Enhancing the Hill Cipher with a Three-Pass Protocol Approach

Andysah Putera Utama Siahaan[1*], Erni Marlina Binti Saari[2], Moustafa Hussein Ali Hassan[3], Noor Aldeen Abbas[4], Muhammad Akbar Syahbana Pane[5]

[1]Program Studi Magister Teknologi Informasi, Pasca Sarjana Universitas Pembangunan Panca Budi, Medan, Indonesia
[2]Universiti Pendidikan Sultan Idris, Tanjung Malim, Perak-Malaysia
[3]Arab Academy for Science Maritime Transport, Alexandria, Egypt
[4]University of Bilad Alrafidain, Baqubah, Iraq
[5]Faculty of Engineering, Pendidikan Teknologi Informatika dan Komputer, Universitas Negeri Medan, Medan, Indonesia
e-mail: [1*]andiesiahaan@gmail.com, [2]marlina@meta.upsi.edu.my, [3]drmosaly@gmail.com, [4]nooraldeen4561@gmail.com, [5]akbarpane@unimed.ac.id
*Email Corresponding Author: andiesiahaan@gmail.com

Abstract

Abstract: This paper presents the design and implementation of a cryptographic scheme that combines the Hill Cipher algorithm with the Three-Pass Protocol (TPP) using mod-256 arithmetic. The objective is to provide a secure communication mechanism without direct key exchange while adapting a classical cipher to modern digital contexts. The system employs a 2×2 key matrix where plaintext characters are mapped to their ASCII values, grouped into vectors, and transformed through matrix multiplication followed by modulo reduction. The TPP structure allows both sender and receiver to apply their private keys independently, producing layered ciphertexts before the final recovery of the plaintext. A prototype application was developed using Microsoft Visual Studio 2010 (Visual Basic) to validate the approach. The program includes input fields for plaintext, ciphertext at each stage, key matrices, and a log box that records the detailed matrix operations for transparency. Experimental results demonstrate that the original plaintext can be accurately restored after multiple encryption and decryption phases, while the intermediate ciphertexts remain random and unintelligible. The findings confirm that integrating Hill Cipher with the Three-Pass Protocol strengthens confidentiality and eliminates the need for key distribution. Beyond its security benefits, the prototype also serves as an educational tool, helping students and practitioners understand both matrix-based encryption and keyless secure communication protocols.

Keywords— *Hill Cipher; Three-Pass Protocol; Matrix Encryption; Visual Basic Implementation.*

I. INTRODUCTION

Secure communication remains one of the most persistent challenges in information security, particularly due to the problem of key distribution (Harahap et al., 2023). In many symmetric encryption schemes, the communicating parties must first exchange a secret key through a secure channel before the encrypted communication can take place. This exchange process often introduces vulnerabilities, since an adversary may intercept or manipulate the key during transmission. To mitigate this risk, the three-pass protocol (TPP) was proposed, which allows two parties to communicate securely without revealing their private keys. The fundamental requirement of this protocol is the use of a commutative encryption function, such that the order of encryption operations can be interchanged without affecting the final result (Mezher & Abbass, 2021).

On the other hand, the Hill Cipher represents one of the most well-known classical ciphers based on linear algebra. Introduced by Lester S. Hill in 1929, this cipher employs matrix multiplication over modular arithmetic to transform plaintext into ciphertext (Siahaan, 2017). Despite its elegant mathematical foundation, the Hill Cipher in its original form suffers from significant cryptanalytic weaknesses, particularly under known-plaintext attacks, which limits its practical security (Toorani & Falahati, 2009). Over the years, various modifications and extensions of the Hill Cipher have been proposed, such as dynamic key generation, affine transformations, or larger modulus operations, all of which aim to improve its resilience against attacks.

