Mathematics and Statistics 12(2): 135-141, 2024
DOI: 10.13189/ms.2024.120203 http://www.hrpub.org

Applications of Onto Functions in Cryptography

K Krishna Sowmya[1,*], **V Srinivas**[2]

[1]Department of Mathematics, TSWRDC(W) Mahabubnagar, Telangana, India

[2] Department of Mathematics, University College of Science, Osmania University, India

Received November 18, 2023; Revised January 24, 2024; Accepted February 17, 2024

Cite This Paper in the following Citation Styles

***(a)**: [1] K Krishna Sowmya, V Srinivas, "Applications of Onto Functions in Cryptography," Mathematics and Statistics, Vol.12, No.2, pp. 135-141, 2024. DOI: 10.13189/ms.2024.120203*

***(b)**: K Krishna Sowmya, V Srinivas (2024). Applications of Onto Functions in Cryptography. Mathematics and Statistics, 12(2), 135-141. DOI: 10.13189/ms.2024.120203*

Abstract The concept of onto functions plays a very important role in the theory of Analysis and has got rich applications in many engineering and scientific techniques. Here in this paper, we are proposing a new application in the field of cryptography by using onto functions on the algebraic structures like rings and fields to get a strong encryption technique. A new symmetric cryptographic system based on Hill ciphers is developed using onto functions with two keys- Primary and Secondary, to enhance the security. This is the first algorithm in cryptography developed using onto functions which ensures a strong security for the system while maintaining the simplicity of the existing Hill cipher. The concept of using two keys is also novel in the symmetric key cryptography. The usage of onto functions in the encryption technique eventually gives the highest security to the algorithm which has been discussed through different examples. The original Hill cipher is obsolete in the present-day technology and serves as pedagogical purpose but whereas this newly proposed algorithm can be safely used in the present-day technology. Vulnerability from different types of attacks of the algorithm and the cardinality of key spaces have also been discussed.

Keywords Onto Function, Cryptography, Encryption, Decryption, Hill Ciphers, Matrices

1 Introduction

Hill ciphers is one of the classical examples under the symmetric key cryptography developed by L. S Hill[1] in 1929, which uses the matrix multiplication for its encryption and decryption.

Hill ciphers has the advantage of disguising letter frequencies of the plain text as it takes the plain text in blocks of size $n \times 1$ and multiplies these blocks with a key matrix of size $n \times n$ [1],[2],[3]. Another advantage of hill ciphers is that its simplicity, as it uses only some simple matrix multiplication for its encryption and one extra step for the decryption to calculate the inverse of the matrix. Computationally, it is easy to implement this technique. Due to these advantages this serves as an important pedagogical role in mathematical cryptography. But the Hill ciphers are vulnerable to the known plain text and cipher text attack due to which it is not in present day usage[4].

In this paper, a new cryptographic system is developed for the first time in the literature using the onto functions in the encryption technique. The algorithm also uses two keys which makes the system more secured among all the symmetric key cryptographic algorithms.

The original hill ciphers along with an example is discussed in the next section of this paper and the proposed algorithm with some examples are discussed in the third section, the fourth section deals about the key space and then the crypt analysis is dealt in the fifth section and last section deals about conclusion.

2 Hill Cipher

Hill Cipher was discovered by L. S. Hill in his paper "Cryptography in an algebraic alphabet" published in the AMM journal(1921). The encryption in Hill cipher that involves with an n-block plain text is multiplied by an $n \times n$ invertible matrix considered as the key in order to get the cipher text.

The cipher text is multiplied by the inverse of the key matrix which gives back the plain text.

2.1 Encryption

Step 1: Convert the alphabetical Plain Text into numericals.
Step 2: Construct the key K as an $n \times n$ invertible matrix in $\mathbb{Z}_{26}$.
Step 3: Divide the numerical plain text in Step 1 into blocks B of size n(i.e. column matrices $n \times 1$).
Step 4: Cipher text C is obtained as C = KB.

Figure 1 below represents the encryption technique of Hill Cipher.

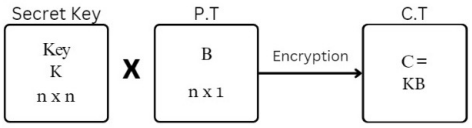

Figure 1. Hill Cipher Encryption.

