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

(3s.) **v. 2026 (44) 17** : 1–13.
ISSN-0037-8712
doi:10.5269/bspm.82359

A Cryptographic Approach Using Partial Affine Bijective Mapping and Recursive Hill Cipher

Sontay Manusha and Veladi Srinivas

ABSTRACT: This study introduces a hybrid encryption framework that integrates Partial Affine Bijective Mapping with a Recursive Hill Cipher, employing modulo 27 arithmetic to encompass all 26 English alphabetic characters along with the space symbol. In the proposed scheme, plaintext is initially converted into its numeric representation through partial affine bijective mapping. Subsequently, encryption is performed using a Hill Cipher, wherein the key matrix is recursively updated across successive rounds. This recursive key evolution significantly strengthens the cryptographic system by expanding the effective key space, enhancing statistical randomness, and mitigating susceptibility to classical cryptanalytic techniques such as frequency analysis and bruteforce attack. In this paper, the proposed framework is further extended to modulo 37 arithmetic to additionally incorporate numeric digits ($0-9$), thereby improving its applicability to alphanumeric data without altering the core encryption structure.

Keywords: Encryption, decryption, partial affine bijective mapping, recursive Hill Cipher.

Contents

1. Introduction

In the digital age, secure communication is essential due to the widespread exchange of sensitive information over open networks. [1] Classical cryptographic techniques such as affine and Hill ciphers are mathematically efficient but suffer from inherent weaknesses, [2] including fixed key structures and vulnerability to frequency analysis and known-plaintext attacks. [3]These limitations motivate the development of enhanced encryption schemes that improve security while retaining computational simplicity. [4] This paper presents a hybrid encryption framework that integrates Partial Affine Bijective Mapping with a Recursive Hill Cipher. Plaintext is first converted into numerical form using partial affine bijective mapping, introducing additional confusion before encryption. [5] The transformed data is then encrypted using a Hill Cipher with a key matrix that is recursively updated across multiple rounds, [6] significantly expanding the effective key space and improving resistance to brute-force and statistical attacks. The scheme initially employs modulo 27 arithmetic to represent alphabetic characters and space. In the same paper, the framework is extended to modulo 37 arithmetic to include numeric digits from 0 to 9 , [7] enhancing applicability to alphanumeric data.

2. Mathematical Background

Definition 2.1 *Partial Affine Bijective Mapping is a cryptographic technique that applies a mathematical transformation to a part of the data, rearranging and substituting values in a one-to-one (bijective) manner. "Affine" refers to a linear transformation combined with a constant shift, while "bijective" ensures that every input maps to a unique output, making the process reversible for decryption. By applying this mapping partially, only selected elements of the data are transformed, which increases security while*

2020 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted March 04, 2026. Published June 24, 2026.

keeping computational complexity low.

Example 2.1
Suppose we have a set of numbers representing characters $S = \{0, 1, 2, 3, 4, 5, 6\}$
We decide to apply a bijective mapping only to a part of the set, say $\{0, 1, 2, 3\}$
Let's define a bijective function for this part:

$$f(x) = (x + 2) \mod 4 \tag{2.1}$$

mapping applied to the partial set:

- $0 \to 2$
- $1 \to 3$
- $2 \to 0$
- $3 \to 1$

The remaining elements $\{4, 5, 6\}$ are unchanged.
Result after partial mapping:$\{2, 3, 0, 1, 4, 5, 6\}$

Definition 2.2 *The Recursive Hill Cipher is an enhanced version of the classical Hill cipher [8] in which the key matrix evolves recursively for each round or block of encryption. Instead of using a fixed key matrix K for all plaintext blocks, a sequence of key matrices $K_1, K_2, K_3, \ldots$ is generated [9] recursively according to a defined relation.*

Two common recursive formulations are:
Additive Recursion

$$K_{i+1} = K_i + I (\mathrm{mod} 26)$$

Exponential Recursion

$$K_{i+1} = K_i^2 (\mathrm{mod} 26)$$

In this form, each successive key matrix is obtained by squaring the previous key matrix (mod 26).
where I is the identity matrix. Here, the key matrix is updated by adding the identity matrix [10] at each step. The encryption [11] process for the i^{th} plaintext block P_i is then given by:

$$C_i = K_i \cdot P_i (\mathrm{mod} 26)$$

and decryption [12] uses the modular inverse of the corresponding key:

