# การปรับปรุงรหัสลับฮิลล์โดยอาศัยการเข้ารหัสลับเป็นคาบสองชั้น และการแปรผันความยาว

# A Modification of the Hill Cipher Based on Doubly Periodic Encryption and Length Variation

Jirawat Jantarima[1] and Thotsaphon Thongjunthug[1*]

[1]Department of Mathematics, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand

[*]Corresponding Author, Email: thotho@kku.ac.th

## บทคัดย่อ

ในงานวิจัยนี้ เราจะนำเสนอวิธีการปรับปรุงรหัสลับฮิลล์โดยอาศัยการเข้ารหัสลับเป็นคาบสองชั้น ซึ่งใช้กุญแจลับ 2 ชนิดที่มีคาบแตกต่างกันในการเข้ารหัสลับบล็อกของข้อความปกติแต่ละบล็อก และอาศัยการแปรผันความยาว เพื่อเปลี่ยนความยาวของข้อความรหัสลับให้ยาวขึ้นกว่าเดิม ทำให้ได้ข้อความรหัสลับภาคขยายมากมายหลายแบบ ซึ่งเป็นอุปสรรคต่อการที่บุคคลภายนอกจะหาขนาดของกุญแจลับได้สำเร็จ จากการศึกษาพบว่า รหัสลับฮิลล์ที่ปรับปรุงใหม่นั้นสามารถต่อต้านการโจมตีรหัสลับแบบทราบข้อความต้นฉบับ การโจมตีรหัสลับแบบทราบข้อความรหัสลับเท่านั้น และการวิเคราะห์ความถี่ ได้ดีกว่ารหัสลับฮิลล์ที่ปรับปรุงโดย Adinarayana Reddy และคณะ (2012) และใช้เนื้อที่ในการเก็บกุญแจลับน้อยกว่าที่รหัสลับฮิลล์แบบดั้งเดิมใช้

## ABSTRACT

In this research, we propose a modification of the Hill cipher using doubly periodic encryption, which requires two types of keys with different periodicity when encrypting each block of plaintext. Length variation is also used for extending the ciphertext so that there are several extended ciphertexts available, which prevent any third-party to determine the true length of secret keys successfully. Our study shows that our modified Hill cipher is more resistant to known-plaintext attack, ciphertext-only attack and frequency analysis, than the modified Hill cipher proposed by Adinarayana Reddy et al. (2012). Moreover, our modified Hill cipher requires less space for the secret keys than the classical Hill cipher.

**คำสำคัญ:** การเข้ารหัสลับ การถอดรหัสลับ รหัสลับฮิลล์ การแปรผันความยาว การเป็นคาบสองชั้น
**Keywords:** Encryption, Decryption, Hill cipher, Length variation, Double periodicity

## 1. INTRODUCTION

The Hill cipher is a polygraphic cipher which was invented by Lester S. Hill (1929). Although the Hill cipher is strong against a ciphertext-only attack, it is easily broken with a known-plaintext attack (Stallings, 2011). Thus, several researches have been done to improve the security of the Hill cipher. Acharya et al. (2009) tried to make the Hill cipher more secure by using involutory, permuted and reiterative key matrix generation to generate different keys of data encryption, thereby significantly increases its resistance to various attacks. Toorani and Falahati (2009) also proposed a modification to the Hill cipher based on affine transform and one-way hash function. Moreover, Acharya et al. (2009) presented a novel technique which is a modified version of the Hill cipher algorithm for image encryption named Hill-Shift-XOR (H-S-X) which can be applied to any type of images. Adinarayana Reddy et al. (2012) tried to improve the Hill cipher using circulant matrices, which enhances its performance against known-plaintext attack and chosen-plaintext attack. Magamba et al. (2012) proposed a variable-length key matrix obtained from a maximum distance separable (MDS) master key matrix, which used a different key matrix and this renders the ciphertext immune to known-plaintext and ciphertext-only attacks. However, it is worth pointing out that the proposed algorithm relies on many matrix transformations and this slows down the algorithm. Krishna and Madhuravani (2012) claimed that, using randomized approach, the output of the Hill cipher is randomized to generate multiple ciphertexts for one plaintext. Any one ciphertext is then used for transmission of data. As randomization of ciphertext is made, it is relatively free from known-plaintext and chosen-ciphertext attacks at slightly more computational overhead.

