IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

# Design of Hybrid Cryptography System based on Vigenere Cipher and Polybius Cipher

**Abhishek Mishra, Abhishek Rai, Dheeraj Gurjar**
Department of Computer Science & Engineering
Dronacharya Group of Institutions, Greater Noida, India

**Abstract:** *The Cryptography is gotten from a Greek word which implies the craft of ensuring data by changing it into a muddled organization and unreadable format. It is a mix of arithmetic and software engineering. The dynamite growth of the Internet has made an expanded familiarity with intrigue uncertainty issues. Even though security is the measure worries over the internet, numerous applications have been created and structured without considering fundamental destinations of data security that is confidentiality, authentication, and protection. As our day by day exercises become increasingly more dependent upon data networks, the significance of an understanding of such security issues and trouble will also increase. To forestall some undesirable clients or individuals to gain admittance to the data, cryptography is required. .This paper introduces a new hybrid security cipher by combining the two most important Ciphers such as Polybius Cipher and Vigenere Cipher. This` hybrid encryption cipher provides greater security as compared to classic ciphers*

**Keywords:** Encryption, Cryptography, Polybius Ciphers, Vigenere Ciphers

## I. INTRODUCTION

In the present direction of the world, the innovations have progressed so much that the vast majority of the people incline toward utilizing the internet as the essential intends to consign data starting with one end then onto the next over the world. There are numerous potential approaches to communicate data utilizing the internet: through messages, talks, and so on. The data change is made very snap, quick and exact utilizing the internet. In any case, one of the primary tests with sending data over the internet is the "security risk" it presents, for example, the individual or privy data can be packed away or hacked from various perspectives. In this way, it turns out to be essential to mull over data security, as it is one of the most vital variables that need consideration during the process of data transfer [1].

Security is a significant factor in the open system and cryptography assumes a significant job in this field. Cryptography is old and made sure about the system of information out in the open system. Be that as it may, the goal of cryptography is utilized not exclusively to give classification, yet in addition to giving arrangements to different issues: data trustworthiness, verification, non-denial [2]. Cryptography is a term defined as encapsulating and contriving techniques which permit important information and data to be sent in a protected structure so that the main individual ready to recover this information is the conscious beneficiary [2].

Cryptography is a systematic technique and procedure to hide the data and information over a communication channel. It is a craftsmanship to hide the data from outsiders. As the innovation grows step by step the need for data security over the communication channel is expanded to a high degree. Encryption is defined as a systematic procedure of changing over plain message text into ciphertext. Encryption process needs any programmed encryption algorithm and a key to change over the plain message text into cipher r [3].

In the cryptography system encryption execute at the message sender side. Encryption executes the message at sender's side before sending it to the receiver. Decryption is an opposite systematic procedure of encryption. It transforms the encrypted ciphertext into a message plaintext. In cryptography system decryption procedure execute at the receiver side. The process of decryption algorithm requires a couple of steps such as - a Decryption algorithm and a key.

Cryptography is extensively isolated into two classes relying on the Key; which is characterized as the guidelines used to change over a unique book into scrambled content: Asymmetric Key Encryption and Symmetric Key Encryption. A symmetric key encryption utilizes a similar key for decryption and encryption processes. This system is a basic yet groundbreaking yet key circulation is the main issue that should be addressed. While asymmetric key encryption utilizes two mathematically related keys: Public Key and Private Key for encryption. The public key is accessible to everybody

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

except the data once encoded by the public key of any client must be decrypted by the private key of that specific client as either sender or receiver

## II. LITERATURE SURVEY

In the security for web keeping money, account passwords, messages account secret word, etc requires content protection in mechanized media [4]. It shows the security besides, pressure for the information with the move encryption standard. The Number of continuous rounds increases the greater security that can be break by active and passive attacks by software engineers, intruders and hackers.