$$P_i = K_i^{-1} \cdot C_i (\mathrm{mod} 26)$$

Encryption
Step 1: Convert the alphabetical Plain Text into numerical and divide numerical as a block of three and name the i^{th} block as P_i.
Step 2: Pick the initial key K_1 a 3 by 3 invertible matrix under modulo 26.
Step 3: Define additive recursion $K_{i+1} = K_i + I (\mathrm{mod} 26)$ and find recursive key matrices.
Step 4: Cipher text C is obtained as $C_i = K_i \cdot P_i (\mathrm{mod} 26)$.
Decryption
Step 1: Convert the obtained cipher text into numerical and divide numerical as a block of three and name i^{th} block as C_i.
Step 2: Now construct inverse of each K_i in $\mathbb{Z}_{26}$.
Step 3: To each block apply the matrix multiplication $P_i = K_i^{-1} \cdot C_i (\mathrm{mod} 26)$. So the plain text is obtained.
Example 2.2

Table 1: table of alphabets

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		

The plaintext "SECRET" is divided into groups of three letters after converting each letter into its corresponding numerical value based on the provided table.

Encryption

Step 1: Convert the alphabetical Plain Text into numerical and divide numerical as a block of three and name the i^{th} block as P_i.

$S-18 \quad E-4 \quad C-2 \quad R-17 \quad E-4 \quad T-19$

$$P_1 = \begin{bmatrix} 18 \\ 4 \\ 2 \end{bmatrix} \quad P_2 = \begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix} \tag{2.2}$$

Step 2: Pick the initial key K_1 a 3 by 3 invertible matrix under modulo 26.

$$K_1 = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Step 3: Define additive recursion $K_{i+1} = K_i + I(\text{mod}26)$ and find recursive key matrices

$$K_2 = K_1 + I(\text{mod}26)$$

$$K_2 = \begin{bmatrix} 3 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix}$$

Step 4: Cipher text C is obtained as $C_i = K_i \cdot P_i(\text{mod}26)$

$$C_1 = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 18 \\ 4 \\ 2 \end{bmatrix} (\text{mod}26) \tag{2.3}$$

$$C_1 = \begin{bmatrix} 14 \\ 24 \\ 6 \end{bmatrix} (\text{mod}26) \tag{2.4}$$

$$C_2 = \begin{bmatrix} 3 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix} (\text{mod}26) \tag{2.5}$$

$$C_2 = \begin{bmatrix} 3 \\ 18 \\ 16 \end{bmatrix} (\text{mod}26) \tag{2.6}$$

Hence cipher text is obtained as $14 \quad 24 \quad 6 \quad 3 \quad 18 \quad 16$

The receiver receives the code OYGDSQ.

Decryption Step 1: Convert the obtained cipher text into numerical and divide numerical as a block of three.

$O-14 \quad Y-24 \quad G-6 \quad D-3 \quad S-18 \quad Q-16$

$$C_1 = \begin{bmatrix} 14 \\ 24 \\ 6 \end{bmatrix} \tag{2.7}$$

$$C_2 = \begin{bmatrix} 3 \\ 18 \\ 16 \end{bmatrix} \tag{2.8}$$

Step 2: Now construct inverse of each K_i in Z_{26}.

$$K_1^{-1} = \begin{bmatrix} 0 & 1 & 25 \\ 1 & 24 & 2 \\ 25 & 2 & 25 \end{bmatrix}$$

$$K_2^{-1} = \begin{bmatrix} 19 & 22 & 15 \\ 22 & 12 & 7 \\ 15 & 7 & 23 \end{bmatrix}$$

Step 3: To each block apply the matrix multiplication $P_i = K_i^{-1} \cdot C_i(\text{ mod } 26)$ So the plain text is obtained.

$$P_1 = K_1^{-1} \cdot C_1(\text{mod}26)$$

$$P_1 = \begin{bmatrix} 0 & 1 & 25 \\ 1 & 24 & 2 \\ 25 & 2 & 25 \end{bmatrix} \begin{bmatrix} 14 \\ 24 \\ 6 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 18 \\ 4 \\ 2 \end{bmatrix} \tag{2.9}$$

$$P_2 = K_2^{-1} \cdot C_2(\text{mod}26)$$

$$P_2 = \begin{bmatrix} 19 & 22 & 15 \\ 22 & 12 & 7 \\ 15 & 7 & 23 \end{bmatrix} \begin{bmatrix} 3 \\ 18 \\ 16 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix} \tag{2.10}$$

The required plain text is obtained by converting this numerical into plaintext as SECRET.