2.2 Decryption

Step 1: Receiver gets the cipher text as C = KB.
Step 2: Construct the inverse of key K^{-1} in $\mathbb{Z}_{26}$.
Step 3: Divide the numerical cipher text in Step 1 into blocks C of size n.
Step 4: To each block apply the matrix multiplication $B = K^{-1}C$.
2 below represents the encryption technique of Hill Cipher.

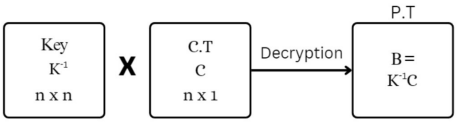

Figure 2. Hill Cipher Decryption.

2.2.1 Example:

Encryption:
Consider the plain text: " MATH IS BEAUTIFUL" taken in blocks of 3 (trigraphs) after its conversion to numerical value, according to the table given below :

A	B	C	D	E	F	G	
0	1	2	3	4	5	6	
H	I	J	K	L	M	N	
7	8	9	10	11	12	13	
O	P	Q	R	S	T	U	
14	15	16	17	18	19	20	
V	W	X	Y	Z			
21	22	23	24	25			

$$MAT|HIS|BEA|UTI|FUL$$
$$12\,0\,19|7\,8\,18|1\,4\,0|20\,19\,8|5\,20\,11$$

$$B_1 = \begin{bmatrix}12\\0\\19\end{bmatrix}\ B_2 = \begin{bmatrix}7\\8\\18\end{bmatrix}\ B_3 = \begin{bmatrix}1\\4\\0\end{bmatrix}\ B_4 = \begin{bmatrix}20\\19\\8\end{bmatrix}\ B_5 = \begin{bmatrix}5\\20\\11\end{bmatrix}$$

Let the Key matrix be $K = \begin{bmatrix}2 & 3 & 1\\7 & 6 & 5\\4 & 3 & 2\end{bmatrix}$

$$C_1 = KB_1 = \begin{bmatrix}2 & 3 & 1\\7 & 6 & 5\\4 & 3 & 2\end{bmatrix}\begin{bmatrix}12\\0\\19\end{bmatrix}\ (mod\ 26)$$
$$= \begin{bmatrix}17\\23\\8\end{bmatrix}\ (mod\ 26)$$

$$C_2 = KB_2 = \begin{bmatrix}2 & 3 & 1\\7 & 6 & 5\\4 & 3 & 2\end{bmatrix}\begin{bmatrix}7\\8\\18\end{bmatrix}\ (mod\ 26)$$
$$= \begin{bmatrix}4\\7\\10\end{bmatrix}\ (mod\ 26)$$

$$C_3 = KB_3 = \begin{bmatrix}2 & 3 & 1\\7 & 6 & 5\\4 & 3 & 2\end{bmatrix}\begin{bmatrix}1\\4\\0\end{bmatrix}\ (mod\ 26)$$
$$= \begin{bmatrix}14\\5\\16\end{bmatrix}\ (mod\ 26)$$

$$C_4 = KB_4 = \begin{bmatrix}2 & 3 & 1\\7 & 6 & 5\\4 & 3 & 2\end{bmatrix}\begin{bmatrix}20\\19\\8\end{bmatrix}\ (mod\ 26)$$
$$= \begin{bmatrix}1\\8\\23\end{bmatrix}\ (mod\ 26)$$

$$C_5 = KB_5 = \begin{bmatrix}2 & 3 & 1\\7 & 6 & 5\\4 & 3 & 2\end{bmatrix}\begin{bmatrix}5\\20\\11\end{bmatrix}\ (mod\ 26)$$
$$= \begin{bmatrix}3\\2\\24\end{bmatrix}\ (mod\ 26)$$

The Cipher text is now obtained as 17 23 8 4 7 10 14 5 16 1 8 23 3 2 24.
The Receiver gets the encoded text as RXIEHKOFQBIXDCY.

Decryption:
Step 1: Convert the alphabets into corresponding numericals as follows:
17 23 8 4 7 10 14 5 16 1 8 23 3 2 24.
Step 2: Consider the trigraphs(Blocks of 3 letters):

$$C_1 = \begin{bmatrix}17\\23\\8\end{bmatrix}; C_2 = \begin{bmatrix}4\\7\\10\end{bmatrix}; C_3 = \begin{bmatrix}14\\5\\16\end{bmatrix};$$
$$C_4 = \begin{bmatrix}1\\8\\23\end{bmatrix}; C_5 = \begin{bmatrix}3\\2\\24\end{bmatrix}$$

