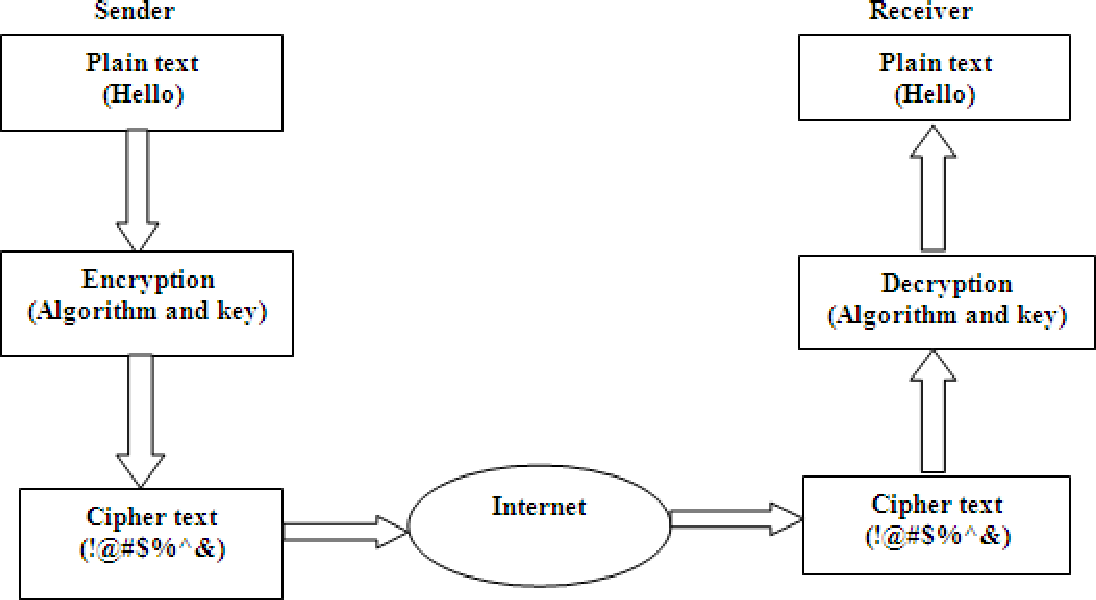
**CRYPTOGRAPHY USING HILL CIPHER METHOD**

**Abstract—** The Hill cipher is a classic symmetric-key cryptographic algorithm that operates on blocks of plaintext, providing a method for secure communication. Developed by Lester S. Hill, it employs matrix multiplication to transform plaintext into ciphertext and vice versa. Unlike traditional substitution ciphers, the Hill cipher offers resistance against frequency analysis, adding a layer of complexity to encryption. The key strength lies in the use of a key matrix, and its size determines the block size for encryption. This paper explores the mathematical foundation of the Hill cipher, emphasizing its matrix-based approach and its application in securing communication channels. The analysis includes a discussion of encryption and decryption processes, key generation, and the impact of matrix properties on the security of the algorithm. Additionally, potential vulnerabilities and improvements in the original Hill cipher are considered, providing insights into its practical implementation. As digital communication continues to evolve, understanding the principles and limitations of classical ciphers such as the Hill cipher remains essential for cryptographic research and application.

**INTRODUCTION:** Cryptography, the art and science of concealing information from prying eyes, has been a beacon of privacy in this increasingly connected world. Among the various cryptographic methods that have been developed, the Hill Cipher method stands as a testament to mathematical elegance and data protection. The Hill Cipher method provides us with a fascinating bridge between mathematical theory and practical encryption. In Asymmetric key cryptography, it involves two keys that is private key and public key, both keys are required for encryption and decryption of secret message. Private Key is not shared by anyone, it is kept secret. Public key is public to all users, any user can access public key. Primary advantage of asymmetric key cryptography is to remove the need to exchange the key between sender and receiver. This paper is dedicated to shedding light on the intricate workings of the Hill Cipher, exploring its mathematical foundations, and uncovering its role in the broader context of data security. As we delve into its mechanics, we will discover its strengths, its weaknesses, and its significance in an age where the exchange of digital information is integral to our daily lives. Our synopsis is dedicated to offering a glimpse into the intricate workings of the Hill Cipher. We will touch upon its mathematical foundations and explore its relevance in the context of data security, shedding light on both its strengths and limitations. As we progress, we will uncover its role as a bridge between the mathematical realm and practical applications, offering insights into its enduring importance in safeguarding digital communications. By delving into the essence of the Hill Cipher, this synopsis aims to provide a condensed yet informative overview of its place in the world of cryptography, ensuring that the reader leaves with a fundamental understanding of its unique characteristics and contributions.