3. Proposed Algorithm

The proposed Cryptographic scheme consists of encryption and decryption. The detailed steps are presented below.

Encryption

Step 1: Translate the plaintext letters into numbers using the mapping $A \to 0, B \to 1, \ldots, Z \to 25$, and space $\to 26$. Group the resulting sequence into blocks of three and denote the i^{th} block by P_i.

Step 2: Specify a partial affine mapping on $\mathbb{Z}_{27}$.

Step 3: Apply this affine transformation to each component of the blocks produced in Step 1. The transformed blocks will be written as P_i'.

Step 4: Choose an initial 3 by 3 matrix K_1 that is invertible over modulo 27.

Generate the remaining key matrices recursively by

$$K_{i+1} \equiv K_i + I(\text{mod}27)$$

where I is the 3×3 identity matrix.

Step 5: Compute the ciphertext blocks using

$$C_i \equiv K_i \cdot P_i'(\text{mod}27)$$

Decryption
Step 1: Convert the ciphertext characters back into their numerical equivalents and divide the sequence into three-element blocks, naming the i^{th} block C_i.
Step 2: Compute the modular inverse of every key matrix K_i in $\mathbb{Z}_{27}$.
Step 3: Recover the intermediate blocks by

$$P_i' \equiv K_i^{-1} \cdot C_i (\text{mod} 27)$$

Step 4: Determine the inverse of the affine mapping used during encryption.
Step 5: Apply this inverse affine map to each $\mathrm{P_i}'$ to obtain the original plaintext blocks, and then convert the numbers back into characters.
Example: Consider the plaintext "GO TO BED" convert this into numbers according to the given table

Table 2: table of alphabets and space

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	space	
21	22	23	24	25	26	

Encryption
Step 1: Translate the plaintext letters into numbers using the mapping $A \to 0, B \to 1, \ldots, Z \to 25$, and space $\to$ 26. Group the resulting sequence into blocks of three and denote the i^{th} block by P_i.
$G-6 \quad O-14 \quad space-26 \quad T-19 \quad O-14 \quad space-26 \quad B-1 \quad E-4 \quad D-4$

$$P_1 = \begin{bmatrix} 6 \\ 14 \\ 26 \end{bmatrix} P_2 = \begin{bmatrix} 19 \\ 14 \\ 26 \end{bmatrix} \quad P_3 = \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix} \tag{3.1}$$

Step 2: Specify a partial affine mapping on $\mathbb{Z}_{27}$.

$$f(x) = \begin{cases} 5x + 3(\text{mod} 27) & \text{if } x \in U(27) \\ x & \text{else} \end{cases} \tag{3.2}$$

Step 3: Apply this affine transformation to each component of the blocks produced in Step 1.
The transformed blocks will be written as P_i'.
For $P_1 = \begin{bmatrix} 6 \\ 14 \\ 26 \end{bmatrix}$

$$\begin{aligned} f(6) &= 6(\text{ since } 6 \notin U(27)) \\ f(14) &= 5(14) + 3(\text{mod} 27) = 73 \bmod 27 = 19 \\ f(26) &= 5(26) + 3(\text{mod} 27) = 133 \bmod 27 = 25 \end{aligned} \tag{3.3}$$

$$P_1' = \begin{bmatrix} 6 \\ 19 \\ 25 \end{bmatrix}$$

For $P_2 = \begin{bmatrix} 19 \\ 14 \\ 26 \end{bmatrix}$

$$\begin{aligned} f(19) &= 5(19) + 3(\text{mod}27) = 98 \bmod 27 = 17 \\ f(14) &= 5(14) + 3(\text{mod}27) = 73 \bmod 27 = 19 \\ f(26) &= 5(26) + 3(\text{mod}27) = 133 \bmod 27 = 25 \end{aligned} \tag{3.4}$$

$$P_2' = \begin{bmatrix} 17 \\ 19 \\ 25 \end{bmatrix}$$

For $P_3 = \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix}$

$$\begin{aligned} f(1) &= 5(1) + 3(\text{mod}27) = 8 \\ f(4) &= 5(4) + 3(\text{mod}27) = 23 \\ f(3) &= 3(\text{ since } 3 \notin U(27)) \end{aligned} \tag{3.5}$$

$$P_3' = \begin{bmatrix} 8 \\ 23 \\ 3 \end{bmatrix}$$

Step 4: Choose an initial 3 by 3 matrix K_1 that is invertible over modulo 27. Generate the remaining key matrices recursively by