In this research, we will propose a modification of the Hill cipher which utilizes several techniques mentioned above. In particular, we will use doubly periodic encryption, i.e., an encryption technique based on two independent types of keys with different periodicity, and length variation for disguising the true length of ciphertext block.

## 2. RESEARCH METHODOLOGY

### 2.1 Overview

In this research, we propose a modification of the Hill cipher which consists of the following four main parts:

**1. Encryption**

(a) Choose positive integers $m, n$ such that $1 < n^2 < m$.

(b) Let $G$ be an $n \times n$ matrix such that $G$ is invertible modulo $m$ and all of its entries are incongruent modulo $m$. Let $G'$ be a matrix such that the following hold:

1. The number of rows and the number of columns of $G'$ are greater than $n$.
2. The top-left corner of $G'$ is $G$, i.e., $G' = \begin{pmatrix} G & A \\ B & C \end{pmatrix}$ for some matrices $A, B, C$.

The matrix $G'$ will be used as one of the two public keys.

(c) A sender and a recipient choose a matrix $V = (v_1 \quad v_2 \quad \cdots \quad v_n)$ such that the following hold:

1. $v_1, v_2, \ldots, v_n$ are incongruent modulo $m$;
2. $\gcd(v_i, m) = 1$ for all $i = 1, 2, \ldots, n$;
3. $\gcd(v_1 + v_2 + \cdots + v_n, m) = 1$.

The matrix $V$ will be kept as one of the two secret keys.

(d) The sender and the recipient choose a positive integer $\alpha$ such that $\gcd(\alpha, m) = 1$. The integer $\alpha$ will be used as another secret key.

(e) Calculate key $K = (v_1 v_2 \cdots v_n)G \mod m$.

(f) Let $P$ be the plaintext and $P_i$ be the $i$th block of plaintext. Each $P_i$is viewed as an $n \times 1$ matrix.

(g) Use the matrix $K$ to generate matrices $K_1, K_2, \ldots, K_{p_K}$, where $p_K$ is the number of all distinct matrices generated by $K$ (see Section 2.2 and Theorem 1). Note that all matrices $K_i$ are invertible modulo $m$.

(h) From the chosen $V$, generate $V_1, V_2, \ldots, V_{p_V}$, where $p_V$ is the number of all distinct matrices generated by $V$ (see Section 2.3 and Theorem 2). Note that $p_K \neq p_V$.

(i) For each block $P_i$ of plaintext, the associated block $C_i$ of ciphertext is calculated by

$$C_i = K_j P_i + V_k^{\mathrm{T}} \bmod m$$

where

$$j = \begin{cases} i \bmod p_K & \text{if } p_K \nmid i, \\ p_K & \text{if } p_K \mid i, \end{cases}$$

and

$$k = \begin{cases} i \bmod p_V & \text{if } p_V \nmid i, \\ p_V & \text{if } p_V \mid i. \end{cases}$$

(j) All blocks $C_i$ is then combined to form the ciphertext $C$.

**2. Extending the ciphertext**

After encryption, we find a method to extend the length of ciphertext so that we obtain an extended ciphertext $C^{\text{ext}}$ whose length is at most two times of the length of $C$ (see Section 2.4).

**3. Reducing an extended ciphertext**

After receiving an extended ciphertext $C^{\text{ext}}$, we find a method to reduce the length of extended ciphertext into the original ciphertext $C$ (see Section 2.5). The ciphertext $C$ is then split as a number of blocks $C_i$, each of which is viewed as an $n \times 1$ matrix.

**4. Decryption**

(a) Calculate $K^{-1} = (v_1 v_2 v_3 \cdots v_n)^{-1} G^{-1} \mod m$.

(b) For each block $C_i$ of ciphertext, the associated block of plaintext is calculated by

$$P_i = K_j^{-1}(C_i - V_k^{\top}) \bmod m.$$

In addition, cryptanalysis of our modified Hill cipher will be conducted in terms of frequency analysis, ciphertext-only attack, and known-plaintext attack.