Caesar cipher, otherwise called the shift cipher, is least perplexing and large known old-style encryption systems. It is a sort of replacement cipher in which each letter in the plaintext is supplanted. For instance, with a move of 2, A would be supplanted by C, B would become D, and similarly. The encryption technique system performed by Caesar ciphers is a combination and thoroughly goes together as a disputed and complex growth plan as Vigenere Cipher and to date,` it has advantages in the ROT13 framework and paraphrase system. Similarly, in substitution ciphers, the Caesar cipher is effortlessly and discreetly broken and in present-day structure, the use shows no correspondence security and protection [5].

Caesar Cipher's strategy is one of the soonest and least complex techniques for the encryption method. Its a kind of replacement cipher, i.e., each letter of a given text is supplanted by a letter some fixed number of positions down the letters in order. For instance, with a move of 1, M would be supplanted by N, N would become O, and so on. This technique is named after Julius Caesar, who utilized it to speak with his authorities. Accordingly, to cipher a given text we need a whole number worth, known as a move which demonstrates the quantity of position each letter of the the text has been descended. The transposition cipher is a process and adaptive system of encryption system by which location and position held by units of plaintext are moved by a standard structure or model so that the ciphertext includes a phase of the plaintext. The location is the main substitute that is always occupied and pre location movement by given derived metric graph that can be used by string or message given by the sender [6] [7].

In [8] changed variation of Vigenere cipher algorithm was` derived as scrabbled and scattering is given by combination and summation of a subjective piece to each byte and bits before the message and string are mixed using the system Vigenere cipher. This procedure crashes and burns the so-` called Kasiski attack to find the length of the key because of the padding of the message and string with sporadic bits. The central drawback and nil improvement of this framework are that the size of the mixed text and string will be expanded by approximately calculated 56%.

Another strategy for executing the Vigenere algorithm was` introduced and brought up as through normally and systematically for encryption and diffusion of message need key to be replaced again and again. But here primary keys act as Continuation for exchange of replaced key for the process [9].

New technique has been Introduced in this paper as Vigenere Cipher constitute alphabetic numerical and punctuation marks as colon, comma, semicolon, question marks, underline, full stop and brackets are used as the key instead of character to formed it increasingly hard for active and passive assault and attacks and spreading this spread the rang, so literate people who understand basic of cryptography can recognize the message [10] [11].

It addresses that the internet is one of the most perilous communication medium because of immense association and open system. Data assurance is one of the basic parametric prerequisite. At present different security algorithms are proposed to accomplish security during communication. Every one of them has certain valid statements and certain awful points. To improve the quality of the encryption algorithm they proposed a hybrid model. The proposed model is a blend combination of AES and DES algorithmic cryptographic. The two algorithms are symmetric key procedure and itself they are especially able for encryption. Reconciliation of AES and DES would give a solid degree of security at encryption end. A critical improvement in results has been seen with the proposed arrangement [12].

## III. THEORIES

PCs will be undependable if they are associated with a worldwide system, particularly the internet [2]. The locales visited a great extent have infections, malware or the like that can take singular data from a PC. Security is fundamental to keep up a key good way from data replication, stealing, visualizing, detection and intrusion. The core of PC security is done to guarantee the PC and its system to ensure the data safe and secure inside the system [13].