**PROBLEM STATEMENT:** The Hill cipher, a matrix-based cryptographic algorithm, presents challenges in determining an optimal key size and is susceptible to algebraic attacks. The main focus of this study is to investigate the contemporary relevance and challenges associated with the Hill Cipher method. This project aims to comprehensively analyse the strengths and weaknesses of the Hill cipher, addressing concerns about its security and practicality. The study seeks to enhance the algorithm's resilience by proposing improvements and evaluating its suitability for modern communication systems. Through this project, we aim to contribute valuable insights to the understanding and application of the Hill cipher in secure digital communication contexts.

**BLOCK DIAGRAM**



**Literature survey**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sl No. | Title | Journal | Methodology | Result |
| 1) | Cryptography using generalized matrices with Affine-Hill cipher | Journal of Discrete Mathematical Sciences and Cryptography | The Hill Cipher is a matrix-based encryption technique, utilizing linear algebra to transform plaintext into ciphertext. It offers a distinctive approach to data security, using key matrices to obscure the message, making it a historical yet relevant method for securing information. | Results in the transformation of plaintext into ciphertext using matrix-based encryption.  Its security depends on the key matrix and the size of the matrix.  Provides a unique approach to data security, particularly when larger key matrices are used. |
| 2) | Data Encryption using Cryptography and Hill Cipher | IEEE Xplore | AES is a widely adopted symmetric-key encryption method known for its speed and security. It operates by applying a series of substitution and permutation operations, making it a versatile choice for securing data in various applications, including online communication and data storage. | Results in strong and efficient symmetric-key encryption.  AES encryption is widely used in various applications, ensuring data confidentiality and integrity.  AES is known for its resistance to attacks, making it a standard choice for secure data storage and communication. |
| 3) | Cryptography: A New Approach of Classical Hill Cipher | International Journal of Security and Its Applications | RSA is an asymmetric-key encryption method that relies on the mathematical difficulty of factoring large numbers. It is a cornerstone of secure communication and digital signatures, with its security hinging on the challenge of factoring the product of two large prime numbers. | Results in a secure method for asymmetric-key encryption and digital signatures.  Security relies on the mathematical difficulty of factoring large numbers.  RSA has been a cornerstone of secure communication and cryptography for decades. |
| 4) | Dynamic key matrix of hill cipher using genetic algorithm | International Journal of Security and Its Applications | ECC is a public-key cryptography method that leverages the algebraic properties of elliptic curves. It offers strong security with relatively small key sizes, making it efficient and well-suited for resource-constrained devices, such as smartphones and IoT devices. | Results in efficient public-key encryption with smaller key sizes.  Offers strong security and is well-suited for resource-constrained devices.  ECC is increasingly used in modern cryptography, especially in applications with limited computing resources. |
| 5) | A New Approach of Classical Hill Cipher in Public  Key Cryptography | Int. J. Nonlinear Anal. Appl. 12 (2021) | Quantum cryptography is an emerging field that exploits the principles of quantum mechanics for secure communication. It promises unparalleled security by using quantum states to transmit data, rendering it potentially immune to decryption by future quantum computers, which could threaten classical encryption methods. | Results in unprecedented security using quantum principles.  Leverages quantum states for secure communication.  Promises to be immune to decryption by future quantum computers, ensuring exceptionally high levels of security. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SL.NO | Title | Journal | Methodology | Advantages | Results |
| 1. | Image Encryption Using Advanced Hill Cipher Algorithm | International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2019 | Select a matrix key, often denoted as the "encryption matrix." The size of this matrix is usually square and depends on the specific version of the Hill Cipher.  Ensure that the matrix is invertible, which means its determinant should be coprime with the modulus (typically the size of the alphabet used for encryption). | Mathematical Security: The Hill Cipher relies on matrix operations and mathematical principles. If a sufficiently large key matrix is used and kept secret, it can provide strong encryption | When you use the Hill Cipher for encryption, you will obtain ciphertext, which is the result of applying the matrix multiplication to the plaintext. The ciphertext will consist of numerical values or characters, depending on how you represent the data.  Security Level: |