**2.2 Generating matrices $K_j$**

Our procedure for generating the keys $K_j$from a given matrix $K$ consists of the following steps:

1. Set $L = 1$, $R = 2$, $U = 1$, $D = 2$, and $j = 1$.

2. Let $K_1 = K$.

3. Repeat the following:

(a) While $L \leq n$, repeat the following:

i. Let $K_{j+1}$ be the matrix obtained by swapping the $L$th column and the $R$th column of $K_j$.

ii. Increase $j$ by $1$.

iii. Increase $L$ by $1$.

iv. If $L = n$, then we set $R = 1$; otherwise, increase $R$ by $1$.

(b) If $U > n$, then this process terminates.

(c) Let $K_j$ be the matrix obtained by switching the $U$th row and the $D$th of $K$.

(d) Increase $j$ by $1$.

(e) Increase $U$ by $1$.

(f) If $U = n$, then we set $D = 1$; otherwise, we increase $D$ by $1$.

(g) Reset $L = 1$ and $R = 2$.

(h) Repeat step 3.

This procedure can be summarized as the flowchart shown in Figure 1. It should be noted that our procedure only switches rows and columns of $K$, and so $\det(K_j) = \pm\det(K)$. Hence, all matrices $K_j$ are invertible modulo $m$ if and only if $K$ is invertible modulo $m$.

**2.3 Generating matrices $V_k$**

Our procedure for generating the keys $V_k$ from a given initial matrix $V$ consists of the following steps:

1. Let $V_1 = V$.

2. Set $k = 2$ and $j = 1$.

3. Let $V$ be the row obtained by swapping the $j$th column and the $(j+1)$th column of $V_{k-1}$. For example, if $V_{k-1} = (a_1\ a_2\ a_3\ \ldots\ a_n)$, then $V' = (a_2\ a_1\ a_3\ \ldots\ a_n)$.

4. If $V' = V_1$, then our generating procedure terminates; otherwise, we define $V_k = V'$.

5. Increase $k$ by $1$.

6. If $j = n - 1$, then we reset $j = 1$; otherwise, we increase $j$ by $1$.

7. Back to step 3.

This procedure can be summarized as the flowchart shown in Figure 2.

