by approximately 56%."

"An alternative approach to implementing the Vigenère algorithm involves systematically replacing the key for encryption and diffusion of messages, where primary keys serve as continuations for the exchange of replaced keys in the process. This new technique, presented in this paper, enhances the Vigenère Cipher by incorporating alphanumeric characters and punctuation marks such as colons, commas, semicolons, question marks, underscores, periods, and brackets into the key. This makes it more challenging for both active and passive attacks, broadening the scope so that those familiar with basic cryptography can decode the message.

The internet is recognized as one of the most perilous communication mediums due to its extensive connectivity and openness. Data protection is a fundamental requirement under these conditions. Various security algorithms have been proposed to enhance communication security, each with its strengths and weaknesses. To strengthen encryption algorithms, a hybrid model combining AES and DES cryptographic algorithms has been proposed. Both AES and DES are symmetric key procedures known for their encryption capabilities. Integrating AES and DES provides a robust level of security for encryption. Significant improvements have been observed with this integrated approach."

III. THEORIES

Computers connected to a global network, especially the internet, can become vulnerable to various threats such as viruses and malware when visiting websites. Ensuring security is crucial to prevent data replication, theft, manipulation, detection, and intrusion. The essence of computer security is to safeguard both the computer and its network to ensure the confidentiality and integrity of data within the system.

Computer security encompasses several aspects, including:

- Privacy: Ensuring that confidential information is protected so that unauthorized individuals cannot access it. Encryption technology is commonly used for prevention, ensuring that only the data owner can access the actual information.
- Confidentiality: Enforced through confidentiality agreements or policies that restrict access to certain types of information. This ensures that, when required to disclose information, such as in

legal matters, the information custodian will either provide the requested data or maintain confidentiality for clients.

- Non-repudiation: Ensures that the parties involved in a contract or communication cannot deny the authenticity of their signature on a document or the transmission of a message they initiated. Non-repudiation aims to prevent individuals from later denying actions they have undertaken. For instance, registered mail prevents the recipient from denying receipt of a letter. Similarly, digital signatures on the internet not only confirm that a message or document was electronically signed by its intended creator but also ensure that the signer cannot later deny authorship.
- Authentication: Authentication is a security measure designed to establish the validity and identity of a transmission, message, or originator, or to verify a person's authorization to access specific classifications of information. It ensures that the login user attempting to access the message is verified by checking their details such as username and password. Authentication is critical for information protection.
- Availability: Availability ensures that systems, applications, and data are accessible to users whenever they need them. The most common attack affecting availability is denial of service, where an attacker disrupts access to information, systems, devices, or other network resources. Within an internal vehicular network, denial of service could cause an Electronic Control Unit (ECU) to lose access to necessary operational data, rendering it non-functional or potentially endangering the entire system. To mitigate availability issues, redundancy paths and failover procedures should be integrated during planning. Additionally, intrusion prevention systems that monitor network traffic patterns, detect abnormalities, and block traffic as necessary are essential.

Cryptography: Cryptography consists of four fundamental components:

1. Plaintext: The original readable message.
2. Ciphertext: The encrypted, unreadable message.
3. Key: A crucial element defining cryptographic techniques such as symmetric and asymmetric encryption.
4. Algorithm: A procedural method for executing encryption and decryption

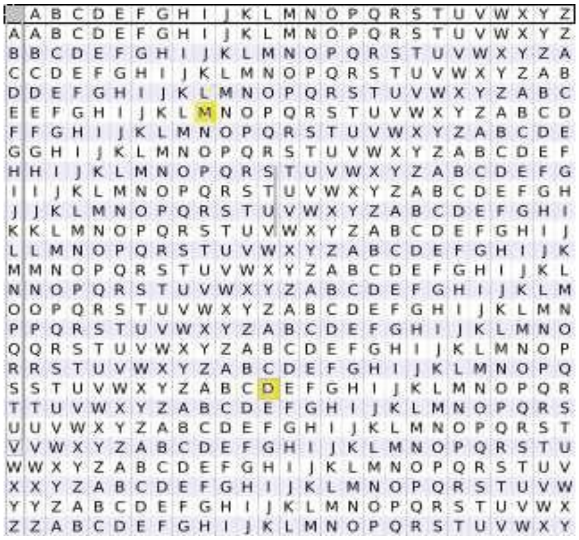
- Authentication: Authentication is a critical security measure aimed at establishing the validity and identity of a transmission, message, or originator, as well as verifying a person's authorization to access specific categories of information. It ensures that the user attempting to access the message is authenticated through verification processes like username and password checks. Authentication plays a pivotal role in safeguarding sensitive information.
- Availability: Availability ensures that systems, applications, and data are accessible to users as needed. Denial of service attacks, which disrupt access to network resources, pose significant threats to availability. For instance, within vehicular networks, denial of service attacks can impair essential Electronic Control Units (ECUs) by preventing access to critical operational data. To mitigate such risks, redundancy strategies and failover mechanisms are essential during system planning. Intrusion prevention systems that monitor and respond to abnormal network traffic patterns also contribute to maintaining availability.