Step 3: The inverse of K is $K^{-1} = \begin{bmatrix}17 & 17 & 1\\18 & 0 & 17\\17 & 18 & 25\end{bmatrix} (mod\ 26)$

Step 4: The plain Text is obtained by multiplying each block with inverse of K, i.e. $B_i = K^{-1}C_i$

$$B_1 = K^{-1}C_1 = \begin{bmatrix}17 & 17 & 1\\18 & 0 & 17\\17 & 18 & 25\end{bmatrix}\begin{bmatrix}17\\23\\8\end{bmatrix} = \begin{bmatrix}12\\0\\19\end{bmatrix}$$

$$B_2 = K^{-1}C_2 = \begin{bmatrix}17 & 17 & 1\\18 & 0 & 17\\17 & 18 & 25\end{bmatrix}\begin{bmatrix}4\\7\\10\end{bmatrix} = \begin{bmatrix}7\\8\\18\end{bmatrix}$$

$$B_3 = K^{-1}C_3 = \begin{bmatrix}17 & 17 & 1\\18 & 0 & 17\\17 & 18 & 25\end{bmatrix}\begin{bmatrix}14\\5\\16\end{bmatrix} = \begin{bmatrix}1\\4\\0\end{bmatrix}$$

$$B_4 = K^{-1}C_4 = \begin{bmatrix}17 & 17 & 1\\18 & 0 & 17\\17 & 18 & 25\end{bmatrix}\begin{bmatrix}1\\8\\23\end{bmatrix} = \begin{bmatrix}20\\19\\8\end{bmatrix}$$

$$B_5 = K^{-1}C_5 = \begin{bmatrix}17 & 17 & 1\\18 & 0 & 17\\17 & 18 & 25\end{bmatrix}\begin{bmatrix}3\\2\\24\end{bmatrix} = \begin{bmatrix}5\\20\\11\end{bmatrix}$$

The required plain text is obtained by converting numbers into alphabets as MATHISBEAUTIFUL.

3 Proposed Algorithm

The algorithm is based on the construction of onto functions from the set $\mathbb{Z}_{26}$ *onto* $\mathbb{U}(26)$ and uses the basic idea of Hill ciphers.

This algorithm maintains the simplicity of Hill ciphers as well as enhances the security to the system.

3.1 Encryption

Step 1: Convert the plain text into numerical blocks of nx1 column matrices as $B_1B_2...B_r$
Step 2: Generate an onto function f from $\mathbb{Z}_{26}$ *onto* $\mathbb{U}(26)$.
Step 3: Apply the onto function to the matrices in step 1
Step 4: Generate a parity block matrix P_i corresponding to the plain text block matrix and append it to the plain text. $P' = B'_1P_1B'_2P_2...B'_rP_r$

Step 5: Take K = $[a_{ij}]$, an nxn invertible matrix as a primary key and $a_{ii} \neq 0$, for each i, as secondary key.
Multiply the primary key K with B'_i and a_{ii} with P_i.
Figure 3 below represents the encryption technique of proposed algorithm.

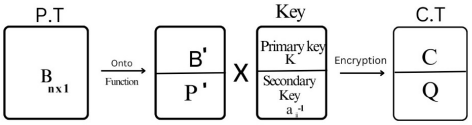

Figure 3. Proposed Algorithm - Encryption.

3.2 Decryption

Let the cipher text received by the receiver be $C = C_1Q_1C_2Q_2...C_rQ_r$
Step 1: Calculate the inverse of primary key K in $\mathbb{Z}_{26}$
Step 2: Multiply each C_i with K^{-1}
Step 3: Calculate the inverse of a_{ii} in $\mathbb{R}$ and multiply these values with Q_i respectively.
Step 4: Add the matrices obtained in step 2 and step 3 correspondingly coordinate wise.
Step 5: The resultant string of block matrices are the numerical form of Plain Text, assign the alphabet to each corresponding integer.
Figure 4 below represents the decryption technique of proposed algorithm.

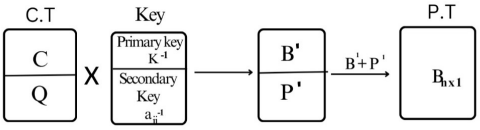

Figure 4. Proposed Algorithm - Decryption.