$$K_{i+1} \equiv K_i + I(\text{mod}27)$$

Take key matrix as $K_1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 3 \end{bmatrix}$

$$K_2 \equiv K_1 + I(\text{mod}27)$$

$$K_2 = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 4 \end{bmatrix}$$

$$K_3 \equiv K_2 + I(\text{mod}27)$$

$$K_3 = \begin{bmatrix} 3 & 1 & 1 \\ 1 & 4 & 1 \\ 1 & 1 & 5 \end{bmatrix}$$

Step 5: Compute the ciphertext blocks using

$$C_i \equiv K_i \cdot P_i'(\text{mod}27)$$

$$\begin{aligned} &C_1 \equiv K_1 \cdot P_1'(\text{mod}27) \\ &C_1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 6 \\ 19 \\ 25 \end{bmatrix} (\text{mod}27) = \begin{bmatrix} 23 \\ 15 \\ 19 \end{bmatrix} \end{aligned} \tag{3.6}$$

$$\begin{aligned} &C_2 \equiv K_2 \cdot P_2'(\text{mod}27) \\ &C_2 = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 4 \end{bmatrix} \begin{bmatrix} 17 \\ 19 \\ 25 \end{bmatrix} (\text{mod}27) = \begin{bmatrix} 24 \\ 18 \\ 1 \end{bmatrix} \end{aligned} \tag{3.7}$$

$$C_3 \equiv K_3 \cdot P_3'(\text{mod}27)$$
$$C_3 = \begin{bmatrix} 3 & 1 & 1 \\ 1 & 4 & 1 \\ 1 & 1 & 5 \end{bmatrix} \begin{bmatrix} 8 \\ 23 \\ 3 \end{bmatrix} (\text{mod}27) = \begin{bmatrix} 23 \\ 22 \\ 19 \end{bmatrix} \tag{3.8}$$

So the cipher text is now obtained as 23 15 19 24 18 1 23 22 19
Ciphertext is XPTYSBXWT.

Decryption

Step 1: Convert the ciphertext characters back into their numerical equivalents and divide the sequence into three-element blocks, naming the i^{th} block C_i.

$X-23 \quad P-15 \quad T-19 \quad Y-24 \quad S-18 \quad B-1 \quad X-23 \quad W-22 \quad T-19$

$$C_1 = \begin{bmatrix} 23 \\ 15 \\ 19 \end{bmatrix} C_2 = \begin{bmatrix} 24 \\ 18 \\ 1 \end{bmatrix} \quad C_3 = \begin{bmatrix} 23 \\ 22 \\ 19 \end{bmatrix} \tag{3.9}$$

Step 2: Compute the modular inverse of every key matrix K_i in $\mathbb{Z}_{27}$.

$$K_1^{-1} = \begin{bmatrix} 16 & 26 & 13 \\ 26 & 1 & 0 \\ 13 & 0 & 14 \end{bmatrix}$$
$$K_2^{-1} = \begin{bmatrix} 7 & 3 & 11 \\ 3 & 2 & 19 \\ 11 & 19 & 13 \end{bmatrix}$$
$$K_3^{-1} = \begin{bmatrix} 2 & 1 & 21 \\ 1 & 10 & 14 \\ 21 & 14 & 4 \end{bmatrix}$$

Step 3: Recover the intermediate blocks by

$$P_i' \equiv K_i^{-1} \cdot C_i(\text{mod}27)$$

$$P_1' \equiv K_1^{-1} \cdot C_1(\text{mod}27)$$
$$\text{P}_1' = \begin{bmatrix} 16 & 26 & 13 \\ 26 & 1 & 0 \\ 13 & 0 & 14 \end{bmatrix} \begin{bmatrix} 23 \\ 15 \\ 19 \end{bmatrix} (\text{mod}27) = \begin{bmatrix} 1005 \\ 613 \\ 565 \end{bmatrix} (\text{mod}27) = \begin{bmatrix} 6 \\ 19 \\ 25 \end{bmatrix} \tag{3.10}$$

$$P_2' \equiv K_2^{-1} \cdot C_2(\text{mod}27)$$
$$P_2' = \begin{bmatrix} 7 & 3 & 11 \\ 3 & 2 & 19 \\ 11 & 19 & 13 \end{bmatrix} \begin{bmatrix} 24 \\ 18 \\ 1 \end{bmatrix} (\text{mod}27) = \begin{bmatrix} 233 \\ 127 \\ 619 \end{bmatrix} (\text{mod}27) = \begin{bmatrix} 17 \\ 19 \\ 25 \end{bmatrix} \tag{3.11}$$