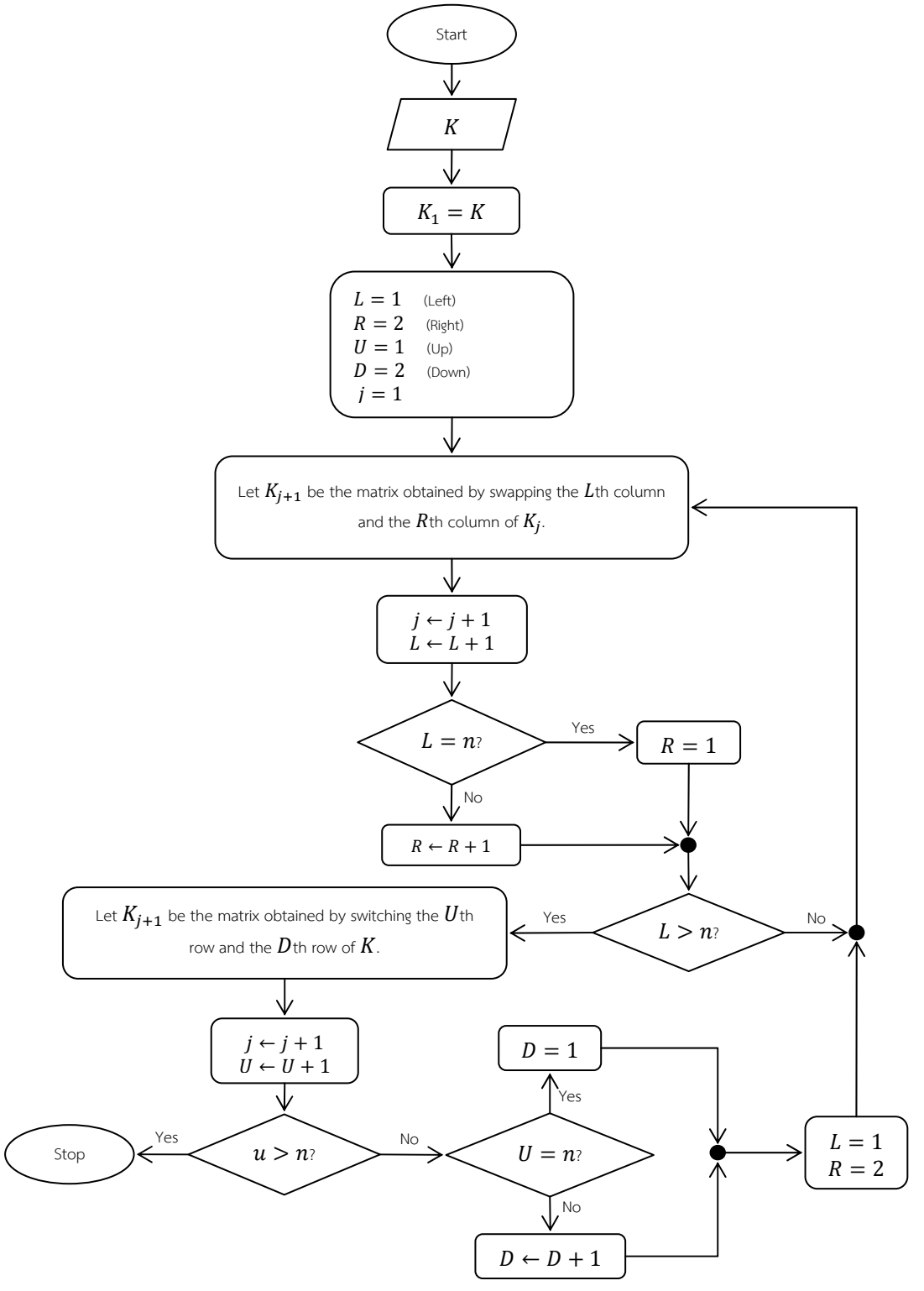


**Figure 1** The procedure for generating matrices $K_j$ from a given matrix $K$

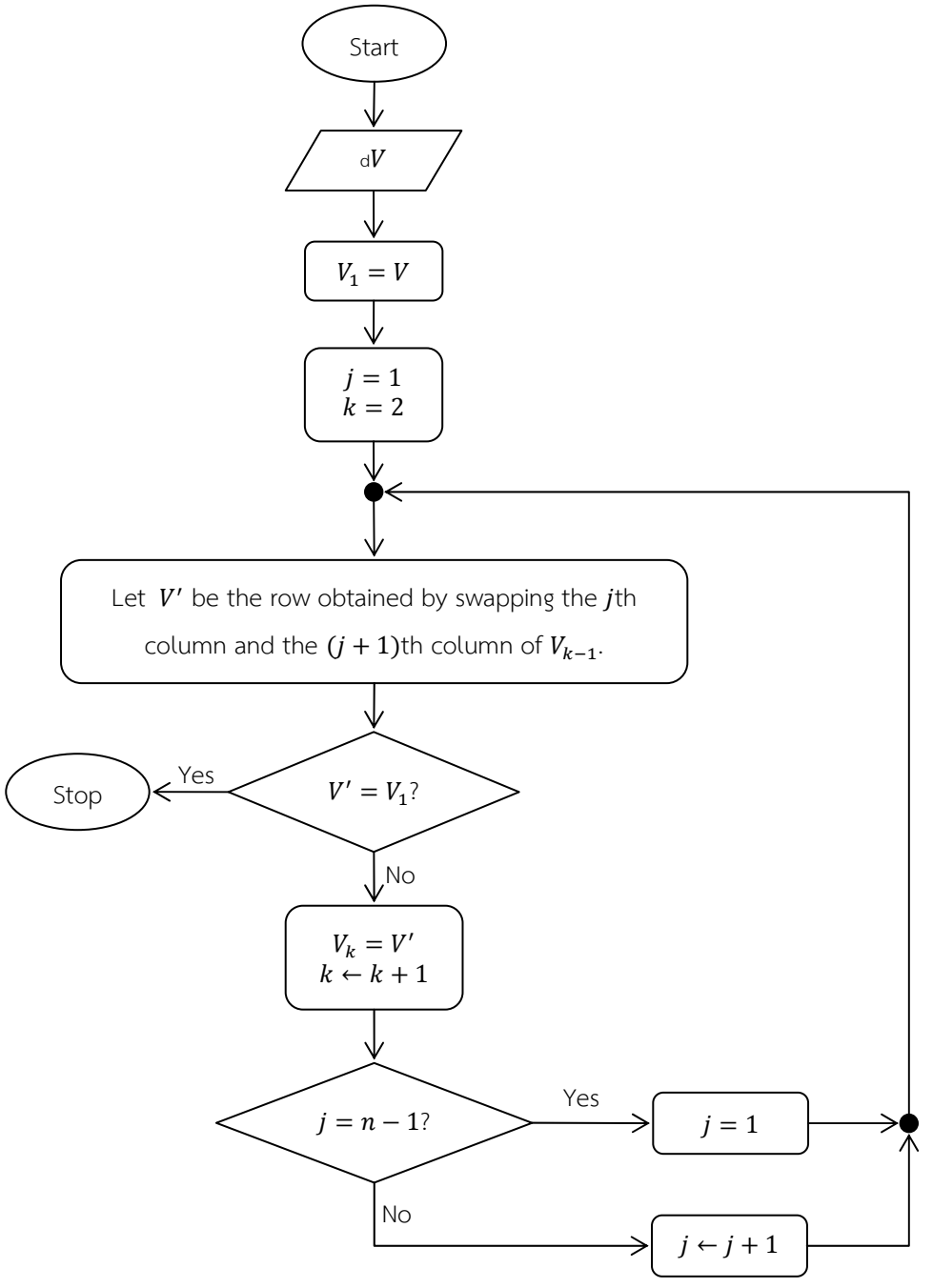


**Figure 2** The procedure for generating $V_k$ from a given matrix $V$

**2.4 Extending the Ciphertext**

The length of ciphertext can be extended using the following steps:

1. The sender chooses a positive integer $s$ and defines the set of **addenda** $\{a_1, a_2, \dots, a_s\}$ where

$$a_i = i(v_1 + v_2 + \cdots + v_n) \bmod m$$

for all $i = 1, 2, \dots, s$. The integer $s$ (with $s < m$) is used as another public key.

2. For each pair[1] of entries in the ciphertext, consider the following cases:

**Case 1.** If the pair matches any two addenda, then we insert a different addendum at the end of each entry in the pair.

**Case 2.** If exactly one entry in the pair matches an addendum, then we insert a different addendum at the end of the addendum found in the pair, and insert an addendum next to the non-addendum entry in the pair.

**Case 3.** If the pair does not match any addendum, then insertion is not required. But if we choose to do insertion, then an addendum is inserted next to each entry in the pair.

3. Multiply each entry obtained from step 2 by $\alpha$.

One can see easily that, given the ciphertext, this method can yield different extended ciphertexts, each of which has length up to two times of the length of the ciphertext. Therefore, the true

