Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 6** : 1–11.
ISSN-0037-8712
doi:10.5269/bspm.81033

# Contribution to the Study of Linear Cryptosystems: An Analysis of Non-Invertible Matrix-Based Techniques Beyond the Hill Cipher

N. Rafi, K. Khalouki, K. Bouzkoura and A. Chillali

ABSTRACT: Linear cryptosystem, such as the Hill cipher, are foundational in symmetric-key encryption but are limited by the requirement of invertible key matrices, reducing key space and security. This study investigates the use of non-invertible matrices to enhance cryptographic complexity and resilience. We analyze the mathematical principles, design optimized encryption and decryption algorithms, and evaluate their performance against known attacks. Experimental results show that non-invertible matrix-based methods provide stronger data protection than conventional approaches while remaining practically feasible. This proposed symmetric encryption algorithm advances matrix-based cryptography, offering a robust framework for secure communication and guiding future cryptosystem development.

Keywords: Cryptography, symmetric key cryptography, encryption, Hill Cipher, homomorphism.

## Contents



## 1. Introduction

Currently , classical cryptography has attracted renewed interest, not only as a foundation for modern encryption methods but also as a pedagogical tool to study the strengths and weaknesses of substitution–permutation systems. Among these classical methods, the Hill cipher, introduced by Lester S. Hill in 1929, is notable for being one of the first polygraphic substitution ciphers based on linear algebra. Previous studies have shown that the Hill cipher offers faster encryption and decryption compared to many other classical ciphers. Despite these advances, it is also well known that the original Hill cipher is vulnerable to known-plaintext attacks due to its linear structure and invertibility requirements.
Therefore, the aim of this study is to propose a new version of the Hill cipher that we will generalize by using a non-invertible matrix for key generation to make its determination more challenging. To encrypt a message, it is divided into blocks of equal length to the number of rows in the key matrix.
This study provides new insights into strengthening classical ciphers, and the proposed cryptosystem may have implications for lightweight encryption, educational purposes, and the design of hybrid cryptographic systems.
This paper is organized as follows: Section 2 provides a brief review of the mathematical foundation and cryptographic background. Section 3 presents the main mathematical results that motivate the proposed modification and insights used to design the improved version of the Hill cipher. Section 4 describes the

2020 *Mathematics Subject Classification:* 94A60.
Submitted December 26, 2025. Published February 17, 2026

details of the proposed encryption scheme, including the decryption process and the design principles of the key management with an experimental example. Section 5 discusses the results, highlighting improvements over the classical Hill cipher. Finally, Section 6 concludes the paper and outlines potential directions for future.

## 2. Mathematical and Cryptographic Foundations

### 2.1. Mathematical Background

In this section, we present important algebraic results that will be utilized in our proposed cryptosystem.
Let $(F_q, +, .)$ be a finite commutative field, where $q$ is a power of a prime number. Let $\mathbb{D} = M_{n,m}(F_q)$ be the set of all $n \times m$ matrices over $F_q$. This set formes a vector space over $F_q$ under the standard matrix addition $\oplus$ and scalar multiplication $*$.
Let $\mathcal{B} = (E_{ij})$ be a family of matrices in $M_{n,m}(F_q)$ where the coefficients of each matrix $E_{ij}$ are given by the Kronecker delta:
$E_{ij} = (e^{ij}_{pq})_{\substack{1\leq p\leq n\\ 1\leq q\leq m}}$ where $e^{ij}_{pq} = \delta_{ip}\delta_{jq}$ for $1 \leq i \leq n$ and for $1 \leq j \leq m$
This is the standard basis for the vector space of n×m matrices which shows that $\mathbb{D}$ has a finite dimension and equal to nm .
In the following, we state some key properties of a homomorphism between two vector spaces of matrices, D and E , over the finite field $F_q$.
Let $(\mathbb{D}, \oplus_{\mathbb{D}}, *_{\mathbb{D}})$ and $(\mathbb{E}, \oplus_{\mathbb{E}}, *_{\mathbb{E}})$ two vector spaces over $F_q$ with a finite dimensions
Let $\varphi : \mathbb{D} \longrightarrow \mathbb{E}$ be a homomorphism i.e:

- $\varphi(A \oplus_{\mathbb{D}} B) = \varphi(A) \oplus_{\mathbb{E}} \varphi(B)$
- $\varphi(\alpha *_{\mathbb{D}} A) = \alpha *_{\mathbb{E}} \varphi(A)$, with $\alpha \in F_q$