$$P_3' \equiv K_3^{-1} \cdot C_3(\text{mod}27)$$
$$P_3' = \begin{bmatrix} 2 & 1 & 21 \\ 1 & 10 & 14 \\ 21 & 14 & 4 \end{bmatrix} \begin{bmatrix} 23 \\ 22 \\ 19 \end{bmatrix} (\text{mod}27) = \begin{bmatrix} 467 \\ 509 \\ 867 \end{bmatrix} (\text{mod}27) = \begin{bmatrix} 8 \\ 23 \\ 3 \end{bmatrix} \tag{3.12}$$

Step 4: Determine the inverse of the affine mapping used during encryption.

$$f^{-1}(\text{y}) = \begin{cases} 11(y-3)(\text{mod}27) & \text{if y} \in \text{U(27)} \\ y & \text{else} \end{cases} \tag{3.13}$$

Step 5: Apply this inverse affine map to each P_i' to obtain the original plaintext blocks, and then convert the numbers back into characters. For $P_1' = \begin{bmatrix} 6 \\ 19 \\ 25 \end{bmatrix}$

$$\begin{aligned} f^{-1}(6) &= 6(\text{ since } 6 \notin U(27)) \\ f^{-1}(19) &= 11(19-3) \bmod 27 = 176 \bmod 27 = 14 \\ f^{-1}(25) &= 11(25-3) \bmod 27 = 242 \bmod 27 = 26 \end{aligned} \tag{3.14}$$

$$P_1 = \begin{bmatrix} 6 \\ 14 \\ 26 \end{bmatrix}$$

For $P_2' = \begin{bmatrix} 17 \\ 19 \\ 25 \end{bmatrix}$

$$\begin{aligned} f^{-1}(17) &= 11(17-3) \bmod 27 = 154 \bmod 27 = 19 \\ f^{-1}(19) &= 11(19-3) \bmod 27 = 176 \bmod 27 = 14 \\ f^{-1}(25) &= 11(25-3) \bmod 27 = 242 \bmod 27 = 26 \end{aligned} \tag{3.15}$$

$$P_2 = \begin{bmatrix} 19 \\ 14 \\ 26 \end{bmatrix}$$

For $P_3' = \begin{bmatrix} 8 \\ 23 \\ 3 \end{bmatrix}$

$$\begin{aligned} f^{-1}(8) &= 11(8-3) \bmod 27 = 55 \bmod 27 = 1 \\ f^{-1}(23) &= 11(23-3) \bmod 27 = 220 \bmod 27 = 4 \\ f^{-1}(3) &= 3(\text{ since } 3 \notin U(27)) \end{aligned} \tag{3.16}$$

$$P_3 = \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix}$$

So the plaintext is obtained as 6 14 26 19 14 26 1 4 3
The plaintext is GO TO BED.

4. Extension for the Proposed Algorithm

To extend the plaintext symbol set and improve the algebraic structure of the cipher, we replace the working ring $\mathbb{Z}_{27}$. with the finite field $\mathbb{Z}_{37}$, where 37 is prime. This modification provides the following benefits:

Prime-field arithmetic: Because 37 is prime, $\mathbb{Z}_{37}$. forms a field in which every nonzero element has a multiplicative inverse, ensuring stable and well-defined modular operations.

More invertible matrices: The prime modulus expands the space of invertible 3×3 times 3×3 matrices, providing stronger key variability and improved security.

Expanded symbol set: With 37 residue classes available, the system can naturally encode all 26 letters, the 10 digits ($0-9$), and the space character without collisions.

Reliable affine and matrix transformations: Working in a prime modulus eliminates the modular singularities and degeneracies possible in composite moduli like 27 , ensuring consistent encryption and decryption.