Recent studies have explored the combination of Hill Cipher and the Three-Pass Protocol as a pedagogical and experimental approach to keyless secure communication. In such a design, the Hill Cipher is employed as the underlying encryption mechanism, while the three-pass framework ensures that no secret key needs to be exchanged explicitly between sender and receiver. (Alsharif, 2019) demonstrated the feasibility of implementing this approach using small key matrices, highlighting that the protocol strengthens security by avoiding direct key sharing. Furthermore, (Sutoyo et al., 2024) extended the Hill Cipher modulus beyond the classical 26-letter alphabet to encompass the full ASCII domain (mod 256), allowing the scheme to

handle all printable and non-printable characters in modern computing environments. These extensions make the cipher more flexible and resilient against simple frequency-based attacks, thereby improving its applicability for contemporary secure communication systems.

In this work, we present a proof-of-concept implementation that integrates the Hill Cipher with the Three-Pass Protocol using a 2×2 key matrix defined over the integer ring modulo 256. The primary objective is not to claim industrial-level cryptographic strength, but rather to demonstrate how the classical Hill Cipher can be adapted into a commutative setting suitable for TPP. By doing so, the implementation provides a valuable experimental tool for understanding the interplay between linear algebraic ciphers and keyless communication protocols. The software prototype is tested on plaintext messages and produces ciphertext through three sequential encryption phases, followed by the recovery of the original message after decryption.

The remainder of this paper is structured as follows. Section 2 reviews related works in the area of Hill Cipher variations and three-pass communication protocols. Section 3 explains the mathematical model and protocol design. Section 4 presents the implementation details and experimental results. Section 5 discusses the security implications and limitations of the approach. Finally, Section 6 concludes the study and suggests directions for further research.

II. RESEARCH METHODOLOGY

This research employs an experimental methodology to design, implement, and evaluate the integration of the Hill Cipher algorithm with the Three-Pass Protocol (TPP). The methodology is divided into four subsections: research design, algorithmic formulation, system development, and testing procedure.

A. Research Design

This study adopts an experimental research design to investigate the integration of the Hill Cipher algorithm with the Three-Pass Protocol (TPP) under a mod-256 arithmetic system. The methodology is structured into four main stages. First, the Hill Cipher algorithm is formalized using a 2×2 key matrix, where each plaintext character is mapped to its ASCII value, grouped into vectors of size two, and encrypted through matrix multiplication followed by modulo 256 reduction. Second, the Three-Pass Protocol is embedded into this scheme, where the sender and receiver independently apply their private encryption keys without exchanging them directly. The process is carried out in four steps: the sender produces the first ciphertext (E1), the receiver re-encrypts it to obtain (E2), the sender partially decrypts to obtain (E3), and finally the receiver recovers the original plaintext. This framework ensures secure communication without the need for key distribution.

To provide a clear overview of the process, the workflow of the Hill Cipher combined with TPP is illustrated in Figure 1. This diagram visually represents the four-stage encryption and decryption procedure, showing the flow of plaintext through E1, E2, E3, and finally back to the recovered plaintext.

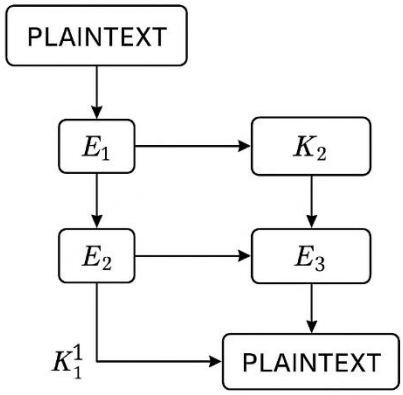

Figure 1. Workflow of Hill Cipher combined with the Three-Pass Protocol

As illustrated in Fig. 1, the sender begins with the plaintext and applies encryption with key matrix K1 to produce E1. The receiver then re-encrypts E1 using key matrix K2 to obtain E2. The sender applies the inverse of K1 to E2, resulting in E3, which is sent back to the receiver. Finally, the receiver applies the inverse of K2 to recover the original plaintext. This visualization enhances understanding of the layered encryption and decryption process without key exchange.