**Lemma 2.1.** *$\varphi$ is injective if and only if $ker\varphi = \{A \in \mathbb{D}/\varphi(A) = 0_{\mathbb{E}}\} = \{0_{\mathbb{D}}\}$*

We denote dim $Im(\varphi) = rk(\varphi)$
If $\varphi$ is surjective:

- we have $span(\varphi(\mathcal{B})) = Im(\varphi) = \mathbb{E}$.
- If $\varphi(\mathcal{B})$ is linear independent, then dim $\mathbb{D}$ = dim $\mathbb{E}$, if not dim $\mathbb{E} < dim\mathbb{D}$.

So,

**Theorem 2.2.** *dim $\mathbb{D}$ = rk $\varphi$ + dim ker $\varphi$*

### 2.2. Cryptographic Background

Symmetric cryptography is a method of encryption in which the same secret key is used for both encrypting and decrypting information. It relies on fast and efficient algorithms, making it suitable for securing large volumes of data. Classical and modern symmetric techniques include block ciphers, such as AES, and stream ciphers. The security of symmetric cryptography depends fundamentally on the confidentiality of the secret key; once the key is compromised, all encrypted data becomes exposed.

Among the classical symmetric cryptosystems, the Hill cipher stands out as one of the most notable. It introduced the innovative use of linear algebra and matrix operations in encryption, marking a significant development in the history of symmetric cryptography. Despite its vulnerability to certain attacks, the Hill cipher remains an important pedagogical and conceptual model, illustrating how algebraic structures can be embedded within cryptographic protocols.

#### Hill Cipher Protocol Details

The Hill cipher encryption and decryption process can be described as a structured protocol with the following steps.

*Key Generation*

- Choose a square matrix $K$ of size $n \times n$ as the secret key.
- Ensure that $K$ is invertible modulo 26, i.e.,

$$\det(K) \not\equiv 0 \pmod{26} \qquad \text{and} \qquad \gcd(\det(K), 26) = 1.$$

- Keep $K$ secret and share it only with authorized parties.

*Plaintext Preparation*

- Represent the plaintext message as numerical values, mapping letters $A \to Z$ to $0 \to 25$.
- Divide the plaintext into blocks of size $n$ to match the dimensions of the key matrix.
- If the last block is incomplete, pad it with a neutral value (e.g., $X \to 23$).

*Encryption*

- Convert each plaintext block into a column vector $P$ of size $n \times 1$.
- Compute the ciphertext vector $C$ using matrix multiplication modulo 26:

$$C = KP \pmod{26}.$$

- Convert the resulting numerical vector $C$ back into letters to form the ciphertext block.
- Repeat for all plaintext blocks.

*Transmission* Send the ciphertext blocks to the recipient over the communication channel. The security of the message relies entirely on the secrecy of the key matrix $K$.

*Decryption*

- The recipient computes the modular inverse of the key matrix, $K^{-1}$, such that

$$K^{-1}K \equiv I \pmod{26}.$$

- For each received ciphertext block $C$, compute the plaintext vector:

$$P = K^{-1}C \pmod{26}.$$

- Convert $P$ back to letters to recover the original message.

## 3. Principal Theoretical Results

Let $(\mathbb{F}_q, +, .)$ be a finite commutative field, where $q$ is a power of a prime number p and let $A \in \mathcal{M}_{n,m}(\mathbb{F}_q)$. We consider

$$\begin{aligned} \varphi_A : \mathcal{M}_{n,n}(\mathbb{F}_q) &\to \mathcal{M}_{n,m}(\mathbb{F}_q) \\ M &\mapsto MA \end{aligned}$$

Such that,

- $\varphi_A(M + M') = (M + M')A = MA + M'A = \varphi_A(M) + \varphi_A(M')$
- $\varphi_A(\alpha M) = (\alpha M)A = \alpha(MA) = \alpha\varphi_A(M)$
  $\varphi_A$ is a homomorphism.