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

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

- Privacy is usually that is confidential. The fact of the matter is anticipation with the goal that unapproved individuals don't get to information and data. Avoidance is conceivable to utilize encryption innovation, so just the information proprietor can discover genuine information. ▪Confidentiality involves a set of rules or a promise usually executed through confidentiality rule agreements that limit access or places restrictions on certain types of information. It shows when requested to demonstrate somebody's wrongdoing, regardless of whether the information keeper will offer information to the individual who mentioned it or keep up the customers.
- Non-repudiation is the process that sides to the capacity to guarantee that involved with an agreement or a communication can't prevent the realness from securing their mark on an archive or the sending of a message that they started. To disavow intends to deny. For a long time, specialists have looked to make repudiation unthinkable in certain circumstances. We may send enlisted mail, for instance, so the beneficiary can't deny that a letter was conveyed. Thus, an authoritative archive regularly expects observers to mark with the goal that the individual who signs can't deny having done as such. On the Internet, an advanced mark is utilized not exclusively to guarantee that a message or report has been electronically marked by the individual that implied to sign the archive, yet additionally, since a computerized mark must be made by one individual, to guarantee that an individual can't later deny that they outfitted the mark.
- Integrity, Data integrity defines as alludes to the dependability and reliability of data all through its lifecycle. It can portray the condition of your data e.g., substantial or invalid or the process of guaranteeing and protecting the legitimacy and precision of data.
- Authentication is a safety effort planned and processed to build up the legitimacy and oneness of a transmission, message, or pre originator, or methods for checking a persons authorization to get explicit classifications of data. It is done to verify the login user who is trying to log in for the procurement of the message. It checks first the user details for login as username and password. Then after checking the whole details, it allows entering the system. It is an important process for the protection of Information.
- Availability ensures that systems, applications and data are accessible to clients when they need them. The most widely recognized assault that impacts accessibility is disavowal of administration in which the assailant interferes with access to data, framework, gadgets or other network assets. A refusal of administration in an inward vehicular network could bring about an ECU not having the option to access the data expected to work and the ECU could become nonoperational or even most noticeably terrible it could carry the framework to a hazardous state. To keep away from accessibility issues, it is important to incorporate repetition ways and failover procedures in the planning stage, just as to incorporate interruption avoidance systems that can monitor network traffic design, decide whether there is an abnormality and square network traffic when required.

Cryptography has four fundamental parts, for example:

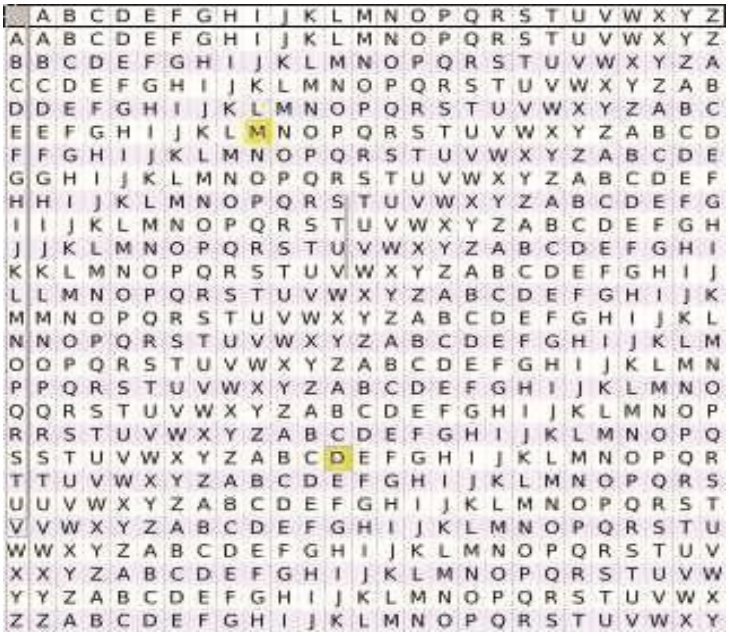
1. The plaintext is defined as a message that can be perused.
2. The ciphertext is a random unscripted, disputed and an informal message that is unable to be perused.
3. The key is a vital aspect for defining the cryptographic techniques such as symmetric and asymmetric.
4. An algorithm is a procedural solution to execute encryption and decryption algorithms in the system.

*Cipher:* IIn cryptography, a cipher (or cipher) is an algorithm for performing encryption or decryption (unscrambling) a progression of very much characterized advances that can be followed as a method. Another option, less regular term is encipherment. To encipher or encode is to change over data from plaintext into cipher or code. In nontechnical use, a 'cipher' is a similar thing as a 'code'; nonetheless, the ideas are unmistakable in cryptography. In customary cryptography, ciphers were recognized from codes. Codes usually substitute differing length arrangement of characters in the yield, while ciphers regularly substitute an unclear number of characters from are input. There are exceptional cases and some cipher systems may use possibly more, or less, characters when yield versus the number that was input.