ciphertext and the length of each ciphertext block are completely disguised. Moreover, since each entry in the extended ciphertext is multiplied by $\alpha$, the set of addenda is also disguised.

**2.5 Reducing the extended ciphertext**

This method consists of the following steps:

1. Multiply each entry of the extended ciphertext by $\alpha^{-1}$, the inverse of $\alpha$ modulo $m$.

2. Considers one pair of entries in the extended ciphertext at a time. Each pair then contributes up to two entries to the ciphertext, depending on the following cases:

**Case 1.** If the pair matches any two addendum, then we discard the last entry in the pair and the rest is contributed to the ciphertext.

**Case 2.** If only one addendum is found in the pair, then only the non-addendum entry is contributed to the ciphertext.

[1] If the length of the ciphertext is odd, then the last entry is considered as a pair.

**Case 3.** If the pair does not match any addendum, then the whole pair is contributed to the ciphertext.

## 3. RESULTS

**Theorem 1.** *There are* $(n+1)^2$ *matrices which are generated by* $K$ *(of dimension* $n \times n$*), all of which are distinct modulo* $m$*.*

*Proof.* Recall that $K = (v_1 v_2 v_3 \cdots v_n)G \mod m$. Since all entries of $G$ are distinct modulo $m$ and $\gcd(v_1 v_2 \cdots v_n, m) = 1$, it follows that all entries of $K$ are also distinct modulo $m$. Moreover, since $G$ is invertible modulo $m$, it follows that $K^{-1} = (v_1 v_2 v_3 \cdots v_n)^{-1} G^{-1} \mod m$ exists, i.e., $K$ is also invertible modulo $m$.