- Let $\mathbb{B}$ denote the canonical basis of $\mathcal{M}_{n,n}$.
  $\mathbb{B} = (E_{ij})_{1\leq i,j\leq n}$, $E_{ij} = (e^{ij}_{pq})_{\substack{1\leq p\leq n\\ 1\leq q\leq n}}$, where $e^{ij}_{pq} = \delta_{ip}\delta_{jq}$

- Let $\mathbb{B}'$ denote the canonical basis of $\mathcal{M}_{n,m}$.
  $\mathbb{B}' = (F_{lk})_{\substack{1\leq l\leq n\\ 1\leq k\leq m}}$, $F_{lk} = (f^{lk}_{pq})_{\substack{1\leq p\leq n\\ 1\leq q\leq m}}$, where $f^{lk}_{pq} = \delta_{lp}\delta_{kq}$

$$\begin{aligned}\varphi_A(E_{ij}) &= E_{ij}A\\ &= \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0\\ 0 & \cdots & 1 & \cdots & 0\\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}\begin{pmatrix} a_{11} & \cdots & a_{1m}\\ \vdots & \ddots & \vdots\\ a_{n1} & \cdots & a_{nm} \end{pmatrix}\\ &= \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0\\ a_{j1} & \cdots & a_{ji} & \cdots & a_{jm}\\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}\end{aligned}$$

$$\mathcal{M}(\varphi_A,\mathbb{B},\mathbb{B}') = \begin{pmatrix} a_{11} & \cdots & a_{n1} & \cdots & 0 & 0 & 0\\ \vdots & \ddots & \vdots & \cdots & 0 & 0 & 0\\ a_{1m} & \cdots & a_{nm} & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & a_{11} & \cdots & a_{n1}\\ 0 & 0 & 0 & \cdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & 0 & a_{1m} & \cdots & a_{nm} \end{pmatrix}$$

$$= \begin{pmatrix} {}^tA & 0 & \cdots & 0 & 0\\ 0 & {}^tA & 0 & \cdots & 0\\ \vdots & & \ddots & \cdots & 0\\ 0 & 0 & \cdots & {}^tA & 0\\ 0 & 0 & \cdots & 0 & {}^tA \end{pmatrix}$$

The matrix representation of $\varphi_A$ with respect to the bases $\mathbb{B}$ and $\mathbb{B}'$. This matrix has nm rows and $n^2$ column and $rk(\mathcal{M}(\varphi_A,\mathbb{B},\mathbb{B}')) = n.rk({}^tA) = n.rk(A)$.

**Lemma 3.1.** *$rk(\varphi_A)$ =$n.rk(A)$.*

We already have $rk(A) \leq min(n,m)$

- First case :

  If $m < n$ and $min(n,m) = m$, that gives $rk(A) \leq m < n$
  and then $rk(\mathcal{M}(\varphi_A,\mathbb{B},\mathbb{B}')) = nrk(A) \leq nm < n^2 = dimM_{n,n}$
  Hence $dim(ker(\varphi_A) = n^2 - rk(\mathcal{M}(\varphi_A,\mathbb{B},\mathbb{B}')) > 0$

- Second case :
  If $m \geq n,\ min(n,m) = n$, and we have rk(A) ≤ n

  i) If $rk(A) < n$
  then $rk(\mathcal{M}(\varphi_A,\mathbb{B},\mathbb{B}')) = n.rk(A) < n^2 = dimM_{n,n}$
  We have : $dim(Ker\varphi_A) = n^2 - rk(\mathbb{M}(\varphi_A,\mathcal{B},\mathcal{B}')) > 0$
  the same conclusion.

ii) If $rk(A) = n = min(n, m)$ with $n \leq m$
then $rk(\mathcal{M}(\varphi_A, \mathbb{B}, \mathbb{B}')) = n.rk(A) = n^2 = dim M_{n,n}$
We have : $dim(Ker\varphi_A) = n^2 - rk(\mathcal{M}(\varphi_A, \mathbb{B}, \mathbb{B}')) = 0$
So $\varphi$ is injective.

Consequently, the homomorphism $\varphi_A : \mathcal{M}_{n,n} \to \varphi_A(\mathcal{M}_{n,n})$ is isometric if the number of columns of the matrix A is greater then or equal to her number of rows and $rk(A)$ equal to the number of rows .
In what follows, let A be an $n \times m$ matrix of rank n (with $n \leq m$ ). Consequently, the vector space spanned by its m columns has dimension n, which guarantees that a basis of n linearly independent columns can be extracted from them.
We select n linearly independent columns from A to form a new matrix LA.. Since $L_A$ has linearly independent columns, it is invertible. We denote its inverse by $L_A^{-1}$.