**A. Vigenere Cipher`**

Vigenere Cipher is a strategy for scrambling [A to Z] letters` message. It utilizes a basic type of polyalphabetic replacement. A polyalphabetic cipher is known cipher that is dependent on replacement, utilizing numerous replacement letter sets .The encapsulation of the first plaintext is finished utilizing the Vigenere square table [14].`

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252



| | 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: Vigenere Square Table`

**Encryption:**

The main letter of the plaintext, alphabet *S* is that is in a row combined with alphabet *L* is the key that is a column, the primarily given letter of the sender and receiver side key that results in the output as *D*. Then *E* is a row and key *I* is a column now it will result as *M* in the crossover of both rows as Message by sender and column as the key. Similarly, other letters will be processed in the same format and will result in encoded message. The plaintext (*P*) and key (*K*) is added to the modulus of 26.

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

$$E_i = [P_i + K_i] modulus (26) \qquad (1)$$

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

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

**Decryption:**

Decryption is resulted by systematically heading off to the row in the table comparing to key, finding the situation of the ciphertext letter that is in this row, and afterward utilizing the column's name as plaintext. As an instance, in row L (from LIONLION) that is key, and the ciphertext appears D in the column, which will result in the plaintext output as S in the row. So, similarly, the other alphabets will be seen in row and column and then the exact plaintext will come as output.

The simpler and easier approach is to view Vigenere log-` arithmically and changing over alphabets [A-Z] into numerically as [0-25].

$$D_i = (E_i - K_i + 26) modulus 26$$

| | 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

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

**B. Polybius Square Cipher**

The Polybius square is shown as a figure of 5x5 grids occupied with letters inside for encryption. Polybius Square is a table that permits somebody to change over letters into numbers. To make the encryption minimal harder, this table can be randomized and imparted to the beneficiary. To fit the 26 letters of the letters in order into the 25 cells made by the table, the letters 'I' and 'J' are generally consolidated into a solitary cell. Initially, there was no such issue because the old Greek letters in order have 24 letters. A table of greater size could be utilized if a language contains a huge number of letters in order [15].

Encryption: Example: D is placed in row 1 and column 4, so it results in output coded as 14; O is placed in row 3, column 3, it is result output coded as 34. So, Encrypted message result message DOG as 14, 34, 23.

Decryption: Polybius decryption requires knowing the grid and consists of a substitution of a couple of coordinates by the corresponding letter in the grid.

Example: 12 visualize for 1st line and 2nd column, as result letter B, 45 visualize for 4th line and 5th column that result U and continues as same. Decrypted message result as BUS.

## IV. METHODOLOGY

The strategy utilizes a combination of Vigenere cipher` and Polybius Square Cipher in its encryption process. The ciphertext will initially be worked on utilizing Vigenere cipher.` A picked key out of arbitrary will start the process. Toward the finish of the process, the subsequent ciphertext then turns into a key for the Polybius Square Cipher process. The key is used to work on the message which is the plaintext to create the last ciphertext. This process will wind up making the last ciphertext progressively hard to be broken utilizing existing cryptanalysis processes.

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 cryptanalysis technique will be performed on the ciphertext. A flowchart depicting the Hybrid Algorithm is as shown in Fig. 3.

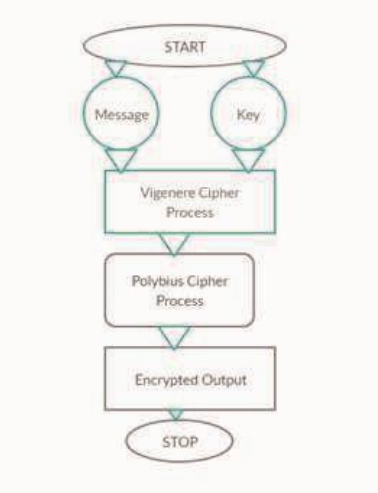



Fig. 3: Flowchart of Hybrid Algorithm

**Encryption**

| |
|---|
| Phase 1 (Vigenere Cipher)` |
| STEP1: MESSAGE - AMERICANVIRUS |
| STEP2: KEY- DELHI |
| STEP3: OUTPUT- DQPYQFEYCQUYD |
| Phase 2 (Polybius Cipher) |
| STEP4: TEXT-DQPYQFEYCQUYD |
| STEP5: OUTPUT-41145345141251453114544541 |

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

We can see output is in a NUMERICAL format where sender has sent as in ALPHABETICAL format. Even the Vigenere cipher result outputs as in distributed, jumbled and` unformatted ALPHABETS which is also secured but again passing that treating Vigenere outputs as Polybius input and` then result in numerical format that makes it greater secure and complex than the use of single ciphers.