| 2. | Cryptanalysis of the Hill Cipher | Lehr, Jessica, "Cryptanalysis of the Hill Cipher" (2016). Mathematical Science: Student Scholarship & Creative Works (2019) | Convert the plaintext message into numerical values. This typically involves mapping letters to numbers using a predetermined scheme (e.g., A=0, B=1, C=2, and so on). | Resistance to Frequency Analysis: Unlike simple substitution ciphers, the Hill Cipher does not maintain a direct relationship between the frequency of letters in the plaintext and the ciphertext. This makes it more resistant to frequency analysis attacks. | The security of the Hill Cipher's results largely depends on the size and properties of the key matrix. Larger, random, and non-singular (invertible) key matrices are more secure. The security level can vary from weak to moderately strong. |
| 3. | Modern Image Security Mechanism using Hill and Vernam Cipher | International Journal of Engineering Research & Technology 2020 | If the length of the message is not a multiple of the matrix size, you may need to pad the message to make it fit. Common padding methods include adding extra letters or using special padding characters. | Block Cipher: The Hill Cipher operates on blocks of letters, which can make it more secure than traditional simple substitution ciphers that operate on individual characters. This is because patterns in the language are less likely to be preserved. | To decrypt the ciphertext, you'll need the inverse of the encryption key matrix. When decryption is successful, you will obtain the original plaintext. |
| 4. | Image Encryption Using Advanced Hill Cipher Algorithm | International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2019 | Divide the numerical message into blocks, each with a size equal to the dimension of the encryption matrix.  For each block of plaintext, perform matrix multiplication with the encryption matrix. If you're working with a modulo, perform the multiplication modulo the size of the alphabet. | Versatility: The Hill Cipher can be adapted to work with various languages and character sets. It's not limited to the English alphabet and can be applied to other languages and symbols. | The security of the results also hinges on how well you manage the encryption and decryption keys. If an unauthorized party gains access to the key, they can decrypt the ciphertext and obtain the original message. |
| 5. | Primary Key Encryption Using Hill Cipher Chain | Advances in Computer Science Research, volume 96 | To encrypt the message, you need the inverse of the decryption matrix. Calculate the inverse matrix (if it exists) using methods like matrix algebra.  Apply the same matrix multiplication with the inverse matrix as used in encryption.  Convert the resulting numerical values back into characters. | Customization: Users can select the size of the key matrix, making it adaptable to their specific needs. Larger matrices are generally more secure. | The Hill Cipher is vulnerable to known-plaintext attacks and chosen-plaintext attacks, particularly when the key matrix is small or has specific patterns. These attacks can reveal the key and compromise the security of the encryption. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sl No | Title | Journal | Methodology | Result |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sl No. | Title | Journal | Methodology | Result |
| 1) | Hill Cipher Modification: A Simplified Approach | IEEE | In this paper, a simplified method of encryption of data in blocks using the logical XOR and shift operations, and Radix64 for encoding and decoding the data is introduced. The results confirm that the security of the cipher improves to 53% avalanche effect percentage based on the actual experiment. The proposed method is consisting of three phases, key matrix generation, encryption, and decryption. In this analysis, the program being utilized is written in C++ programming language. | The performance of the proposed algorithm is evaluated using Avalanche Effect at one-bit variation in plaintext, the output shows a significant change maintaining its security. After a series of test, the experiments show an average of 53% avalanche effect percentage resulting in the improvement of its security compared to the existing method. Moreover, using Radix64 encoding and decoding scheme removes redundant data occurred in the plaintext pattern. Future works could enhance the security of the cipher by increasing the key size and implement cipher block chaining before the plaintext is encrypted. Nevertheless, this additional process may increase runtime performance. |