**Lemma 3.2.** *The matrix $AI_i$ is the matrix A without the i-th column, where $I_{i,m-1}$ denotes the $m \times m$ identity matrix with the ith column removed.*

$$I_{i,m-1} = \begin{pmatrix} 1 & \cdots & 0 & & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & & 0 & \cdots & 0 \\ & & & \vdots & & & \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & \underbrace{\qquad}_{\text{i-th col. removed}} & & & \\ 0 & \cdots & 0 & & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & & 0 & \cdots & 1 \end{pmatrix}_{(m,m-1)}$$

Let $J = \{j_1, j_2, ..., j_{m-n}\}$ that were omitted in the construction of $L_A$. Then, we have the following lemma:

**Lemma 3.3.** *We have: $L_A = A \prod_{k \in \{1,...,m-n\}} I_{j_k,m-k}$, where:*
*$I_{j_k,m-k}$ is the matrix of type $(m-k+1, m-k)$ defined in Lemma 3.2 that removes the $j_k$-th column of the matrix $A \prod_{l \in \{1,...,k-1\}} I_{j_l,m-l}$*

*Proof.* We define a sequence of matrices:
$A^{(0)} = A$,
$A^{(1)} = AI_{j_1,m-1}$ The matrix A without $j_1$-th column, then $AI_{j_1}$ of type $(n, m-1)$,
$A^{(2)} = A^{(1)} I_{j_2,m-2}$ The matrix of A without the columns $j_1$-th and $j_2$-th,
$\vdots$
$A^{(l)} = A^{(l-1)} I_{j_l,m-l}$ The matrix of A without the columns $j_1$-th, $j_2$-th,....,$j_l$-th, for $l \in \{1, ..., m-n\}$
Consequently,

$$L_A = A \prod_{k \in \{1,...,m-n\}} I_{j_k}$$

□

In the following theorem, we present a significant result regarding the existence of an important homomorphism.

**Theorem 3.4.** *Let $\phi_A$ defined by:*

$$\begin{aligned} \phi_A : \mathcal{M}_{n,m} &\to \mathcal{M}_{n,n} \\ M &\mapsto M \prod_{k \in \{1,...,m-n\}} I_{j_k,m-k} L_A^{-1} \end{aligned}$$

*Then, we have:*

$$\phi_A \circ \varphi_A = Id_{n,n}$$

*Proof.* Let m $\in \mathcal{M}_{n,n}$, $\varphi_A(m) = mA$

$$\begin{aligned}\phi_A \circ \varphi_A(m) &= \phi_A(mA)\\ &= (mA) \prod_{k\in\{1,\dots,m-n\}} I_{j_k} L_A^{-1}\\ &= m(A \prod_{k\in\{1,\dots,m-n\}} I_{j_k}) L_A^{-1}\\ &= mL_A L_A^{-1}\\ &= m\end{aligned}$$

Then, $\phi_A \circ \varphi_A = Id_{n,n}$ □

## 4. Proposed Cryptographic Application: Homomorphic Hill Cipher Variant Using Non-Invertible Matrices

Building upon the principal theoretical results and the homomorphism $\phi_A$ introduced in Section 3, this section proposes an updated variant of the Hill cipher. This novel symmetric cryptosystem exploits matrix operations in conjunction with the previously established homomorphic mapping, offering a secure and systematic method for encryption and decryption.

This section is structured in three parts. The first part conceptualizes the cryptosystem protocol, demonstrating how the theorems from Section 3 underpin the construction of key generation, encryption, and decryption algorithms. The second part examines the practical application of the proposed protocol, highlighting its security enhancements and efficiency. And the third part presents a numerical example, implemented over the finite field $F_q$ with $n$ an integer

This updated Hill cipher variant represents a significant improvement over classical versions, providing a robust framework that can be reused and further explored in future cryptographic implementations. The system is defined over the finite field $F_q$ with $n$ an integer, setting the stage for subsequent computational examples.

### 4.1. Detailed Description of the proposed cryptosystem

.

This subsection provides a detailed description of the proposed cryptosystem, outlining its key generation, encryption, and decryption processes, and demonstrating how the integration of the homomorphism $\phi_A$ and non-invertible matrices enhances both security and computational efficiency.