3.3 Example 1

3.3.1

Encryption: Consider the same plain text: " MATH IS BEAUTIFUL" taken in blocks of 3 (trigraphs) after its conversion to numerical value
$MAT|HIS|BEA|UTI|FUL$

12 0 19|7 8 18|1 4 0|20 19 8|5 20 11

Consider one of the onto functions $f : \mathbb{Z}_{26}$ *onto* $\mathbb{U}(26)$ defined as
$0, 1 \mapsto 1;\ 2, 3 \mapsto 3;\ 4, 5 \mapsto 5;\ 6, 7 \mapsto 7;\ 8, 9 \mapsto 9;\ 10, 11 \mapsto 11;\ 12, 13, 14, 15 \mapsto 15;\ 16, 17 \mapsto 17;\ 18, 19 \mapsto 19;\ 20, 21 \mapsto 21;\ 22, 23 \mapsto 23;\ 24, 25 \mapsto 25;$

The new block matrices of plain text after applying this function and the their parity matrices are given by

$$B_1' = \begin{bmatrix}15\\1\\19\end{bmatrix} \text{ and } P_1 = \begin{bmatrix}-3\\-1\\0\end{bmatrix}$$
$$B_2' = \begin{bmatrix}7\\9\\19\end{bmatrix} \text{ and } P_2 = \begin{bmatrix}0\\-1\\-1\end{bmatrix}$$
$$B_3' = \begin{bmatrix}1\\5\\1\end{bmatrix} \text{ and } P_3 = \begin{bmatrix}0\\-1\\-1\end{bmatrix}$$
$$B_4' = \begin{bmatrix}21\\19\\9\end{bmatrix} \text{ and } P_4 = \begin{bmatrix}-1\\0\\-1\end{bmatrix}$$
$$B_5' = \begin{bmatrix}5\\21\\11\end{bmatrix} \text{ and } P_5 = \begin{bmatrix}0\\-1\\0\end{bmatrix}$$

The cipher text is obtained by multiplying each block matrix by primary key matrix K and parity matrix by secondary keys as the diagonal elements in K and finally by adding these correspondingly:

Let the primary key matrix be $K = \begin{bmatrix}2&3&1\\7&6&5\\4&3&2\end{bmatrix}$ and the secondary keys are 2,6,2.

$$C_1 = KB_1' = \begin{bmatrix}2&3&1\\7&6&5\\4&3&2\end{bmatrix}\begin{bmatrix}15\\1\\19\end{bmatrix}(mod\ 26) = \begin{bmatrix}22\\10\\15\end{bmatrix}(mod\ 26)$$

$$C_2 = KB_2' = \begin{bmatrix}2&3&1\\7&6&5\\4&3&2\end{bmatrix}\begin{bmatrix}7\\9\\19\end{bmatrix}(mod\ 26) = \begin{bmatrix}8\\16\\15\end{bmatrix}(mod\ 26)$$

$$C_3 = KB_3' = \begin{bmatrix}2&3&1\\7&6&5\\4&3&2\end{bmatrix}\begin{bmatrix}1\\5\\1\end{bmatrix}(mod\ 26) = \begin{bmatrix}19\\16\\21\end{bmatrix}(mod\ 26)$$

$$C_4 = KB_4' = \begin{bmatrix}2&3&1\\7&6&5\\4&3&2\end{bmatrix}\begin{bmatrix}21\\19\\9\end{bmatrix}(mod\ 26) = \begin{bmatrix}4\\20\\3\end{bmatrix}(mod\ 26)$$

$$C_5 = KB_5' = \begin{bmatrix}2&3&1\\7&6&5\\4&3&2\end{bmatrix}\begin{bmatrix}5\\21\\11\end{bmatrix}(mod\ 26) = \begin{bmatrix}6\\8\\1\end{bmatrix}(mod\ 26)$$

The Cipher text is now obtained as

$$\begin{bmatrix}22\\10\\15\end{bmatrix}\begin{bmatrix}-6\\-2\\0\end{bmatrix}\begin{bmatrix}8\\16\\15\end{bmatrix}\begin{bmatrix}0\\-6\\-6\end{bmatrix}\begin{bmatrix}19\\16\\21\end{bmatrix}\begin{bmatrix}0\\-2\\-2\end{bmatrix}$$
$$\begin{bmatrix}4\\20\\3\end{bmatrix}\begin{bmatrix}-2\\0\\-2\end{bmatrix}\begin{bmatrix}6\\8\\1\end{bmatrix}\begin{bmatrix}0\\-6\\0\end{bmatrix}$$

So now the cipher text is the string of matrices $B_1'P_1B_2'P_2B_3'P_3B_4'P_4B_5'P_5$.

