Model of Cryptography system by using Vigenere Cipher and Polybius Cipher

Amita V. Shah[1], Pooja Shah[2]

[1]Ph.D. Scholar, Computer/IT Engineering, Gujarat Technological University, Gujarat, India
[2]Assistant professor, Indus University, Gujarat, India

***Abstract*: Cryptography, derived from a Greek word, is the art of safeguarding information by transforming it into an intricate and unreadable format. It encompasses both mathematics and computer science. The exponential growth of the Internet has raised awareness about concerns related to privacy and uncertainty. Despite security being a significant concern over the internet, numerous applications have been developed and designed without considering the fundamental objectives of data security, namely confidentiality, authentication, and protection. As our daily activities increasinglyrely on data networks, understanding these securityissues andchallenges becomes crucial. Cryptography is necessary to prevent unauthorized access to data by undesirable users or individuals. This paper presents a novel hybrid security cipher that combines two vital ciphers: the Polybius Cipher and the Vigenère Cipher. This hybrid encryption cipher offers enhanced security compared totraditional ciphers.**

***Index Terms*: Encryption, Cryptography, PolybiusCiphers, Vigenere Ciphers**

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 10, Issue 6, Nov-Dec 2022

I.INTRODUCTION

In the current global landscape, technological advancements have reached a point where the majority of people prefer using the internet as the primary means of transmitting data worldwide. There are numerous methods available to convey information through the internet, including emails, chats, and more. The internet facilitates quick, seamless, and accurate data exchange. However, one of the main challenges associated with transmitting data over the internet is the inherent "security risk," wherein personal or confidential information can be compromised or hacked through various means. Consequently, it becomes crucial to prioritize data security, as it represents one of the most significant factors requiring attention during the data transfer process [1].

Cryptography plays a significant role in ensuring security within open systems. It is an ancient and secure method of protecting information in public networks. However, the purpose of cryptography extends beyond confidentiality and also provides solutions for various issues such as data integrity, authentication, and non-repudiation [2]. The term cryptography refers to the encapsulation and development of techniques that enable the transmission of valuable information and data in a secure format, ensuring that only the intended recipient can access and decipher this information [2].

Cryptography is an art form that involves systematic techniques and procedures to conceal data and information transmitted over communication channels. Its primary objective is to keep the data hidden from unauthorized parties. With the continuous advancement of technology, the demand for data security over communication channels has significantly increased.

Encryption is a systematic procedure defined as the conversion of plain message text into ciphertext. The encryption process requires a programmed encryption algorithm and a key to convert the plain message text into cipher [3]. In the cryptography system, encryption is performed at the message sender's side. Before sending the message to the receiver, encryption is carried out by the sender to secure the content.

Decryption is the reverse systematic procedure of encryption. It involves transforming the encrypted ciphertext back into plaintext message. In the cryptography system, the decryption process is performed at the receiver's side. The decryption algorithm and a key are essential components in the decryption procedure, which consists of several steps.

Cryptography is divided into two main classes based on the key used to convert original text into encrypted content. These classes are Asymmetric Key Encryption and Symmetric Key Encryption. In Symmetric Key Encryption, the same key is used for both encryption and decryption processes. This method is simple yet powerful, although the distribution of the key poses a significant challenge. On the other hand, Asymmetric Key Encryption utilizes two mathematically related keys: the Public Key and the Private Key, for encryption. The public key is accessible to everyone, but any data encrypted with a user's public key can only be decrypted using that specific user's private key, whether they are the sender or the receiver.

II. LITERATURE SURVEY

In the security of online banking, account passwords, and email account passwords, there is a need for content protection in digital media [4]. This emphasizes the importance of security and the need for data encryption standards. Increasing the number of continuous encryption rounds enhances security, making it more difficult for hackers, intruders, and software engineers to break through active and passive attacks.

The Caesar cipher, also known as the 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 replaced. For example, with a shift of 2, A would be replaced by C, B would become D, and so on. The encryption method employed by Caesar ciphers is often combined and utilized alongside other encryption techniques such as the Vigenère Cipher. However, the Caesar cipher is easily and quietly broken, particularly in substitution ciphers. In modern applications, it offers no substantial communication security or protection. Despite this, it still finds utility in frameworks like ROT13 and paraphrase systems [5].