*Key exchange protocol*

- Alice and Bob agree on public prime number p and $A$ is a $n \times m$ matrix of rank n (with $n \leq m$) with coefficients in the finite field $\mathbb{F}_q$, were $q$ is a power of p.
- Alice choose a private keys: $l_1, l_2 \in \mathbb{N}^*$, the invertible matrix $X \in M_{n,n}(\mathbb{F}_q)$ and publish the set $E_X$ determined by the matrices of same order than $X$ that pairwise commute, excluding the zero and identity matrices. In turn, Bob choose a private keys:
  $k_1, k_2 \in \mathbb{N}^*$, the invertible matrix $D \in \mathcal{M}_{n,n}(\mathbb{F}_q)$ and publish the set $E_D$ determined by the matrices of same order than $D$ that pairwise commute, excluding the zero and identity matrices.
- Alice choose an other private key: the invertible matrix $Y \in E_D$. She calculated a matrix $X^{l_1}AY^{l_2}$ and send $X^{l_1}AY^{l_2}$ to Bob. In turn, Bob choose an other private key: the invertible matrix $C \in E_X$. He calculated a matrix $C^{k_1}AD^{k_2}$ and send $C^{k_1}AD^{k_2}$ to Alice. With their private keys $l_1, l_2$ and $k_1, k_2$, Alice and Bob calculate separately the matrices: $C^{k_1}X^{l_1}AY^{l_2}D^{k_2}$.
  Note that $C^{k_1}X^{l_1}AY^{l_2}D^{k_2}$ is an $n \times m$ matrix of rank n.

*Encryption algorithm:* The process of encrypting plaintext (the original message) consists:

- If $rk(A) \neq n$, then we return to the key exchange protocol.
- Else, The sender determinate a plaintext $M \in \mathcal{M}_{n,n}$

$$C = M \times B = \varphi_B(M) \text{ where } B = C^{k_1} X^{l_1} A Y^{l_2} D^{k_2}$$

with $C$ is the ciphertext of $M$

*Decryption Algorithm:*

- Upon receiving the ciphertext, the receiver selects $n$ linearly independent columns of the secret key $K$ to determine the $L_B$ matrix and the decryption function $D(.) = \phi_B(.)$ as follows:

$$D(C) = \phi_B(C) = M$$

### 4.2. Cryptosystem protocol

.

In the following subsection, we present the proposed cryptosystem protocol

**Key generation**

---

*Input:* Random matrix.
*Output:* Generate Private key.

---

Step 1: Select a large prime number $q = p$
Step 2: Choose an $n \times m$ matrix A of rank n uniformly at random from $\mathbb{D}$ ( with $n \leq m$).
Step 3: Return Private key (A, p)

**Encryption algorithm**

---

*Input* : Plaintext M
*Output* : Ciphertext C

---

Step 1: Include the Plaintext M.
Step 2: Encrypt the Plaintext $M$ with (B, mod p).
$C = E(M) = M \times B$ mod p, ( Where $(\times)$ is the usual matrix multiplication).
Step 3: Return the ciphertext C

**Decryption algorithm**

---

Input : Ciphertext
Output : Plaintext

---

Step 1: Include the Ciphertext C.
Step 2: Calculate $M = \phi_A(C)$ mod p.
Step 3: Return the Plaintext M.

### 4.3. Numerical example of the proposed cryptosystem

.

In order to understand the relevance of this proposed work, we will provide in the following section a step-by-step example of the proposed cryptosystem. We will use a key matrix $A$ with coefficients in the field $\mathbb{F}_p$ ( with p a large prime number)and a plaintext matrix $m$ to demonstrate the encryption and decryption algorithms.
Let's assume that Alice wants to send a plaintext matrix $M$ to Bob.