Decryption:

Calculate the inverses of primary key K and secondary keys a_{ii}:

$$K^{-1} = \begin{bmatrix}17&17&1\\18&0&17\\17&18&25\end{bmatrix}(mod\ 26)$$

$a_{11}^{-1} = 2^{-1}\ a_{22}^{-1} = 6^{-1}\ a_{33}^{-1} = 2^{-1}$

In order to get the plain text, the string of cipher text matrices must be multiplied with K^{-1} and a_{ii}^{-1} alternatively. Then we obtain the string of matrices after multiplying with their corresponding inverses as

$$\begin{bmatrix}15\\1\\19\end{bmatrix}\begin{bmatrix}-3\\-1\\0\end{bmatrix}\begin{bmatrix}7\\9\\19\end{bmatrix}\begin{bmatrix}0\\-1\\-1\end{bmatrix}\begin{bmatrix}1\\5\\1\end{bmatrix}\begin{bmatrix}0\\-1\\-1\end{bmatrix}\begin{bmatrix}21\\19\\9\end{bmatrix}\begin{bmatrix}-1\\0\\-1\end{bmatrix}$$
$$\begin{bmatrix}5\\21\\11\end{bmatrix}\begin{bmatrix}0\\-1\\0\end{bmatrix}$$

The plain text is obtained by adding the two adjacent matrices:

$$\begin{bmatrix}15\\1\\19\end{bmatrix} + \begin{bmatrix}-3\\-1\\0\end{bmatrix} = \begin{bmatrix}12\\0\\19\end{bmatrix}$$

$$\begin{bmatrix}7\\9\\19\end{bmatrix} + \begin{bmatrix}0\\-1\\-1\end{bmatrix} = \begin{bmatrix}7\\8\\18\end{bmatrix}$$

$$\begin{bmatrix}1\\5\\1\end{bmatrix} + \begin{bmatrix}0\\-1\\-1\end{bmatrix} = \begin{bmatrix}1\\4\\0\end{bmatrix}$$

$$\begin{bmatrix}21\\19\\9\end{bmatrix} + \begin{bmatrix}-1\\0\\-1\end{bmatrix} = \begin{bmatrix}20\\19\\8\end{bmatrix}$$

$$\begin{bmatrix}5\\21\\11\end{bmatrix} + \begin{bmatrix}0\\-1\\0\end{bmatrix} = \begin{bmatrix}5\\20\\11\end{bmatrix}$$

Finally the plain text is obtained by converting the numericals into corresponding alphabets.

3.4 Example 2

3.4.1

Encryption: Consider a cipher text as "LOCK DOWN" taken in blocks of 2 in $\mathbb{Z}_{29}$ assigned as in the table below.

A	B	C	D	E	F	G	H	I	J	
0	1	2	3	4	5	6	7	8	9	
K	L	M	N	O	P	Q	R	S	T	
10	11	12	13	14	15	16	17	18	19	
U	V	W	X	Y	Z	!	?	Space		
20	21	22	23	24	25	26	27	28		

LO; CK; DO; WN converted into the numericals as 11 14; 2 10; 3 14; 22 13, So the Plain text in block matrices is given as $\begin{bmatrix}11\\14\end{bmatrix}, \begin{bmatrix}2\\10\end{bmatrix}, \begin{bmatrix}3\\14\end{bmatrix}, \begin{bmatrix}22\\13\end{bmatrix}$.

Let the Key matrix be $K = \begin{bmatrix}1 & 3\\6 & 8\end{bmatrix}$

The block matrices after applying a certain onto function and multiplied by the key matrix K are given as follows:

$B_1' = \begin{bmatrix}8\\18\end{bmatrix}, B_2' = \begin{bmatrix}17\\26\end{bmatrix}, B_3' = \begin{bmatrix}1\\3\end{bmatrix}, B_4' = \begin{bmatrix}3\\12\end{bmatrix}$.

So that the corresponding cipher text will be ISR!BDDM.

The parity matrices are given by

$P_1 = \begin{bmatrix}-15\\11\end{bmatrix}, P_2 = \begin{bmatrix}-3\\-3\end{bmatrix}, P_3 = \begin{bmatrix}-16\\11\end{bmatrix}, P_4 = \begin{bmatrix}10\\7\end{bmatrix}$.