We define the initial matrix $K_1 = K := \begin{pmatrix} k_{11} & k_{12} & k_{13} & \cdots & k_{1n} \\ k_{21} & k_{22} & k_{23} & \cdots & k_{2n} \\ k_{31} & k_{32} & k_{33} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & k_{n3} & \cdots & k_{nn} \end{pmatrix}$. Consider switching columns by the procedure mentioned in Section 2.2, we obtain the following:

Initial matrix: $K_1 = \begin{pmatrix} k_{11} & k_{12} & k_{13} & \cdots & k_{1n} \\ k_{21} & k_{22} & k_{23} & \cdots & k_{2n} \\ k_{31} & k_{32} & k_{33} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & k_{n3} & \cdots & k_{nn} \end{pmatrix}$.

Switching the columns $L = 1$ and $R = 2$: $K_2 = \begin{pmatrix} k_{12} & k_{11} & k_{13} & \cdots & k_{1n} \\ k_{22} & k_{21} & k_{23} & \cdots & k_{2n} \\ k_{32} & k_{31} & k_{33} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{n2} & k_{n1} & k_{n3} & \cdots & k_{nn} \end{pmatrix}$.

Switching the columns $L = 2$ and $R = 3$: $K_3 = \begin{pmatrix} k_{12} & k_{13} & k_{11} & \cdots & k_{1n} \\ k_{22} & k_{23} & k_{21} & \cdots & k_{2n} \\ k_{32} & k_{33} & k_{31} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{n2} & k_{n3} & k_{n1} & \cdots & k_{nn} \end{pmatrix}$.

Continue switching columns in this fashion. Then we obtain the following:

Switching the columns $L = n-1$ and $R = n$: $K_n = \begin{pmatrix} k_{12} & k_{13} & k_{14} & \cdots & k_{1n} & k_{11} \\ k_{22} & k_{23} & k_{24} & \cdots & k_{2n} & k_{21} \\ k_{32} & k_{33} & k_{34} & \cdots & k_{3n} & k_{31} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ k_{n2} & k_{n3} & k_{n4} & \cdots & k_{nn} & k_{n1} \end{pmatrix}$.

Switching the columns $L = n$ and $R = 1$: $K_{n+1} = \begin{pmatrix} k_{11} & k_{13} & k_{14} & \cdots & k_{1n} & k_{12} \\ k_{21} & k_{23} & k_{24} & \cdots & k_{2n} & k_{22} \\ k_{31} & k_{33} & k_{34} & \cdots & k_{3n} & k_{32} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ k_{n1} & k_{n3} & k_{n4} & \cdots & k_{nn} & k_{n2} \end{pmatrix}$.

Therefore, we obtain $K_1, K_2, \ldots, K_{n+1}$, which are all distinct modulo $m$, in the first round.

Consider switching in the second round. In that round, we obtain the following:

Switching the rows $U = 1$ and $D = 2$ of the initial matrix

$$K_1: K_{n+2} = \begin{pmatrix} k_{21} & k_{22} & k_{23} & \cdots & k_{2n} \\ k_{11} & k_{12} & k_{13} & \cdots & k_{1n} \\ k_{31} & k_{32} & k_{33} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & k_{n3} & \cdots & k_{nn} \end{pmatrix}.$$

Switching columns $L = 1$ and $R = 2$: $K_{n+3} = \begin{pmatrix} k_{22} & k_{21} & k_{23} & \cdots & k_{2n} \\ k_{12} & k_{11} & k_{13} & \cdots & k_{1n} \\ k_{32} & k_{31} & k_{33} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{n2} & k_{n1} & k_{n3} & \cdots & k_{nn} \end{pmatrix}$.

Switching columns $L = 2$ and $R = 3$: $K_{n+4} = \begin{pmatrix} k_{22} & k_{23} & k_{21} & \cdots & k_{2n} \\ k_{12} & k_{13} & k_{11} & \cdots & k_{1n} \\ k_{32} & k_{33} & k_{31} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{n2} & k_{n3} & k_{n1} & \cdots & k_{nn} \end{pmatrix}$.

Continue switching columns in this fashion. Then we obtain the following:

Switching columns $L = n - 1$ and $R = n$: $K_{2n+1} = \begin{pmatrix} k_{22} & k_{23} & k_{24} & \cdots & k_{2n} & k_{21} \\ k_{12} & k_{13} & k_{14} & \cdots & k_{1n} & k_{11} \\ k_{32} & k_{33} & k_{34} & \cdots & k_{3n} & k_{31} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ k_{n2} & k_{n3} & k_{n4} & \cdots & k_{nn} & k_{n1} \end{pmatrix}$.