Example: Consider the plaintext "SECRET CODE1" convert this into numbers according to the given table

Table 3: Alphanumeric table

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	space	0
21	22	23	24	25	26	27
1	2	3	4	5	6	7
28	29	30	31	32	33	34
8	9					
35	36					

Encryption

Step 1: Translate the plaintext letters into numbers using the mapping $A \to 0, B \to 1, \ldots, Z \to 25$, and space $\to$ 26.0 $\to$ 27, ...9 $\to$ 36 Group the resulting sequence into blocks of three and denote the i^{th} block by P_i

$S-18 \quad E-4 \quad C-2 \quad R-17 \quad E-4 \quad T-19 \quad space-26 \quad C-2 \quad O-14 \quad D-3 \quad E-4 \quad 1-28$

$$P_1 = \begin{bmatrix} 18 \\ 4 \\ 2 \end{bmatrix} P_2 = \begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix} \quad P_3 = \begin{bmatrix} 26 \\ 2 \\ 14 \end{bmatrix} P_4 = \begin{bmatrix} 3 \\ 4 \\ 28 \end{bmatrix} \tag{4.1}$$

Step 2: Specify a partial affine mapping on $\mathbb{Z}_{37}$.

$$f(x) = \begin{cases} (3x+5) \bmod 37 & \text{if } x \in \{0, 1, \ldots, 19\} \\ x & \text{if } x \in \{20, 21, \ldots, 36\} \end{cases} \tag{4.2}$$

Step 3: Apply this affine transformation to each component of the blocks produced in Step 1. The transformed blocks will be written as P_i'.

For $P_1 = \begin{bmatrix} 18 \\ 4 \\ 2 \end{bmatrix}$

$$\begin{aligned} f(18) &= 19 \\ f(4) &= 17 \\ f(2) &= 11 \end{aligned} \tag{4.3}$$

$$P_1' = \begin{bmatrix} 19 \\ 17 \\ 11 \end{bmatrix}$$

For $P_2 = \begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix}$

$$P_2' = \begin{bmatrix} 16 \\ 17 \\ 2 \end{bmatrix}$$

For $P_3 = \begin{bmatrix} 26 \\ 2 \\ 14 \end{bmatrix}$

$$P_3' = \begin{bmatrix} 3 \\ 11 \\ 7 \end{bmatrix}$$

For $P_4 = \begin{bmatrix} 3 \\ 4 \\ 28 \end{bmatrix}$

$$P_4' = \begin{bmatrix} 14 \\ 17 \\ 9 \end{bmatrix}$$

Step 4: Choose an initial 3 by 3 matrix K_1 that is invertible over modulo 37.
Generate the remaining key matrices recursively by

$$K_{i+1} \equiv K_i + I(\text{mod}37)$$

Take key matrix as $K_1 = \begin{bmatrix} 1 & 5 & 6 \\ 0 & 2 & 7 \\ 0 & 0 & 3 \end{bmatrix}$

$$K_2 \equiv K_1 + I(\text{mod}37)$$

$$K_2 = \begin{bmatrix} 2 & 5 & 6 \\ 0 & 3 & 7 \\ 0 & 0 & 4 \end{bmatrix}$$

$$K_3 \equiv K_2 + I(\text{mod}37)$$

$$K_3 = \begin{bmatrix} 3 & 5 & 6 \\ 0 & 4 & 7 \\ 0 & 0 & 5 \end{bmatrix}$$

$$K_4 \equiv K_3 + I(\text{mod}37)$$

$$K_4 = \begin{bmatrix} 4 & 5 & 6 \\ 0 & 5 & 7 \\ 0 & 0 & 6 \end{bmatrix}$$

Step 5: Compute the ciphertext blocks using

$$C_i \equiv K_i \cdot P_i'(\text{mod}37)$$

$$C_1 \equiv K_1 \cdot P_1'(\text{mod}37)$$

$$C_1 = \begin{bmatrix} 1 & 5 & 6 \\ 0 & 2 & 7 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 17 \\ 11 \end{bmatrix} (\text{mod}37) = \begin{bmatrix} 170 \\ 111 \\ 33 \end{bmatrix} (\text{mod}37) = \begin{bmatrix} 22 \\ 0 \\ 33 \end{bmatrix} \tag{4.4}$$

$$C_2 = \begin{bmatrix} 2 & 5 & 6 \\ 0 & 3 & 7 \\ 0 & 0 & 4 \end{bmatrix} \begin{bmatrix} 16 \\ 17 \\ 2 \end{bmatrix} (\text{mod}37) = \begin{bmatrix} 18 \\ 28 \\ 8 \end{bmatrix} \tag{4.5}$$

$$C_3 = \begin{bmatrix} 3 & 5 & 6 \\ 0 & 4 & 7 \\ 0 & 0 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 11 \\ 7 \end{bmatrix} (\text{mod}37) = \begin{bmatrix} 32 \\ 19 \\ 35 \end{bmatrix} \tag{4.6}$$

$$C_4 = \begin{bmatrix} 4 & 5 & 6 \\ 0 & 5 & 7 \\ 0 & 0 & 6 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \\ 9 \end{bmatrix} (\text{mod}37) = \begin{bmatrix} 10 \\ 0 \\ 17 \end{bmatrix} \tag{4.7}$$

So the cipher text is now obtained as 22 0 33 18 28 8 32 19 35 10 0 17
Ciphertext is WA6S1I5T8KAR.