Here in this example we provide different variations in the algorithm while converting the parity matrices into cipher text:

i. According to the proposed algorithm, the parity matrices after multiplied by diagonal entries are given by

$P_1' = \begin{bmatrix}-15\\11\end{bmatrix}, P_2' = \begin{bmatrix}-24\\-24\end{bmatrix}, P_3' = \begin{bmatrix}-16\\11\end{bmatrix}, P_4' = \begin{bmatrix}80\\56\end{bmatrix}$.

ii. The diagonal entries in the key matrix are multiplied with parity matrix coordinate wise:

$P_1' = \begin{bmatrix}-15\\88\end{bmatrix}, P_2' = \begin{bmatrix}-3\\-24\end{bmatrix}, P_3' = \begin{bmatrix}-16\\88\end{bmatrix}, P_4' = \begin{bmatrix}10\\56\end{bmatrix}$.

iii. The Parity matrices can be multiplied with the matrix's eigen values instead of diagonal entries. The eigen values of the key matrix are 10 and -1:

$P_1' = \begin{bmatrix}-150\\-11\end{bmatrix}, P_2' = \begin{bmatrix}-30\\3\end{bmatrix}, P_3' = \begin{bmatrix}-160\\-11\end{bmatrix}, P_4' = \begin{bmatrix}100\\-7\end{bmatrix}$.

iv. The parity matrices can be added to eigen vectors $\begin{pmatrix}-3\\2\end{pmatrix}, \begin{pmatrix}1\\3\end{pmatrix}$ of the matrix alternatively which will transform them as follows:

$P_1' = \begin{bmatrix}-18\\13\end{bmatrix}, P_2' = \begin{bmatrix}-2\\0\end{bmatrix}, P_3' = \begin{bmatrix}-19\\13\end{bmatrix}, P_4' = \begin{bmatrix}11\\10\end{bmatrix}$.

3.4.2

Decryption: At the receiver end the decryption can be done much easily with 3 simple steps by calculating the inverse of key matrix K and multiplying the block matrices with the inverse matrix and the parity matrices are obtained by reversing one of the above processes and added to the block matrices which gives the desired text.

Here inverse of the key matrix K is obtained as

$K^{-1} = \frac{1}{10}\begin{bmatrix}-8 & 3\\6 & -1\end{bmatrix} \equiv \begin{bmatrix}10 & 3\\6 & 8\end{bmatrix} (mod\ 29)$

Since $B_i = K^{-1}B_i'(mod\ 29)$, we get the block matrices as :

$B_1 = \begin{bmatrix}26\\3\end{bmatrix}, B_2 = \begin{bmatrix}5\\13\end{bmatrix}, B_3 = \begin{bmatrix}19\\3\end{bmatrix}, B_4 = \begin{bmatrix}12\\6\end{bmatrix}$.

At this step the receiver has to add each parity matrix to the above matrices to get the original message.

i. The Parity matrices are obtained by multiplying each matrix with inverse of diagonal entry.

$P_1 = {a_{11}}^{-1}P_1' = \begin{bmatrix}-15\\11\end{bmatrix}, P_2 = {a_{22}}^{-1}P_2' = 8^{-1}\begin{bmatrix}-24\\-24\end{bmatrix} = \begin{bmatrix}-3\\-3\end{bmatrix}, P_3 = {a_{11}}^{-1}P_3' = \begin{bmatrix}-16\\11\end{bmatrix}, P_4 = {a_{22}}^{-1}P_4' = 8^{-1}\begin{bmatrix}80\\56\end{bmatrix} = \begin{bmatrix}10\\7\end{bmatrix}$.

ii. The parity matrices are obtained by multiplying the diagonal entries coordinate wise

$P_1 = \begin{bmatrix}-15\\88*8^{-1}\end{bmatrix} = \begin{bmatrix}-15\\11\end{bmatrix}, P_2 = \begin{bmatrix}-3\\-24*8^{-1}\end{bmatrix} = \begin{bmatrix}-3\\-3\end{bmatrix}$,

$P_3 = \begin{bmatrix}-16\\88*8^{-1}\end{bmatrix} = \begin{bmatrix}-16\\11\end{bmatrix}, P_4 = \begin{bmatrix}10\\56*8^{-1}\end{bmatrix} = \begin{bmatrix}10\\11\end{bmatrix}$.

iii. The Parity matrices can be obtained by multiplying with the inverse of eigen values coordinate wise. The inverse of eigen values of the key matrix are 10^{-1} and -1^{-1}:

$P_1 = \begin{bmatrix}-150*10^{-1}\\-11*-1^{-1}\end{bmatrix} = \begin{bmatrix}-15\\11\end{bmatrix}, P_2 = \begin{bmatrix}-30*10^{-1}\\3*-1^{-1}\end{bmatrix} = \begin{bmatrix}-3\\-3\end{bmatrix}$,

$P_3 = \begin{bmatrix}-160*10^{-1}\\-11*-1^{-1}\end{bmatrix} = \begin{bmatrix}-16\\11\end{bmatrix}, P_4 = \begin{bmatrix}100*10^{-1}\\-7*-1^{-1}\end{bmatrix} = \begin{bmatrix}10\\11\end{bmatrix}$.

iv. The parity matrices can be obtained by subtracting eigen vectors $\begin{pmatrix}-3\\2\end{pmatrix}, \begin{pmatrix}1\\3\end{pmatrix}$ of the key matrix alternatively to P_i':

$P_1 = \begin{bmatrix}-18\\13\end{bmatrix} - \begin{bmatrix}-3\\2\end{bmatrix} = \begin{bmatrix}-15\\11\end{bmatrix}, P_2 = \begin{bmatrix}-2\\0\end{bmatrix} - \begin{bmatrix}1\\3\end{bmatrix} = \begin{bmatrix}-3\\-3\end{bmatrix}$,

$P_3 = \begin{bmatrix}-19\\13\end{bmatrix} - \begin{bmatrix}-3\\2\end{bmatrix} = \begin{bmatrix}-16\\11\end{bmatrix}, P_4 = \begin{bmatrix}11\\10\end{bmatrix} - \begin{bmatrix}1\\3\end{bmatrix} = \begin{bmatrix}10\\7\end{bmatrix}$.

4 Discussion on Key Spaces

The primary key K is an $n \times n$ invertible matrix in $\mathbb{Z}_{26}$. So $K \in GL(n, \mathbb{Z}_{26})$ [5],[6]. So the key space is given by the cardinality of the set $GL(n, \mathbb{Z}_{26})$which is given by

$$|GL(n, \mathbb{Z}_{26})| = \prod_{k=0}^{n-1}(2^n - 2^k)(13^n - 13^k) \quad (1)$$

So the number of 3×3 invertible matrices in $\mathbb{Z}_{26}$ are obtained as

$$|GL(3, \mathbb{Z}_{26}| = \prod_{k=0}^{2}(2^3 - 2^k)(13^3 - 13^k) = 1.63403819 \times 10^{12} \quad (2)$$

The secondary keys are the n diagonal entries in the n × n primary key matrix K which are the elements in $\mathbb{Z}_{26}$ except zero.

The total number of onto functions from $\mathbb{Z}_{26}$ *onto* $\mathbb{U}(26)$ are

$$\sum_{k=0}^{26} (-1)^k \binom{26}{k} (26-k)^{12} \tag{3}$$

These sums upto be a very huge number with approximately 26 digits and this could be a much larger number if we use a prime number larger than 26.

For example, the total number of onto functions from $\mathbb{Z}_{29}$ *onto* $\mathbb{U}(29)$ is 29!, which is equal to a natural number with 31 digits. So the sender has a large pool of onto functions to choose and the intruders cannot be able to guess the used function even with a super computer in the stipulated time.

If the algorithm is applied on the set of ASCII values i.e. on $\mathbb{Z}_{128}$, then the cardinality of key space increases drastically. That is given by

$$|GL(n, \mathbb{Z}_{128})| = 26^{n^2} \prod_{k=0}^{n-1} (2^n - 2^k)$$

The number of onto functions from $\mathbb{Z}_{128}$ *onto* $\mathbb{U}(128)$ are $\sum_{k=0}^{128} (-1)^k \binom{128}{k} (128-k)^{64}$.

If the algorithm is applied on the set $\mathbb{Z}_{127}$, then the cardinality of key space increases drastically. That is given by

$$|GL(n, \mathbb{Z}_{127})| = \prod_{k=0}^{n-1} (127^n - 127^k)$$

The number of onto functions from $\mathbb{Z}_{127}$ *onto* $\mathbb{U}_{127}$ are 127!, which contains 214 digits.

On comparison with the key space of hill ciphers, the proposed algorithm's primary key space and hill cipher's key space are equal to equation (1). The advantage of the proposed algorithm is it exponentially increases the key space by the usage of onto function. For example if we take a 3 × 3 matrix as primary key over $\mathbb{Z}_{26}$, the key space would be multiple of equations (2) and (3) which is a 38 digit number. This key space would evidently be a very huge number over $\mathbb{Z}_{128}$.