- **Key generation:**
Alice and Bob agree on public prime number $q = p$ and $A$ is a $n \times m$ matrix of rank n (with $n \leq m$) with coefficients in the finite field $\mathbb{F}_p$.
Alice choose a private keys: $l_1 = 2, l_2 = 7$, the matrix $X = \begin{pmatrix} 2 & 8 \\ 1 & 5 \end{pmatrix}$ and send to Bob $E_X = \{B \in M_{2,2}(\mathbb{F}_p)/BX = XB\}$ in this case $B = \begin{pmatrix} l_{11} & 8l_{21} \\ l_{21} & l_{11} + 3l_{21} \end{pmatrix}$
In turn, Bob choose a private keys: $k_1 = 3, k_2 = 5$, the matrix $D = \begin{pmatrix} 0 & 3 & 1 \\ 1 & 4 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ and send to Alice $E_D = \{M \in M_{3,3}(\mathbb{Z}/p\mathbb{Z})/M = aI_{3,3} + bM_1 + cM_2 \quad with \quad a, b, c \in \mathbb{R}\}$ where $M_1 = \begin{pmatrix} 0 & 3 & 1 \\ 1 & 4 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 0 & 10 & 0 \\ 3 & 12 & 1 \\ 1 & 4 & -3 \end{pmatrix}$
Alice choose an other private key: $Y \in E_D$, suppose she has chosen the matrix $I_{3,3} + M_1 + M_2$. She calculated a matrix $X^{l_1}AY^{l_2}$ and send $X^{l_1}AY^{l_2}$ to Bob. In turn, Bob choose an other private key: $C \in E_X$, suppose she has chosen the matrix $C = \begin{pmatrix} 2 & 8 \\ 1 & 5 \end{pmatrix}$. He calculated a matrix $C^{k_1}AD^{k_2}$ and send $C^{k_1}AD^{k_2}$ to Alice. With their private keys $l_1, l_2$ and $k_1, k_2$, Alice and Bob calculate separately the matrices: $C^{k_1}X^{l_1}AY^{l_2}D^{k_2}$.

For $p = 10000000000000000000000013$
$\mathbb{F}_q = \mathbb{F}_p = \mathbb{F}_{10000000000000000000000013}$

$l_1 = 2; \qquad l_2 = 7; \qquad k_1 = 3; \qquad k_2 = 5$

$X = \begin{pmatrix} 2 & 8 \\ 1 & 5 \end{pmatrix}; \quad C = \begin{pmatrix} 85 & 375 \\ 48 & 229 \end{pmatrix}; \quad Y = \begin{pmatrix} 4 & 16 & 2 \\ 5 & 24 & 1 \\ 1 & 6 & 3 \end{pmatrix}; \quad D = \begin{pmatrix} 0 & 3 & 1 \\ 1 & 4 & 0 \\ 0 & 1 & 1 \end{pmatrix};$
$A = \begin{pmatrix} 0 & 1 & 2 \\ 5 & 4 & 3 \end{pmatrix}$

**Alice's public key**

$$X^{l_1}AY^{l_2} = X^2AY^7 = \begin{pmatrix} 1120297587844 & 5261357641512 & 303078822244 \\ 659920011406 & 3099243658508 & 178530938526 \end{pmatrix}$$

**Bob's public key**

$$C^{k_1}AD^{k_2} = C^3AD^5 = \begin{pmatrix} 131266721750 & 616568033125 & 35602999375 \\ 78502353346 & 368730482120 & 21291910060 \end{pmatrix}$$

**The key that is generated by Alice and BOB**

$$B = C^3X^2AY^7D^5 = X^2C^3AD^5Y^7$$

$$= \begin{pmatrix} 74870652952514427944000 & 35162199391271972537600 & 20255058764159747192000 \\ 44775229660315063729088 & 21028206527122576582835 & 12113222900882584937024 \end{pmatrix}$$

- **Encryption part**:
  In this example,
  $B = \begin{pmatrix} 74870652952514427944000 & 35162199391271972537600 & 20255058764159747192000 \\ 44775229660315063729088 & 21028206527122576582835 & 12113222900882584937024 \end{pmatrix}$
  we calculate $C = M \times C^{k_1}X^{l_1}AY^{l_2}D^{k_2} \quad [mod \quad p]$

**The plaintext**

$$M = \begin{pmatrix} 14 & 12 \\ 14 & 8 \end{pmatrix}$$

**The encrypted message**

$$M_c = MB =$$

$$\begin{pmatrix} 15854918972589827559650 56 & 74460926980327853452042 24 & 42892949750882747993228 8 \\ 14063909786177225010487 04 & 66049644369478822818908 16 & 38047660590529714018419 2 \end{pmatrix}$$

- **Decryption Process**:

  After receiving the key $A$ and the ciphertext $C$. Bob calculates $\phi_R(C)$ to retrieve the plaintext matrix $M$:

$$M = \phi_R(C)$$

**The decryption matrix**

$$B' = \begin{pmatrix} 70868754235862585448065 57 & 87733607997559778717992 56 \\ 81580559061380657901536 56 & 20101747649153239322082 44 \\ 0 & 0 \end{pmatrix}$$