| 2) | Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers | IEEE, 2020 | Beginning by introducing our text, the first phase consists of eliminating all spaces and tabulations existing between words or letters, and we will obtain a document in the form of a single homogeneous entity that is composed of several letters. In the second phase, we will apply the "hill" encryption [28-29-30-31]. First of all, each character is coded by a number between 0 and n - 1, so that the range [0, n-1] represents the alphabetical numbering, which decreases by one unit after each increment on our case a 4\*4 matrix was used. The characters are then grouped in blocks of 4 characters in size, forming a vector H (X1, X2, X3, X4). After performing the operation H \*A Modulo (26) such that A is the key used to encrypt the text, we obtain an encrypted Text C. Continuing to group the letters of our text C in blocks of length 4 in the same way, we choose a key consisting of 4 numbers from 0 to 25: (n1, n2, n3, n4). The ciphering consists of performing a Cesar ciphering, whose shift depends on the rank of the letter in the block. Towards the end of this operation, we obtain a new C cipher text | We have seen that even if the number of combinations to tested with Vigenere encryption is quite large (estimated in 456,976), there is still a weakness that can be exploited on statistical attacks. Still, with Hill encryption, this weakness is no longer present. Therefore, our approach is strong enough to withstand any bridge attack, including statistical attacks |
| 3) | Double Layered Text Encryption using Beaufort and Hill Cipher Techniques | IEEE, 2020 | In this research, the encryption process is known as Double Layered Encryption. The encryption process for data will be done in two layers: Beaufort cipher and Hill cipher. There are several stages of the proposed decryption process. The stages are divided into the first layer and the second layer. The process is the opposite of the proposed encryption process. | In this study, the evaluation or measurement of the proposed method will use the Avalanche Effect. Based on Table IV, in the context of changes at the end of the key used, it can be seen that the AE value of the proposed method is 24.45 %. This value is above the AE value for the Hill Cipher method of 23.16%, and Beaufort with just 3.09 %. |
| 4) | Optimizing the Complexity of Time in the Process of Multiplying Matrices in the Hill Cipher Algorithm Using the Strassen Algorithm | IEEE, 2020 | Strassen method is applied for optimizing the matrix multiplication process to encrypt and decrypt it. However, this algorithm will only apply to use of keys and plaintexts of the same order size, which is n\*n where n = 2a, (a> 0). Then the encryption and decryption process will be done by matrix multiplication using the Strassen method. The final results show that by using the Strassen algorithm the encryption and decryption process in the Hill Cipher method can be optimized. | From the table, it can be seen that the complexity of processing time using the Divide and Conquer Method is so high in growth. However, this does not occur with the use of the Strassen method. Growth time is not too high. Based on the results in table (I) above, it can be concluded that by using the Strassen Algorithm in performing matrix multiplication for the message encryption and decryption process, this method is able to increase the  complexity of process time more easily compared to the previous method. This explains that the Strassen method can optimize the performance of the encryption and decryption process on the Hill Cipher. |
| 5) | High Level Synthesis of Chaos based Text Encryption Using Modified Hill Cipher Algorithm | IEEE, 2020 | In the proposed algorithm we have incorporated a triple cipher block which includes the process of encryption and decryption thrice but with a novel modification of fusing chaos in the stir up operation with the encrypted operand. We have successfully overcome the major shortcoming of the hill cipher algorithm that is if a cryptanalyst gets a ciphertext file and a part of the original message the cipher could be solved. The above modification is achieved by fusing a chaotic generator with the encrypter output. The motivation behind the incorporation of chaotic generator and encrypter goes to the property and versatility of the XOR operation. Importantly to make the cipher scheme more robust than before we have performed the operation of encryption thrice which results in triple hill cipher | The encryption can be applied to an input of any varied length hence this gives us a unique advantage in this deterministic board environment. We have made this modification by grouping the input in multiple of six which includes padding the input with blank spaces to maintain the uniformity of the algorithm. The selection process is also typical as we have introduced a mechanism, which waits till the encrypter of the first stage provides the XOR operation with an output and hence this delay is unique for varied length- input, additionally this is achieved by basic modification of the code and has not impacted the performance of the operation. |