5 Analysis

The vulnerability of the algorithm against different attacks is studied here.

Brute force attack involves the search for the key by the trail and error method.
In the proposed algorithm the usage of two keys makes it difficult for brute-force attack as the key space is too large which was discussed in the previous section.
The key space for the primary key, an invertible matrix K in $\mathbb{Z}_m$, for $m \in \mathbb{N}$ is very large as discussed in the above section and hence it is impossible for the attackers to guess the key or the onto function used in the encryption end.

The known plain text attack works by reconstructing the secret key based on part of known plain text and their corresponding cipher text. The original Hill cipher is vulnerable to the known plain text, cipher text attack[7], whereas in this proposed algorithm the intruders cannot be able to find the primary key even after knowing the part of plain and cipher texts. This can be achieved by taking large sized matrices as keys.

One can easily find the diagonal entries a_{ii} of the key matrix by finding the g.c.d of non zero numbers in the parity matrix P'. This can be avoided by either taking larger matrices or the parity matrices can be multiplied by the eigen values of the key matrix instead of diagonal entries as mentioned as a variation in example 2 in section 3 . The knowledge of eigen values alone cannot reveal the entries of the matrix and hence the security of the system can be maintained intact. Mathematically one can construct a similar matrix with the knowledge of eigen values but not the same matrix.

The computation cost of Hill ciphers is given by n^2 matrix multiplications and $n^2 - n$ matrix additions for both encryption and decryption[8],[9],[10]. In the proposed algorithm, the computation cost is same as original Hill cipher for encryption whereas for decryption it is n^2 both matrix multiplication and matrix addition.

6 Conclusion

This algorithm is the first of its kind in the literature which uses the onto functions in the encryption. The onto functions used in the encryption of Hill ciphers act as an added security gate by not allowing the intruders. Besides the matrix multiplication used in hill ciphers , this algorithm uses only matrix addition and onto functions and hence maintains the simplicity of the Hill cipher and yet attains the highest security. Since there are a very huge number of onto functions, even a super computer can take a lot of time to find the correct function used in the encryption which makes this algorithm best suited to use in the present day situation.

The system can be made more complex by taking the secondary keys as some other special numbers like the **n eigen values of the key matrix K** as discussed in the above section.

REFERENCES

[1] Lester S. Hill, "Cryptography in An Algebraic Alphabet", The American Mathematical Monthly, Vol. 36, No. 6, pp. 306-312,1929. DOI: 10.1080/00029890.1929.11986963.

[2] Saeednia, Shahrokh,"How to make the Hill cipher secure", Cryptologia, Vol. 24, pp. 353-360, 2000.

[3] B. Vasuki, L. Shobana, B. Roopa, "Data Encryption Using Face Antimagic Labeling and Hill Cipher," MathematicsandStatistics, Vol.10, No. 2, pp. 431-435, 2022. DOI: 10.13189/ms.2022.100218.

[4] N. Parmar, "Hill Cipher Modifications: A Detailed Review", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, No. 3, pp. 1467-1474, 2015. DOI: 10.15680/ijircce.2015.0303010.

[5] J. Overbey, W. Traves and J. Wojdylo, "On the keyspace of the Hill cipher", Cryptologia, Vol. 29, No. 1, pp. 59-72, 2005.

[6] Joseph A Gallian, "Contemporary Abstract Algebra", 10th ed., Chapman and Hall CRC, 2020, pp. 1-654, DOI: 10.1201/9781003142331.

[7] I A Ismail, M Amin, H Diab, "How to repair the Hill cipher", Journal of Zhejiang University - Science A: Applied Physics and Engineering, Vol. 7, pp. 2022-2030, 2006.

[8] Li Chengqing, Dan Zhang and Guan-rong Chen, "Cryptanalysis of an image encryption scheme based on the Hill cipher", Journal of Zhejiang University: Science A, Vol. 9, pp. 1118-1123, 2007.

[9] M Toorani, A Falahati, "A secure variant of the Hill cipher", IEEE Symposium on Computers and Communications, pp. 313-316, 2009, DOI: 10.1109/ISCC.2009.5202241.

[10] Mohammad Hadi Valizadeh, "Healing the Hill Cipher, Improved Approach to Secure Modified Hill against Zero-plaintext Attack", IACR Cryptol. ePrint Arch., 2016.