Cryptography: Cryptography consists of four fundamental components:
Plaintext: The original, readable message.
Ciphertext: The encrypted, unreadable message.
Key: Essential for defining cryptographic techniques, including symmetric and asymmetric encryption.
Algorithm: A procedural framework for executing encryption and decryption operations.

Cipher: In cryptography, a cipher (or encipherment) refers to an algorithmic process for encryption or decryption—a methodical sequence of steps designed to transform plaintext into ciphertext and vice versa. This process, also known as encipherment, ensures data security by obscuring information through substitution or transformation. While non-technical usage may blur distinctions between ciphers and codes, cryptography emphasizes their distinct roles:

codes substitute varying-length sequences in output, whereas ciphers generally maintain consistency between input and output lengths.

The Vigenère Cipher is a method of encrypting [A to Z] letters in a message. It employs a basic form of polyalphabetic substitution, a type of cipher that uses multiple substitution alphabets. The encryption process begins by using the Vigenère square table to encapsulate the initial plaintext.



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

Encryption:
The plaintext letter 'S' from the sender's message corresponds to row 'L' from the key column, resulting in the encrypted output 'D'. Similarly, letter 'E' from the plaintext aligns with key 'I', resulting in the ciphertext 'M' where rows represent the plaintext and columns represent the key. This process continues for each letter, following the same method to produce the encoded message. Each plaintext letter (P) and corresponding key letter (K) are combined and then applied modulo 26 to obtain the ciphertext.

Encryption formula: Ei=(Pi+Ki) mod 26E_i = (P_i + K_i) \mod 26Ei=(Pi+Ki)mod26

Using this formula, plaintext letters are converted into ciphertext as illustrated."

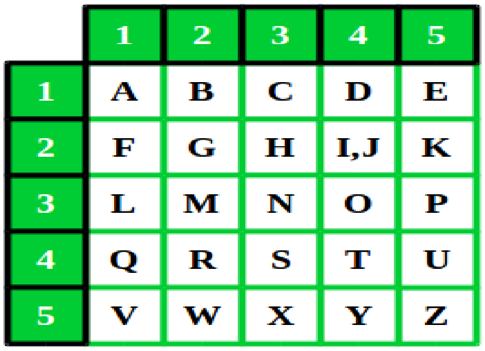
Plaintext: SECURITY
Key: LIONLION
Ciphertext: D M Q H C Q H L

Decryption:
Decryption involves systematically identifying the row in the table corresponding to the key, locating the position of the ciphertext letter within this row, and then using the column label to determine the plaintext output. For example, if the key is represented by row 'L' (from LIONLION) and the ciphertext 'D' appears in the column, decryption yields the plaintext output 'S' found in the row. This process is repeated for each letter, matching ciphertext letters to rows and keys to columns to derive the original plaintext.

An alternative approach simplifies the Vigenère Cipher by converting alphabets [A-Z] into numeric values [0-25]:

Pi=(Ei−Ki+26) mod 26P_i = (E_i - K_i + 26) \mod 26Pi=(Ei−Ki+26) mod26

Using this formula, each ciphertext letter (E_i) is decrypted by subtracting the corresponding key letter (K_i), adding 26 if necessary to ensure non-negative results, and then taking modulo 26 to convert back into plaintext numeric values.



	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

B.Polybius Square Cipher

The Polybius square is depicted as a 5x5 grid filled with letters used for encryption. It functions as a table that allows letters to be converted into numbers. For added complexity, this table can be randomized and shared with the recipient. To accommodate the 26 letters of the alphabet within the 25 cells of the table, the letters 'I' and 'J' are often combined into a single cell. Originally, this was not an issue as the ancient Greek alphabet had 24 letters. Larger tables can be used if a language has more letters in its alphabet.

Encryption Example: For encryption, each letter in the plaintext is located within the Polybius square grid. For instance, 'D' is found at row 1, column 4, resulting in the ciphertext '14'. Similarly, 'O' at row 3, column 3 translates to '34'. Thus, the encrypted message 'DOG' is represented as '14 34 23'.

Decryption Example: Decryption with the Polybius square requires knowledge of the specific grid used. Each pair of digits in the ciphertext corresponds to a row and column in the grid, which is then substituted with the corresponding letter. For example, '12' corresponds to row 1, column 2, resulting in the letter 'B'. '45' corresponds to row 4, column 5, yielding 'U'. This process continues until the entire ciphertext is decrypted. Therefore, decrypting '12 45' results in the plaintext 'BUS'.

IV. METHODOLOGY

The encryption strategy employs a combination of the Vigenère cipher and Polybius Square cipher to enhance security. Initially, the plaintext undergoes encryption using the Vigenère cipher with a randomly chosen key. Subsequently, the resulting ciphertext serves as the key for the Polybius Square cipher. This key is used to encrypt the plaintext once again, producing the final ciphertext. This dual-layered encryption process significantly increases the complexity, making the final ciphertext resistant to conventional cryptanalysis techniques.