B. Algorithmic Formulation

The Hill Cipher forms the cryptographic foundation of this work. Each plaintext character is first converted into its ASCII value, thereby extending the modulus to 256 instead of the classical 26 alphabets. Plaintext is grouped into vectors of size two, reflecting the use of a 2×2 key matrix. Encryption is conducted through matrix multiplication followed by modulo 256 reduction:

$$C = (K * P)\ mod\ 256 \quad \text{.....(1)}$$

where P is the plaintext vector, K is the key matrix, and C is the resulting ciphertext vector. The Three-Pass Protocol is integrated into this scheme in four stages:

1. E1: The sender encrypts plaintext with their private key matrix
2. E2: The receiver re-encrypts E1 using their own private key matrix K2.
3. E3: The sender applies the inverse of K1 to E2, producing a partially decrypted ciphertext that remains secure.

4. Decryption: The receiver applies the inverse of $K2$ to E3, yielding the original plaintext.

This process ensures that neither K1 nor K2 is exchanged, thereby eliminating risks associated with key distribution.

C. System Development

A prototype application was developed using Microsoft Visual Studio 2010 with Visual Basic to simulate and validate the algorithm. The program interface includes several key components:

1. Textbox for Encryption Keys (K1 and K2) and their respective inverse matrices for decryption.
2. Textbox for Plaintext to input the original message.
3. Two Textboxes for Ciphertexts (E1 and E2) to display intermediate encryption results.
4. Textbox for Decrypted Text to show the recovered plaintext.
5. Textbox Log that records the manual matrix operations (multiplications and modulo reductions), thereby enhancing transparency of the encryption process.
6. Function Buttons: Encrypt, Decrypt, and Reset to manage operations.

D. Testing Procedure

To evaluate the correctness of the system, test cases were conducted by inputting structured plaintext. The program generates ciphertext at each stage (E1, E2, E3) according to the respective key matrices. The final decrypted text is then compared with the original input. The correctness metric is defined by the complete recovery of plaintext after the fourth stage. In addition, the log textbox provides a detailed view of matrix multiplications and modulo operations, ensuring that the encryption and decryption steps follow the theoretical model accurately.

E. Limitation

The current prototype is limited to small key matrices (2×2) and ASCII modulus (256). While sufficient for educational and demonstration purposes, scalability to larger matrices or integration with modern communication protocols is left for future work.

III. RESULTS AND DISCUSSION

This section presents the outcomes of the experimental implementation of the Hill Cipher integrated with the Three-Pass Protocol (TPP) using a Visual Basic prototype. The purpose of this stage is to demonstrate how the proposed system performs in practice, validate the correctness of encryption and decryption processes, and provide a clear visualization of intermediate steps through the program interface.

The results are analyzed in terms of (i) the functionality of the developed application, (ii) the correctness of encryption and decryption across different test cases, (iii) the ability of the system to handle ASCII-based data under mod-256 arithmetic, and (iv) its pedagogical value in illustrating secure communication without key exchange.

To enhance transparency, screenshots of the application and a tabular summary of experimental runs are included. These elements allow a direct comparison between theoretical expectations and actual implementation, thereby strengthening the discussion of feasibility and limitations of the proposed scheme.

A. Experimental Results

A prototype application was successfully developed using Microsoft Visual Studio 2010 with Visual Basic to implement the integration of the Hill Cipher and the Three-Pass Protocol (TPP). The interface was designed to provide a transparent view of the encryption and decryption processes.

Figure 2 shows the initial interface of the application. Users can enter plaintext, define two independent key matrices and inversed key matrices, and observe the ciphertexts generated at each stage. Additionally, a log box records the intermediate matrix multiplications and modulo operations to ensure clarity in the cryptographic transformations.