**the original message**

$$M_cB' = \begin{pmatrix} 14 & 12 \\ 14 & 8 \end{pmatrix} = M$$

## 5. Discussion and Conclusion

The proposed cryptosystem represents a departure from the traditional Hill Cipher by incorporating non-invertible matrices and homomorphic principles. This novel approach was designed to address the limitations of the Hill Cipher, primarily its susceptibility to frequency analysis. Experimental results validate the feasibility of these modifications, demonstrating a significant enhancement in cryptographic strength.

The integration of non-invertible matrices substantially expands the key space, rendering brute-force attacks computationally impractical. Moreover, the utilization of homomorphic properties introduces additional complexity, thereby increasing the system's resilience against various cryptanalytic techniques. These advancements collectively contribute to a heightened level of security compared to the original Hill Cipher.

While the proposed system offers promising results, it is essential to acknowledge certain limitations. The increased computational overhead associated with matrix operations might necessitate hardware acceleration for real-time applications. Additionally, a comprehensive security analysis, including resistance against advanced attacks, is imperative to establish the system's robustness.

To quantify the improvements achieved, a comparative analysis was conducted (Table 1 ). The results clearly demonstrate the superior performance of the proposed cryptosystem in terms of key space, security level, and algebraic structure.

| **Feature** | **Original Hill Cipher** | **Proposed method** |
|---|---|---|
| Mathematical Base | Operates over integer matrices | Operates within finite fields of prime-power order |
| Key Space | Limited key space, especially in small fields | Larger key space due to finite field properties |
| Security Level | Vulnerable to linear attacks | Enhanced security against known attacks |
| Computational Efficiency | Relatively efficient finite field arithmetic but less scalable | Efficient operations using finite field arithmetic |
| Implementation Complexity | Simpler implementation with basic matrix operations | More complex due to finite field operations |
| Performance | Moderate performance, can be slower in large matrices | Faster encryption/decryption operations |

Table 1: Comparison Between the proposed Method and the original Hill Cipher

Future research should focus on optimizing computational efficiency while preserving the system's security. Integrating error correction codes and exploring the potential for quantum resistance are promising avenues for further development. A rigorous security evaluation, incorporating advanced cryptanalytic techniques, is crucial to validate the system's suitability for practical applications.

## References

1. Lester S. Hill, *Cryptography in an Algebraic Alphabet*, Amer. Math. Mon., 36 (1929), 306-312.
2. Lester S. Hill, *Concerning Certain Linear Transformation Apparatus of Cryptography*, Amer. Math. Mon., 38 (1931), 135-154.
3. A. Chillali, *Cryptography over elliptic curve of the ring $F_q[e]$, $e_4 = 0$*, World Acad. of Sci., Eng. & Technol., 78 (2011), 848-850.
4. A. Tadmori, A. Chillali & M. Ziane, *The binary operations calculus in Ea,b,c*, Int. J. of Math. Models & Methods in Appl. Sci., 9 (2015), 171-175.
5. C. Koukouvinos & D. E. Simos, *Encryption Schemes based on Hadamard Matrices with Circulant Cores*, J. of Appl. Math. & Bioinform., 3 (1) (2013), 17-41.

*Najat RAFI*
*LAMS laboratory,*
*Department of Mathematics and Computer Science,*
*Ben M'Sick Faculty of Science, University Hassan II of Casablanca,*
*Morocco.*
*E-mail address:* rafinajat22@gmail.com

*and*

*Khalid KHALOUKI*
*LAMS laboratory,*
*Department of Mathematics and Computer Science,*
*Ben M'Sick Faculty of Science, University Hassan II of Casablanca, Morocco.*
*E-mail address:* KHALID150716@gmail.com

*and*

*Khadija BOUZKOURA*
*LAMS laboratory,*
*Department of Mathematics and Computer Science,*
*Ben M'Sick Faculty of Science, University Hassan II of Casablanca, Morocco.*
*E-mail address:* kbouzkoura@gmail.com

*and*

*Abdelhakim CHILLALI*
*Department of Mathematics,*
*Sidi Mohamed Ben Abdallah University, Fez, Morocco.*
*E-mail address:* abdelhakim.chillali@usmba.ac.ma