Switching the columns $L = n$ and $R = 1$: $K_{2n+2} = \begin{pmatrix} k_{21} & k_{23} & k_{24} & \cdots & k_{2n} & k_{22} \\ k_{11} & k_{13} & k_{14} & \cdots & k_{1n} & k_{12} \\ k_{31} & k_{33} & k_{34} & \cdots & k_{3n} & k_{32} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ k_{n1} & k_{n3} & k_{n4} & \cdots & k_{nn} & k_{n2} \end{pmatrix}$.

Therefore, switching in the second round yields $n + 1$ matrices which are distinct modulo $m$.

Repeat this process until we reach the $(n + 1)$th round. In that round, we obtain the following:

Switching the rows $U = n$ and $D = 1$ of the initial matrix

$K_1$: $K_{n^2+n+1} = \begin{pmatrix} k_{n1} & k_{n2} & k_{n3} & \cdots & k_{nn} \\ k_{21} & k_{22} & k_{23} & \cdots & k_{2n} \\ k_{31} & k_{32} & k_{33} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{11} & k_{12} & k_{13} & \cdots & k_{1n} \end{pmatrix}$.

Switching columns $L = 1$ and $R = 2$: $K_{n^2+n+2} = \begin{pmatrix} k_{n2} & k_{n1} & k_{n3} & \cdots & k_{nn} \\ k_{22} & k_{21} & k_{23} & \cdots & k_{2n} \\ k_{32} & k_{31} & k_{33} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{12} & k_{11} & k_{13} & \cdots & k_{1n} \end{pmatrix}$.

Switching columns $L = 2$ and $R = 3$: $K_{n^2+n+3} = \begin{pmatrix} k_{n2} & k_{n3} & k_{n1} & \cdots & k_{nn} \\ k_{22} & k_{23} & k_{21} & \cdots & k_{2n} \\ k_{32} & k_{33} & k_{31} & \cdots & k_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{12} & k_{13} & k_{11} & \cdots & k_{1n} \end{pmatrix}$.

Continue switching columns in this fashion. Then we obtain the following:

Switching the columns $L = n$ *and* $R = 1$: $K_{n^2+2n+1} = \begin{pmatrix} k_{n2} & k_{n3} & k_{n4} & \cdots & k_{nn} & k_{n1} \\ k_{22} & k_{23} & k_{24} & \cdots & k_{2n} & k_{21} \\ k_{32} & k_{33} & k_{34} & \cdots & k_{3n} & k_{31} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ k_{12} & k_{13} & k_{14} & \cdots & k_{1n} & k_{11} \end{pmatrix}$.

Therefore, switching in the $(n + 1)$th round yields $n + 1$ matrices which are distinct modulo $m$.

It is easy to see that swapping rows causes all matrices in different rounds to be different. Moreover, in the same round, it is clear that all $n + 1$ matrices are different. Hence, there are altogether $(n + 1)(n + 1) = (n + 1)^2$ matrices generated by $K$. ❐

**Example 1.** Let $K = \begin{pmatrix} 12 & 28 & 37 \\ 19 & 33 & 18 \\ 7 & 30 & 13 \end{pmatrix}$. One can see that all entries of $K$ are distinct modulo 39. Then we have the following matrices:

$$K_1 = \begin{pmatrix} 12 & 28 & 37 \\ 19 & 33 & 18 \\ 7 & 30 & 13 \end{pmatrix} \Rightarrow K_2 = \begin{pmatrix} 28 & 12 & 37 \\ 33 & 19 & 18 \\ 30 & 7 & 13 \end{pmatrix} \Rightarrow K_3 = \begin{pmatrix} 28 & 37 & 12 \\ 33 & 18 & 19 \\ 30 & 13 & 7 \end{pmatrix} \Rightarrow K_4 = \begin{pmatrix} 12 & 37 & 28 \\ 19 & 18 & 33 \\ 7 & 13 & 30 \end{pmatrix}$$