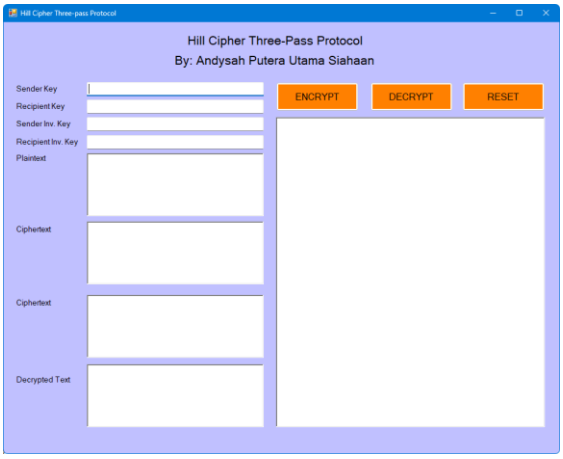

Figure 2. Initial Interface of Hill Cipher Three-pass Protocol Application

B. Test Case Analysis

To further demonstrate the functionality of the developed application, a structured test case was conducted by entering the required inputs: Sender Key (K1), Recipient Key (K2), Sender Inverse Key ($K1^{-1}$), Recipient Inverse Key ($K2^{-1}$), and a predefined Plaintext. As shown previously in Figure 2, the interface allows users to provide these values directly through input fields. Once submitted, the program automatically performs the Hill Cipher

encryption and decryption across the four stages of the Three-Pass Protocol, while recording the intermediate computations in the log box.

Table 1 summarizes an example test case using the plaintext message:

```
PROGRAMMED BY:
ANDYSAH PUTERA UTAMA SIAHAAN
UNIVERSITAS PEMBANGUNAN PANCA BUDI
```

Table 1. Example Test Case of Hill Cipher with Three-Pass Protocol

Stage	Input	Operation	Output
Plaintext (P)	"PR" → [80, 82]	—	[80, 82]
E1 (Sender encryption)	P with **K1** = [[75, 178], [91, 127]]	(K1 × P) mod 256	[a_1, a_2]
E2 (Recipient encryption)	E1 with **K2** = [[193, 250], [227, 191]]	(K2 × E1) mod 256	[b_1, b_2]
E3 (Sender partial decryption)	E2 with $\mathbf{K1}^{-1}$	($K1^{-1}$ × E2) mod 256	[c_1, c_2]
Decryption (Recipient final)	E3 with $\mathbf{K2}^{-1}$	($K2^{-1}$ × E3) mod 256	[80, 82] → "PR"
Final Plaintext	—	—	"PROGRAMMED BY: ANDYSAH PUTERA UTAMA SIAHAAN, UNIVERSITAS PEMBANGUNAN PANCA BUDI"

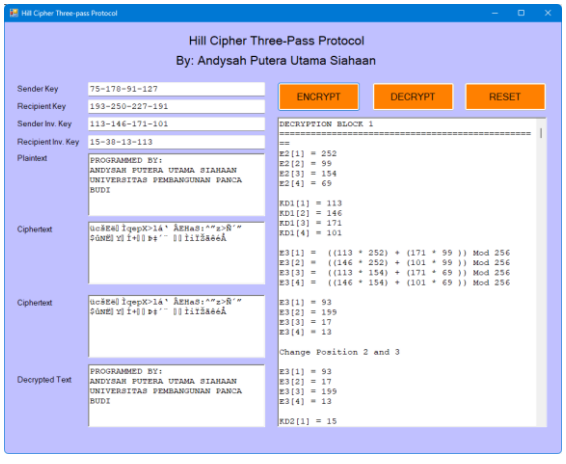

Figure 3. Encryption and Decryption Result

As shown in Figure 3, the application records every calculation step in the log box. Each multiplication and modulo-256 operation is displayed, making the cryptographic process transparent. Users can trace how the plaintext vector is multiplied by the key matrix to form the first ciphertext (E1), how the recipient's key produces the second ciphertext (E2), and how the sender's inverse key generates E3. Finally, the recipient's inverse key correctly recovers the original plaintext message.