***B. Decryption***

| |
|---|
| Phase 1 (Polybius Cipher) |
| STEP1: MESSAGE- 41 STEP2: OUTPUT- D |
| Phase 2 (Vigenere Cipher)` |
| STEP3: TEXT- D |
| STEP3: KEY- DELHI STEP4: OUTPUT-A |

We can see decode output is arriving after reversing the process of through first and foremost Polybius cipher and then Vigenere cipher. This makes complexity for intruders,` attackers and hackers to confuse them and stop them to Replicate, copy, or harm the system through various types of active and passive attacks. The Biggest advantage of this process can be used army, police system, secure message communication and transmission Hence, we can see the implementation of the Encryption and Decryption process of the Hybrid cipher process that flows systematically through Polybius and Vigenere cipher system.` Python Program is written as for the Implementation of Hybrid cipher

## V. CONCLUSION

Cryptography is the generally utilized technique for the security, privacy, confidentiality and reliability of data. Single classic ciphers are cryptographic techniques that are viewed as least complex and most vulnerable because of numerous impediments, restriction, and smooth system. One of the famous ciphers is Vigenere Cipher but it also has few drawbacks. To` conquer the impediments of Vigenere cipher, A new technique` is present an upgraded variant as a combination of Polybius cipher and Vigenere that is a lot more secure against attacks` like Active, passive, Kasiski and Friedman assaults (attacks). Cryptanalysis, recurrence examination, men in middle attacks, frequency analysis, fault analysis attacks, design expectation and brute force attacks on the proposed strategy are likewise much troublesome because of the utilization of product tables for encryption. The altered hybrid combination of the Caesar Cipher and Vigenere Cipher, that's the result in as a high level` of complexity, scattering, distribution, and confusion in the algorithm that creates them making it an exceptionally solid cipher and hard to break. Even though there are numerous cryptographic strategies yet this space still requires genuine consideration of the research network for the up-gradation, refinement and enhancement of data privacy and security. In the coming future, our purpose is to approve the proposed approach by executing security attacks and performance analysis on messages.

## 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 data protection in cloud computing," International Journal of Grid and Distributed Computing, vol. 9, no. 1, pp. 49–56, 2016.

**[3].** A. A. Soofi, I. Riaz, and U. Rasheed, "An enhanced vigenere 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 of modified aes algorithm for data security," Optik, vol. 127, no. 4, pp. 2341–2345, 2016.

**[5].** A. Saraswat, C. Khatri, P. Thakral, P. Biswas et al., "An extended hybridization of vigenere and caesar cipher techniques for secure com-´ munication," Procedia Computer Science, vol. 92, pp. 355–360, 2016.

**[6].** 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.

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

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

**[8].** 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.

**[9].** Q.-A. Kester, "A cryptosystem based on vigenere cipher with varying` key," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 1, no. 10, pp. 108–113, 2012.

**[10].** C. Bhardwaj, "Modification of vigenere cipher by random numbers,` punctuations & mathematical symbols," Journal of Computer Engineering (IOSRJCE) ISSN, pp. 2278–0661, 2012.

**[11].** F. M. S. Ali and F. H. Sarhan, "Enhancing security of vigenere cipher` by stream cipher," International Journal of Computer Applications, vol. 100, no. 1, pp. 1–4, 2014.

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

**[13].** A. P. U. Siahaan, "Protection of important data and information using gronsfeld cipher," 2018.

**[14].** 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.

**[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.