The Caesar Cipher's strategy is one of the earliest and simplest encryption techniques. It is a type of substitution cipher, where each letter in a given text is replaced by a letter a fixed number of positions down the alphabet. For example, with a shift of 1, M would be replaced by N, N would become O, and so on. This technique is named after Julius Caesar, who used it to communicate with his officials. To encrypt a given text using this method, we require a whole number known as the shift value, which indicates the number of positions each letter in the text has been shifted down.

The strategy of the Caesar Cipher is one of the earliest and simplest encryption methods. It is a type of replacement cipher, where each letter in a given text is replaced by a letter a fixed number of positions down the alphabet. For example, with a shift of 1, M would be replaced by N, N would become O, and so on. This technique is named after Julius Caesar, who used it to communicate with his authorities. To encrypt a given text, we need a whole number known as the shift value, which indicates the number of positions each letter in the text has been shifted down.

The transposition cipher is an adaptive encryption system and process whereby the positions and locations of units of plaintext are rearranged according to a predetermined structure or model. This transformation ensures that the ciphertext contains a permutation of the plaintext. The location serves as the primary substitution, and it is constantly occupied and subject to pre-arranged movements based on a derived metric graph. This method can be applied to strings or messages provided by the sender [6] [7].

In [8], a modified version of the Vigenère cipher algorithm was developed, introducing scrambling and scattering techniques through the combination and summation of a random component with each byte and bit before the message and string are mixed using the Vigenère cipher system. This approach effectively thwarts the Kasiski attack, which aims to determine the length of the key, due to the inclusion of random padding bits within the message and string. However, the main drawback of this framework is that the size of the mixed text andstring will increase by an estimated 56%.

A different approach to implementing the Vigenère algorithm was introduced, focusing on encryption and diffusion of messages through the regular and systematic replacement of the key. In this strategy, the primary keys serve as a continuation for the exchange of the replaced key during the process [9].

In this paper, a new technique has been introduced, wherein the Vigenère Cipher incorporates alphabetic, numerical, and punctuation marks such as colons, commas, semicolons, question marks, underlines, full stops, and brackets as the key instead of characters. This modification makes it increasingly difficult for active and passive attacks and enhances the spread of the key range. As a result, even individuals with basic knowledge of cryptography can recognize the message [10] [11].

It acknowledges that the internet, due to its extensive connectivity and open nature, is considered one of the most vulnerable communication mediums. Data protection is identified as a fundamental requirement. Currently, various security algorithms have been proposed to achieve communication security. Each of these algorithms has its strengths and weaknesses. To enhance the encryption algorithm's quality, a hybrid model is proposed. The proposed model combines the AES and DES cryptographic algorithms. Both algorithms are symmetric key procedures and are highly capable of encryption. The integration of AES and DES provides a strong level of security for encryption. Significant improvements in results have been observed with the proposed solution [12].

III. THEORIES

If PCs are connected to a global network, particularly the internet, they can become unreliable [2]. Many websites are infected with viruses, malware, or other malicious entities that can steal personal data from a computer. Security is essential to prevent data duplication, theft, unauthorized access, detection, and intrusion. The foundation of computer security is implemented to protect the computer and its network, ensuring the safety and security of data within the system [13].

PC security works and incorporates a few angles, for example:

- **Privacy** is typically associated with confidentiality. The objective is to prevent unauthorized individuals from accessing information and data. Encryption technology can be used to achieve prevention, ensuring that only the data owner can access the true information.
- **Confidentiality** involves a set of rules or agreements that impose restrictions on access to certain types of information. It is typically executed through confidentiality agreements. When requested to disclose someone's wrongdoing, the information custodian must decide whether to provide the requested information or maintain the confidentiality of their clients.
- **Non-repudiation** is the process that ensures the inability of individuals involved in an agreement or communication to deny the authenticity of their signature on a document or the sending of a message that they initiated. The term "repudiation" refers to denial.

Over the years, efforts have been made to make repudiation impossible in certain situations. For instance, we may send registered mail to prevent the recipient from denying the delivery of a letter. Similarly, an official document often requires witnesses to sign so that the signatory cannot later deny doing so. On the Internet, a digital signature is used not only to verify that a message or document has been electronically signed by the intended person but also, since a digital signature can only be generated by one person, to ensure that an individual cannot later deny providing the signature.