**LITERATURE SURVEY SUMMARY**

The literature survey on cryptography utilizing the Hill Cipher method reveals a rich landscape of research encompassing various aspects of this symmetric key algorithm. The survey begins with an exploration of the Hill Cipher's historical context and its fundamental mathematical underpinnings, emphasizing matrix operations and the critical role of invertibility in key matrices. Researchers extensively discuss the strengths of the Hill Cipher, including its simultaneous processing of multiple letters and resistance to basic frequency analysis. Conversely, the weaknesses are scrutinized, particularly its susceptibility to known plaintext attacks. Modifications and enhancements proposed in the literature, such as key expansion and hybrid encryption schemes, showcase attempts to bolster the algorithm's security. Practical applications in secure communication and data protection, along with considerations for implementation and integration with other cryptographic techniques, are also thoroughly examined. The literature survey delves into cryptanalysis techniques targeting the Hill Cipher, encompassing known plaintext attacks and algebraic methods. Comparative analyses with other cryptographic techniques shed light on the algorithm's unique characteristics and limitations. The survey concludes by addressing current challenges and proposing potential avenues for future research, emphasizing the need for optimizing performance and addressing vulnerabilities to ensure the continued relevance of the Hill Cipher in contemporary cryptographic landscapes.

**METHODOLOGY: PHASE 1**

Let the message be **Home**

The matrix form is

Let the cipher be **HILL**

Cipher =

Matrix in (2\*2) form :