Decryption

Step 1: Convert the ciphertext characters back into their numerical equivalents and divide the sequence into three-element blocks, naming the i^{th} block C_i.

$W-22 \quad A-0 \quad 6-33 \quad 1-28 \quad I-8 \quad 5-32 \quad T-19 \quad 8-35 \quad K-10 \quad A-0 \quad R-17$

$$C_1 = \begin{bmatrix} 22 \\ 0 \\ 33 \end{bmatrix} \quad C_2 = \begin{bmatrix} 18 \\ 28 \\ 8 \end{bmatrix} \quad C_3 = \begin{bmatrix} 32 \\ 19 \\ 35 \end{bmatrix} \quad C_4 = \begin{bmatrix} 10 \\ 0 \\ 17 \end{bmatrix} \tag{4.8}$$

Step 2: Compute the modular inverse of every key matrix K_i in $\mathbb{Z}_{37}$.

$$K_1^{-1} = \begin{bmatrix} 1 & 16 & 10 \\ 0 & 19 & 5 \\ 0 & 0 & 25 \end{bmatrix}$$

$$K_2^{-1} = \begin{bmatrix} 19 & 30 & 30 \\ 0 & 25 & 21 \\ 0 & 0 & 28 \end{bmatrix}$$

$$K_3^{-1} = \begin{bmatrix} 25 & 15 & 23 \\ 0 & 28 & 20 \\ 0 & 0 & 15 \end{bmatrix}$$

$$K_4^{-1} = \begin{bmatrix} 28 & 9 & 17 \\ 0 & 15 & 1 \\ 0 & 0 & 31 \end{bmatrix}$$

Step 3: Recover the intermediate blocks by

$$P_i' \equiv K_i^{-1} \cdot C_i (\text{mod}37)$$

$$P_1' \equiv K_1^{-1} \cdot C_1 (\text{mod}37)$$

$$P_1' = \begin{bmatrix} 1 & 16 & 10 \\ 0 & 19 & 5 \\ 0 & 0 & 25 \end{bmatrix} \begin{bmatrix} 22 \\ 0 \\ 33 \end{bmatrix} (\text{mod}37) = \begin{bmatrix} 19 \\ 17 \\ 11 \end{bmatrix} \tag{4.9}$$

$$P_2' \equiv K_2^{-1} \cdot C_2 (\text{mod}37)$$

$$P_2' = \begin{bmatrix} 19 & 30 & 30 \\ 0 & 25 & 21 \\ 0 & 0 & 28 \end{bmatrix} \begin{bmatrix} 18 \\ 28 \\ 8 \end{bmatrix} (\text{mod}37) = \begin{bmatrix} 16 \\ 17 \\ 2 \end{bmatrix} \tag{4.10}$$

$$P_3' \equiv K_3^{-1} \cdot C_3 (\text{mod}37)$$

$$P_3' = \begin{bmatrix} 25 & 15 & 23 \\ 0 & 28 & 20 \\ 0 & 0 & 15 \end{bmatrix} \begin{bmatrix} 32 \\ 19 \\ 35 \end{bmatrix} (\text{mod}37) = \begin{bmatrix} 3 \\ 11 \\ 7 \end{bmatrix} \tag{4.11}$$

$$P_4' \equiv K_4^{-1} \cdot C_4 (\text{mod}27)$$

$$P_4' = \begin{bmatrix} 28 & 9 & 17 \\ 0 & 15 & 1 \\ 0 & 0 & 31 \end{bmatrix} \begin{bmatrix} 10 \\ 0 \\ 17 \end{bmatrix} (\text{mod}37) = \begin{bmatrix} 14 \\ 17 \\ 9 \end{bmatrix} \tag{4.12}$$

Step 4: Determine the inverse of the affine mapping used during encryption.

$$f^{-1}(y) = \begin{cases} 7y + 5(\text{mod}37) & \text{if y} \in \{0, 1, \ldots, 19\} \\ y & \text{else} \end{cases} \tag{4.13}$$

Step 5: Apply this inverse affine map to each P_{i}' to obtain the original plaintext blocks, and then convert the numbers back into characters.