- **Integrity**, Data integrity refers to the reliability and consistency of data throughout its lifecycle. It encompasses the state of the data, such as whether it is valid or invalid, as well as the processes involved in ensuring and safeguarding the authenticity and accuracy of the data.
- **Authentication** is a security measure designed and implemented to establish the legitimacy and uniqueness of a transmission, message, or originator. It serves as a means of verifying a person's authorization to access specific categories of information. The authentication process begins by verifying the login user's credentials, such as username and password. Once the details are checked, access to the system is granted. Authentication is a crucial process for ensuring the protection of information.
- **Availability** ensures that systems, applications, and data are accessible to clients when they need them. The most common attack that affects availability is a denial of service, where the attacker disrupts access to information, infrastructure, devices, or other network resources. In an internal vehicular network, a denial of service could result in an Electronic Control Unit (ECU) being unable to access the necessary data to function, rendering it non-operational or even causing the system to enter a dangerous state. To mitigate availability issues, it is crucial to incorporate redundancy paths and failover procedures during the planning phase. Additionally, intrusion prevention systems should be implemented to monitor network traffic patterns, detect abnormalities, and block network traffic when necessary.

Cryptography has four fundamental parts, for example:

1) The plaintext is defined as a message that can be perused.
2) The ciphertext is a random unscripted, disputed and an informal message that is unable to be

perused.

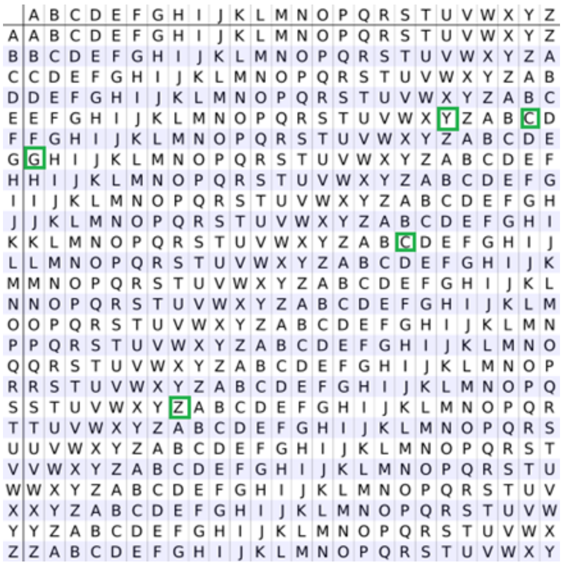
3) The key is a vital aspect for defining the cryptographic technique such as symmetric and asymmetric.

4) An algorithm is a procedural solution to execute encryption and decryption and algorithms in the system.

Cipher: In cryptography, a cipher (or cipher) is an algorithm that performs encryption or decryption (unscrambling) through a series of well-defined steps. An alternative term, less commonly used, is encipherment. To encipher or encode is to convert data from plaintext into cipher or code. In non- technical usage, a 'cipher' is the same thing as a 'code'; however, the concepts are distinct in cryptography. In traditional cryptography, ciphers were distinguished from codes. Codes typically substitute varying length sequences of characters in the output, while ciphers often substitute an indeterminate number of characters from the input. There are exceptions, and some cipher systems may use potentially more or fewer characters in the output compared to the number in the input.

A. Vigenère Cipher

The Vigenère Cipher is a strategy for scrambling letters [A to Z] in a message. It employs a simple form of polyalphabetic substitution. A polyalphabetic cipher is a known cipher that relies on substitution, using multiple substitution alphabets. The encryption of the original plaintext is done using the Vigenère square table.



	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

Fig. 1: Vigenère Square Table

Encryption: The key (K) and plaintext (P) are combined using a specific rule. For example, if the plaintext letter is S and the key letter is L, the resulting letter is D. This process is repeated for each letter in the message. Each letter is matched with a corresponding letter from the key, and the resulting letter is the encoded letter. The combination of rows and columns determines the encoded message. The plaintext and key letters are added together using modulus 26.

The plaintext (*P*) and key (*K*) are added to modulus of 26.

$$Ei = [Pi + Ki]\ modulus(26) \qquad (1)$$

Using (1), one may convert plaintext into ciphertextas shown below.

Plaintext: SECURITY

Key : LIONLION

Ciphertext: D M Q H C Q H L

Decryption: The decryption process involves following a systematic approach. We start by identifying the row in the table that corresponds to the key letter. Then, we locate the position of the ciphertext letter within this row. The column's namein which the ciphertext appears represents the corresponding plaintext letter.

For example, if the key is L (from LIONLION) and the ciphertext letter is D, we find the row L and locate the column where D is located. The corresponding plaintext output in this case is S. We repeat this process for each letter in the ciphertext, matching rows and columns to determine the plaintext output.
A simpler and easier approach is to convert the Vigenère cipher into a logarithmic view by assigning numeric values to each alphabet from A toZ, represented as 0 to 25.