Decryption is performed in reverse order by the receiver to retrieve the original message from the sender.

To demonstrate the effectiveness of this algorithm, a software program will be developed using Python coding. Various cryptanalysis techniques will be applied to analyze the ciphertext.

A flowchart illustrating the Hybrid Algorithm is depicted in Fig. 3.

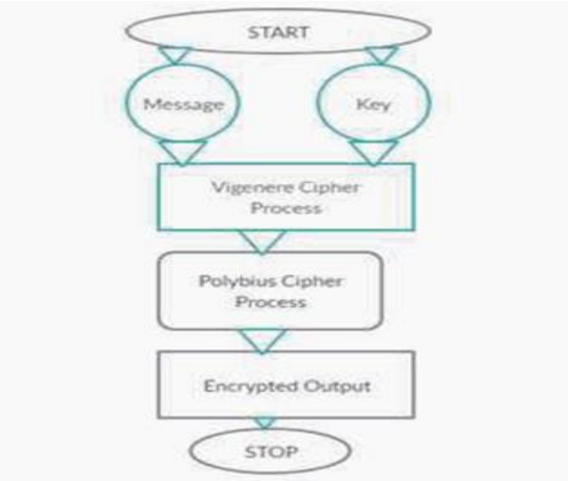


Fig. 3: Flowchart of Hybrid Algorithm

A.Encryption

Phase 1 (Vigenère Cipher)

STEP1: MESSAGE - AMERICANVIRUS
STEP2: KEY- DELHI
STEP3: OUTPUT- DQPYQFEYCQUYD

Phase 2 (Polybius Cipher)

STEP4: TEXT-DQPYQFEYCQUYD
STEP5: OUTPUT-41145345141251453114544541

The output of the encryption process from the sender's perspective is in an alphabetical format. The Vigenère cipher results in ciphertext that appears as distributed, jumbled, and unformatted letters, providing a level of security. However, further enhancing security involves using the output from the Vigenère cipher as input for the Polybius Square cipher. This transforms the ciphertext into numerical format, adding an additional layer of complexity and making it more secure than using either cipher alone.

B. Decryption

Phase 1 (Polybius Cipher)

STEP1: MESSAGE- 41
STEP2: OUTPUT- D

Phase 2 (Vigenère Cipher)

STEP3: TEXT- D
STEP3: KEY- DELHI
STEP4: OUTPUT-A

The output of the encryption process from the sender's perspective is in an alphabetical format. The Vigenère cipher results in ciphertext that appears as distributed, jumbled, and unformatted letters, providing a level of security. However, further enhancing security involves using the output from the Vigenère cipher as input for the Polybius Square cipher. This transforms the ciphertext into numerical format, adding an additional layer of complexity and making it more secure than using either cipher alone.

V. CONCLUSION

Cryptography is widely employed for ensuring data security, privacy, confidentiality, and reliability. Single classic ciphers are often considered simple and vulnerable due to their inherent limitations and predictable patterns. One such cipher, the Vigenère Cipher, although popular, has its drawbacks. To overcome these limitations, an enhanced approach combines the Polybius Cipher with the Vigenère

Cipher, significantly bolstering security against active and passive attacks, as well as Kasiski and Friedman attacks. Cryptanalysis, frequency analysis, man-in-the-middle attacks, fault analysis, and brute-force attacks become challenging due to the use of product tables for encryption. The modified hybrid cipher, integrating elements of the Caesar Cipher and Vigenère Cipher, introduces high complexity, dispersion, distribution, and confusion into the algorithm, rendering it exceptionally robust and difficult to decrypt. Despite the array of cryptographic techniques available, ongoing research is essential for advancing, refining, and enhancing data privacy and security.

In the near future, our aim is to validate this approach through rigorous security and performance analyses on encrypted messages.

REFERENCES

[1] S. Chaudhari, M. Pahade, S. Bhat, C. Jadhav, and T. Sawant, "A research paper on new hybrid cryptography algorithm."

[2] A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced vigene`re cipher for data security," *Int. J. Sci. Technol. Res*, vol. 5, no. 3, pp. 141–145, 2016.

[3] P. Kumar and S. B. Rana, "Development of modified aes algorithm for data security," *Optik*, vol. 127, no. 4, pp. 2341–2345, 2016.

[4] 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.

[5] M. B. Pramanik, "Implementation of cryptography technique using columnar transposition," *International Journal of Computer Application- s*, vol. 975, p. 8887, 2014.

[6] 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.

[7] C. Bhardwaj, "Modification of vigene`re cipher by random numbers, punctuations & mathematical symbols," *Journal of P. Gutmann, Cryptographic security architecture: design and verifica- tion. Springer Science & Business Media, 2003.*

[8] *S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data security using Vigens're cipher and Goldbach codes algorithm," Int. J. Eng. Res. Technol, vol. 6, no. 1, pp. 360–363, 2017.*

[9] *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.*