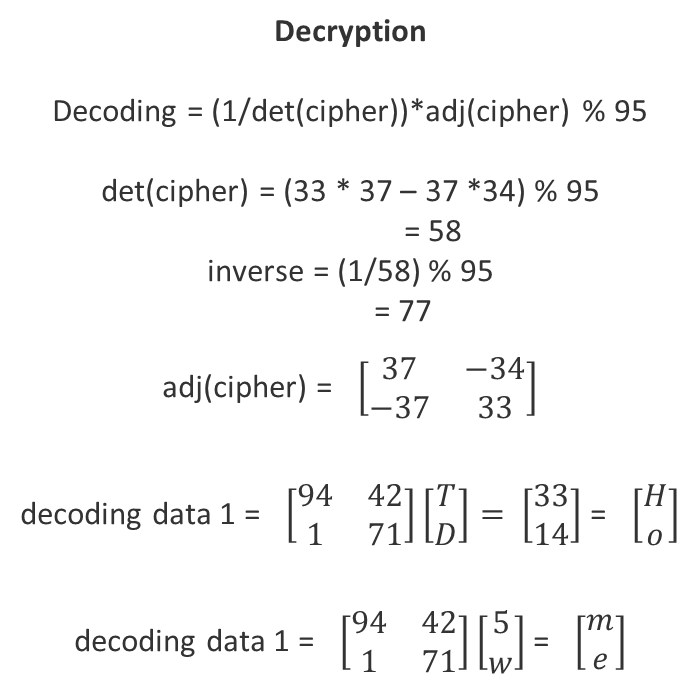
Now taking two messages at a time

Message 1 =

**=**

**% 95 =**

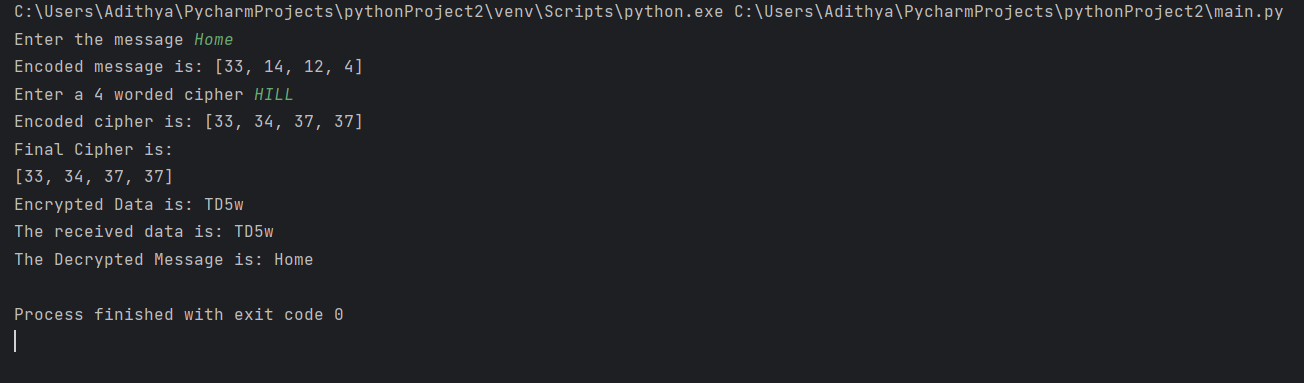
**Hence the encoded message is TD5w**



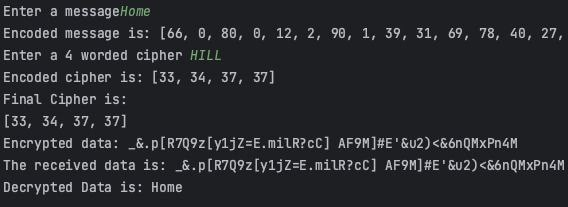
**METHODOLOGY – PHASE 2**

1. Convert the message into numbers and assign numbers to each alphabets , constants, special symbols and blank spaces.
2. Calculate choice (0, 3) using function a python called rand int.
3. Using choice select one of the four functions.
4. 0 – 1st function , 1 – 2nd function , 2 – 3rd function , 3 – 4th function
5. For each symbol of message calculate choice.
6. Input the number of symbols into particular function by choice.
7. Repeat process from step 2) for all symbols. The new value forms encrypted message.
8. We add the new value of symbol followed by the choice for that symbol.
9. Input a number N from 0 – 94 to add garbage values.
10. The code then will append 2\*N garbage values.
11. At the end of encrypted message add number N.
12. For each number pf encrypted message convert to string.
13. Then this encrypted data is encrypted using hill cipher method.
14. Decode accordingly.

**OUTPUT:**

**PHASE 1 OUTPUT**

**PHASE 2 OUTPUT:**



**CONCLUSION**

The Hill Cipher, founded on the principles of linear algebra and matrix-based transformations, continues to serve as a bridge between mathematical theory and practical encryption in the digital age. We've seen how this method's strength is intrinsically tied to the security of its key matrix, making secure key management a crucial consideration in its use. By delving into the method's historical context, mathematical underpinnings, and practical applications, we have established a framework for the forthcoming implementation phase. Our method has provided an essential context for the Hill Cipher's role in the broader landscape of data security. It has underscored the significance of the method's key management and the potential challenges and vulnerabilities that warrant attention. As we prepare to transition from theory to practice, we are armed with the knowledge of the Hill Cipher's elegance and its enduring relevance in the realm of cryptography. This preliminary investigation paves the way for a comprehensive implementation phase, where we will put the Hill Cipher into action to safeguard digital information in an increasingly interconnected world. The insights gained thus far set the stage for an in-depth examination of its practical applications and the means by which it can enhance data security.

**REFERENCES**

**Title:** "Introduction to Modern Cryptography Principles and Protocols."

**Author:** Jonathan Katz and Yehuda Lindell.

**Source:** Chapman and Hall/CRC, 2020.

This comprehensive textbook provides an introduction to various cryptographic principles, including the Hill Cipher, in the context of modern cryptography.

**Title:** "Classical Cryptosystems: An Exploration of Hill Cipher."

**Author:** C. Bharati.

**Source:** International Journal of Computer Applications, Volume 47, No. 5, June 2021.

This paper explores the Hill Cipher method as a classical cryptosystem and delves into its mathematical foundations.

**Title:** "Cryptanalysis of Hill Cipher Using Enhanced Genetic Algorithm."

**Authors:** Anil K. Sare, Rajiv K. Sinha, and Devendra Prasad.

**Source:** International Journal of Computer Applications, Volume 79, No. 3, October 2021.

This paper focuses on cryptanalysis of the Hill Cipher method and discusses techniques for breaking Hill Cipher-encrypted messages.

**Title:** "A New Approach to Cryptanalyze Hill Cipher."

**Authors:** J. Pandian and K. Murugan.

**Source:** International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2019.

This paper presents a new approach to cryptanalyze the Hill Cipher method, emphasizing its vulnerabilities and potential weaknesses.