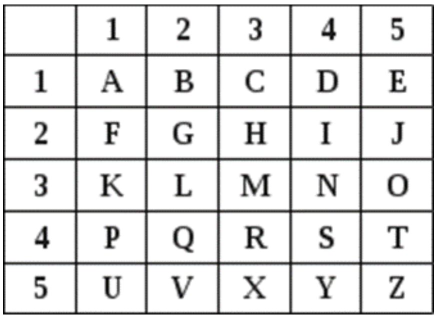
$$Di = (Ei - Ki + 26)\ modulus 26 \qquad (2)$$

Polybius Square Cipher:
The Polybius square is a 5x5 grid containing letters for encryption. It serves as a table for converting letters into numbers. To increase the complexity of encryption, this table can be randomized and shared with the recipient. In order to accommodate the 26 letters of the alphabet within the 25 cells of the table, the letters 'I' and 'J' are usually combined into a single cell. Originally, this was not an issue as the ancient Greek alphabet consisted of 24 letters. A larger table could be used if a language has a larger alphabet size.

Encryption: Example: The letter 'D' is located in row 1 and column 4 of the Polybius square, resulting in the output code of 14. Similarly, the letter 'O' is located in row 3 and column 3, resulting in the output code of 34. Therefore, the encrypted message"DOG" is represented as the sequence of codes: 14,34, 23.
Decryption: Polybius decryption consists of substituting a pair of coordinates with the corresponding letter in the grid. To perform decryption, one must have knowledge of the specificgrid used.
Example: Decrypted message results in "BUS" by visualizing the coordinates 12, which corresponds to the letter B in the 1st row and 2nd column, and 45, which corresponds to the letter U in the 4th row and 5th column.

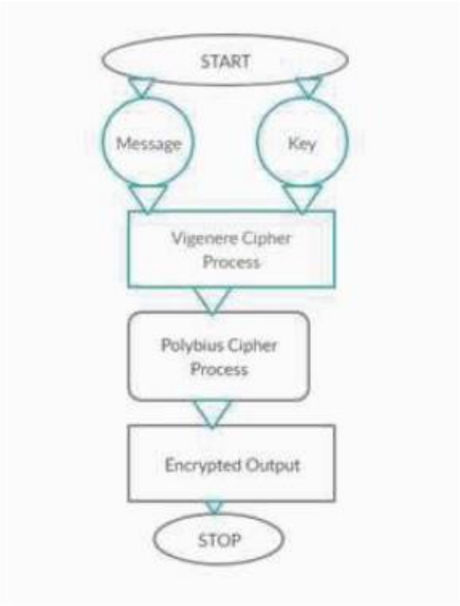
IV: METHODOLOGY

The encryption process utilizes a combination of Vigenère cipher and Polybius Square Cipher. Initially, the ciphertext is processed using the Vigenère cipher, with a randomly chosen key. At the end of this process, the resulting ciphertext becomes the key for the Polybius Square Cipher. This key is then used to process the plaintext message, resulting in the final ciphertext. This encryption method makes the final ciphertext increasingly difficult to break using existing cryptanalysis techniques.



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

Decryption will be done by the receiver in reverse order for retrieval of a message from the sender.
A product program will be composed to exhibit the viability of the calculation utilizing python coding and different cryptanalysis techniquewill be performed on the ciphertext.
A flowchart depicting the Hybrid Algorithm is as shown following figure.



Flow chart of Hybrid algorithm.

A. *Encryption:*

Phase 1 (Vigenère Cipher)

STEP1: MESSAGE – AMERICANVIRUS

STEP2: KEY-DELHI

STEP3: OUTPUT-DQPYQFEYCQUYD

Phase 3 (Polybius Cipher)

STEP4: TEXT-DQPYQFEYCQUYD

STEP5: OUTPUT-41145345141251454454 1

We can see that the output is in a NUMERICAL format, whereas the sender has sent it in an ALPHABETICAL format. Even the output of the Vigenère cipher is in a distributed, jumbled, and unformatted ALPHABETS, which provides some level of security. However, by treating the Vigenère cipher outputs as the input for the Polybius cipher and converting them into a numerical format, we can achieve greater security and complexity compared to the use of single ciphers.