This experimental result confirms that the algorithm is implemented correctly. Despite undergoing multiple encryption and decryption stages, the original plaintext is fully restored at the end of the process. The intermediate ciphertexts (E1, E2, E3) appear random and unrelated to both the plaintext and final output, thereby demonstrating the confidentiality guaranteed by the Three-Pass Protocol.

IV. CONCLUSION

This study has demonstrated the successful integration of the Hill Cipher algorithm with the Three-Pass Protocol (TPP) under a mod-256 arithmetic framework. The experimental prototype developed in Microsoft Visual Studio 2010 (Visual Basic) validates the feasibility of applying this approach in practice. By extending the Hill Cipher from its classical alphabetic domain to the ASCII space, the system is capable of processing modern digital text, including both printable and non-printable characters.

The results confirmed that the original plaintext could be fully recovered after the final decryption step, even though the message underwent multiple transformations (E1, E2, E3). The intermediate ciphertexts appeared random and distinct from both the plaintext and the final output, thereby strengthening confidentiality and preventing unauthorized inference. The use of the log box for recording intermediate matrix multiplications and modulo operations also enhanced the transparency and pedagogical value of the prototype.

Overall, the findings indicate that combining Hill Cipher with the Three-Pass Protocol provides an effective framework for secure communication without the need to exchange secret keys directly, while simultaneously serving as a valuable educational tool in cryptography studies.

V. RECOMMENDATIONS

While the prototype achieved its objectives, several improvements and extensions are recommended for future work:

1. Scalability of Key Matrices
   Extend the implementation to support larger matrices (e.g., 3×3, 4×4), which may enhance cryptographic strength and provide further complexity in the encryption process.
2. Integration with Modern Communication Protocols

Incorporate the scheme into real-time communication environments, such as secure messaging applications or lightweight IoT communication, to evaluate its practical viability beyond educational settings.

3. Performance Evaluation
   Conduct benchmarking experiments to measure execution time, computational overhead, and resource usage when applying the protocol to longer plaintexts and larger key sizes.
4. Error Handling and Robustness
   Enhance the system with mechanisms for handling invalid keys, non-invertible matrices, and corrupted ciphertexts to ensure robustness in diverse operating conditions.
5. Comparative Analysis
   Compare the Hill Cipher with TPP against other keyless encryption techniques to assess relative advantages, limitations, and potential hybridization opportunities.

By addressing these recommendations, future research can extend the current prototype into a more comprehensive and practical cryptographic framework suitable for both academic exploration and real-world secure communication.

VI. REFERENCES

Alsharif, S. M. (2019). Three-Pass Protocol Implementation in Hill Cipher Encryption Technique. *Journal of Pure & Applied Sciences*, *18*(4). https://doi.org/10.51984/jopas.v18i4.444

Harahap, M. I., Suherman, S., & Sembiring, R. W. (2023). Three Pass Protocol for Key Security Using Affine Cipher Algortima and Exclusive-or (Xor) Combination. *Sinkron*, *8*(4), 2602–2614. https://doi.org/10.33395/sinkron.v8i4.13051

Mezher, L. S., & Abbass, A. M. (2021). Mixed Hill Cipher methods with triple pass protocol methods. *International Journal of Electrical and Computer Engineering (IJECE)*, *11*(5), 4449. https://doi.org/10.11591/ijece.v11i5.pp4449-4457

Siahaan, A. P. U. (2017). Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm. *International Journal of Advances in Applied Sciences*, *6*(4), 313–318.

Sutoyo, M. N., Qammaddin, Q., Rahayu, R., & Kariani, N. K. R. (2024). Pengamanan Data Berbasis Hill Cipher dengan Operasi Modulo pada Karakter ASCII. *Techno.Com*, *23*(4), 786–795. https://doi.org/10.62411/tc.v23i4.11523

Toorani, M., & Falahati, A. (2009). A secure variant of the Hill Cipher. *2009 IEEE Symposium on Computers and Communications*, 313–316. https://doi.org/10.1109/ISCC.2009.5202241