For $P_1' = \begin{bmatrix} 19 \\ 17 \\ 11 \end{bmatrix}$

$$\begin{aligned} f^{-1}(19) &= 18 \\ f^{-1}(17) &= 4 \\ f^{-1}(11) &= 2 \end{aligned} \tag{4.14}$$

$$P_1 = \begin{bmatrix} 18 \\ 4 \\ 2 \end{bmatrix}$$

$$For P_2' = \begin{bmatrix} 16 \\ 17 \\ 2 \end{bmatrix} P_2 = \begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix}$$

$$For P_3' = \begin{bmatrix} 3 \\ 11 \\ 7 \end{bmatrix} P_3 = \begin{bmatrix} 26 \\ 2 \\ 14 \end{bmatrix}$$

$$For P_4' = \begin{bmatrix} 14 \\ 17 \\ 9 \end{bmatrix} P_4 = \begin{bmatrix} 3 \\ 4 \\ 28 \end{bmatrix}$$

So the plaintext is obtained as 18 4 2 17 4 19 26 2 14 3 4 28
The plaintext is SECRET CODE1.

5. Conclusion

This paper presented a hybrid encryption framework that combines Partial Affine Bijective Mapping with a Recursive Hill Cipher to enhance the security of classical cryptographic techniques. By applying partial affine bijective mapping prior to encryption and employing a recursively evolving key matrix in the Hill Cipher, the proposed scheme significantly expands the effective key space and improves resistance to classical cryptanalytic attacks such as frequency analysis and brute-force attacks. The initial implementation using modulo 27 arithmetic supports alphabetic characters and space, while the extension to modulo 37 arithmetic enables the inclusion of numeric digits from 0 to 9 without altering the core encryption structure. This extension increases the practicality of the scheme for modern alphanumeric data transmission. Overall, the proposed approach achieves improved randomness and security while maintaining computational efficiency. Future work may explore further extensions to larger symbol sets, integration with modern cryptographic primitives, and performance evaluation in real-time communication environments.

References

1. Sowmya, K.K. and Srinivas, V., *Applications of onto functions in cryptography.* Mathematics and Statistics,12(2), 135-141,(2024).

2. Lester S. Hill., *Cryptography in An Algebraic Alphabet.* The American Mathematical Monthly,36(6), 306-312,(1929).

3. Parmar, N., *Hill Cipher Modifications: A Detailed Review*. International Journal of Innovative Research in Computer and Communication Engineering, 3(3),1467-1474,(2015).

4. Saeednia., Shahrokh., *How to make the Hill cipher secure*. Cryptologia, 24, 353-360,(2000).

5. Joseph A Gallian., *Contemporary Abstract Algebra*. Chapman and Hall CRC,1-654,(2020).

6. Vasuki, B., Shobana, L., Roopa, B., *Data Encryption Using Face Antimagic Labeling and Hill Cipher*. Mathematics and Statistics, 10(2), 431-435,(2022).

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

8. Hong, M., & Chee, W.L., *Hill Cipher Modifications and Dynamic Cryptosystem Design*. 7th International Conference on Cryptography, Security and Privacy (CSP) 176-180,(2023).

9. Sowmya, K. K., & Srinivas, V., *A Novel Asymmetric Encryption Technique Using Onto Functions*. Communications in Mathematics and Applications, 15(5),(2024).

10. AbdElRahman, M.N et al., *Cryptography: A new approach of classical hill cipher*. International Jour nal of Security and Its Applications, 7(2), 179-190,(2013).

11. McAndrew, A.,*Using the hill cipher to teach cryptographic principles*. International Journal of Mathematical Education in Science and Technology,39(7) 967-979,(2008).

12. Reddy, K.A et al., *A modified hill cipher based on circulant matrices*. Procedia Technology, 4,114-118 (2012).

Sontay Manusha,
Department of Mathematics,
University College of Science, Osmania University, Hyderabad-500007, Telangana,
India.
E-mail address: sontaymanusha@gmail.com

and

Veladi Srinivas,
Department of Mathematics,
University College of Science, Saifabad, Osmania University, Hyederabad-500004, Telangana,
India.
E-mail address: srinivasmaths4141@gmail.com