B. Decryption

We can see that the decode output is obtained by reversing the process, first through the Polybius cipher and then the Vigenère cipher. This approach adds complexity for intruders, attackers, and hackers, making it difficult for them to replicate, copy, or harm the system through various types of active and passive attacks. One of the biggest advantages of this process is its potential use in the military, police systems, and secure message communication and transmission.

Hence, the implementation of the Hybrid cipher process can be seen in the systematic flow of the Encryption and Decryption process, which incorporates the Polybius and Vigenère cipher systems. A Python program is written for the implementation of the Hybrid cipher.

IV. CONCLUSION

Cryptography is a widely used technique to ensure the security, privacy, confidentiality, and reliability of data. However, single classic ciphers have their limitations and vulnerabilities, making them less secure. One such cipher is the Vigenère Cipher, which has its drawbacks. To overcome the limitations of the Vigenère cipher, a new technique has been introduced, which combines the Polybius cipher and Vigenère cipher. This hybrid approach offers enhanced security against various attacks, including active, passive, Kaiseki, and Friedman attacks. The proposed strategy also makes cryptanalysis, frequency analysis, fault analysis attacks, and brute force attacks more challenging due to the use of product tables for encryption. The modified hybrid combination of the Caesar Cipher and Vigenère Cipher results in a high level of complexity, scattering, distribution, and confusion in the algorithm, making it a strong cipher that is difficult to break. While there are many cryptographic techniques available, further attention from the research community is required for the continuous improvement and enhancement of data privacy and security in this field.

In the coming future, our purpose is to approve the proposed approach by executing security attacks and performance analysis on messages.

Phase 1 (Polybius Cipher)

STEP1: MESSAGE -41

STEP2: OUTPUT-D

Phase 2 (Vigenère Cipher)

STEP3: TEXT-D

STEP4:OUTPUT-A

REFERENCES

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

[2] K. Jakimoski, “Security techniques for dataprotection in cloud computing,” *International Journal of Grid and DistributedComputing*, vol. 9, no. 1, pp. 49–56, 2016.

[3] A. A. Soofi, I. Riaz, and U. Rasheed, “Anenhanced vigen`ere cipher for data security,” *Int. J. Sci. Technol. Res*, vol. 5, no. 3,pp. 141–145, 2016.

[4] P. Kumar and S. B. Rana, “Development ofmodified aes algorithm for data security,” *Optik*, vol. 127, no. 4, pp. 2341–2345, 2016.

[5] A. Saraswat, C. Khatri, P. Thakral, P. Biswas *etal.*, “An extended hybridization of vigen´ere and caesar ciphertechniques for secure communication,” *Procedia Computer Science*, vol. 92, pp. 355–360, 2016.

[6] J. Chen and J. S. Rosenthal, “Decryptingclassical cipher text using Markov chainmonte carlo, ”*Statistics andComputing*, vol. 22, no. 2, pp. 397–413, 2012.

[7] M. B. Pramanik, “Implementation ofcryptography technique using columnar transposition,” *International Journal ofComputer Applications*, vol. 975, p. 8887, 2014.

[8] C. Sanchez-Avila and R. Sanchez-Reillol, “Therijndael block cipher (aes proposal): a comparison with des,” in *ProceedingsIEEE 35th Annual 2001 International Carnahan Conference onSecurity Technology (Cat. No. 01CH37186)*. IEEE, 2001, pp. 229–234.

[9] Q.-A. Kester, “A cryptosystem based onvigen`ere cipher with varying key,” *International Journal of Advanced Researchin Computer Engineering & Technology (IJARCET)*, vol. 1, no. 10, pp. 108–113, 2012.

[10] C. Bhardwaj, “Modification of Vigenère cipherby random numbers, punctuations & mathematical symbols,” *Journal ofComputer Engineering (IOSRJCE) ISSN*, pp. 2278–0661, 2012.

[11] F. M. S. Ali and F. H. Sarhan, “Enhancingsecurity of Vigenère cipher by stream cipher,” *International Journal ofComputer Applications*, vol. 100, no. 1, pp. 1–4, 2014.

[12] P. Gutmann, *Cryptographic securityarchitecture: design and verification*. Springer Science & Business Media, 2003.

[13] A. P. U. Siahaan, “Protection of important dataand information using gronsfeld cipher,” 2018.

[14] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, “Data security using vigen`ere cipher and goldbach codesalgorithm,” *Int. J. Eng. Res. Technol*, vol. 6, no. 1, pp. 360–363, 2017.

[15] 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.