$$K_5 = \begin{pmatrix} 19 & 33 & 18 \\ 12 & 28 & 37 \\ 7 & 30 & 13 \end{pmatrix} \Rightarrow K_6 = \begin{pmatrix} 33 & 19 & 18 \\ 28 & 12 & 37 \\ 30 & 7 & 13 \end{pmatrix} \Rightarrow K_7 = \begin{pmatrix} 33 & 18 & 19 \\ 28 & 37 & 12 \\ 30 & 13 & 7 \end{pmatrix} \Rightarrow K_8 = \begin{pmatrix} 19 & 18 & 33 \\ 12 & 37 & 28 \\ 7 & 13 & 30 \end{pmatrix}$$

$$K_9 = \begin{pmatrix} 12 & 28 & 37 \\ 7 & 30 & 13 \\ 19 & 33 & 18 \end{pmatrix} \Rightarrow K_{10} = \begin{pmatrix} 28 & 12 & 37 \\ 30 & 7 & 13 \\ 33 & 19 & 18 \end{pmatrix} \Rightarrow K_{11} = \begin{pmatrix} 28 & 37 & 12 \\ 30 & 13 & 7 \\ 33 & 18 & 19 \end{pmatrix} \Rightarrow K_{12} = \begin{pmatrix} 12 & 37 & 28 \\ 7 & 13 & 30 \\ 19 & 18 & 33 \end{pmatrix}$$

$$K_{13} = \begin{pmatrix} 7 & 30 & 13 \\ 19 & 33 & 18 \\ 12 & 28 & 37 \end{pmatrix} \Rightarrow K_{14} = \begin{pmatrix} 30 & 7 & 13 \\ 33 & 19 & 18 \\ 28 & 12 & 37 \end{pmatrix} \Rightarrow K_{15} = \begin{pmatrix} 30 & 13 & 7 \\ 33 & 18 & 19 \\ 28 & 37 & 12 \end{pmatrix} \Rightarrow K_{16} = \begin{pmatrix} 7 & 13 & 30 \\ 19 & 18 & 33 \\ 12 & 37 & 28 \end{pmatrix}.$$

❐

**Theorem 2.** *There are $n(n-1)$ matrices which are generated by $V$ (of dimension $1 \times n$), all of which are distinct modulo $m$.*

*Proof.* We define the first row matrix $V_1 = V := (v_1 \quad v_2 \quad v_3 \quad \dots \quad v_n)$. In the first round, by applying the procedure mentioned in Section 2.3, we obtain

$$\begin{aligned} V_2 &= (v_2 \quad v_1 \quad v_3 \quad v_4 \quad \dots \quad v_n) \\ V_3 &= (v_2 \quad v_3 \quad v_1 \quad v_4 \quad \dots \quad v_n) \\ V_4 &= (v_2 \quad v_3 \quad v_4 \quad v_1 \quad \dots \quad v_n) \\ &\vdots \\ V_{n-1} &= (v_2 \quad v_3 \quad v_4 \quad \dots \quad v_1 \quad v_n) \\ V_n &= (v_2 \quad v_3 \quad v_4 \quad \dots \quad v_n \quad v_1). \end{aligned}$$

Since all entries of $V$ are distinct modulo $m$, it is clear that $V_2, V_3, \dots, V_n$ are distinct modulo $m$. Therefore, we obtain $n-1$ distinct rows $V_k$ in the first round.

Consider switching in the second round. We obtain

$$\begin{aligned} V_{n+1} &= (v_3 \quad v_2 \quad v_4 \quad \dots \quad v_n \quad v_1) \\ V_{n+2} &= (v_3 \quad v_4 \quad v_2 \quad \dots \quad v_n \quad v_1) \\ V_{n+3} &= (v_3 \quad v_4 \quad v_5 \quad v_2 \quad \dots \quad v_n \quad v_1) \\ &\vdots \\ V_{2n-1} &= (v_3 \quad v_4 \quad v_5 \quad \dots \quad v_n \quad v_1 \quad v_2). \end{aligned}$$

Observe that $V_{n+1}, V_{n+2}, \dots, V_{2n-1}$ are distinct, for the location of $v_2$ in each $V_k$ varies. Therefore, we obtain $n-1$ distinct rows $V_k$ in the second round.

Continue this procedure until we reach the $(n-1)$th round. In that round, we obtain

$$\begin{aligned} V_{n^2-3n+4} &= (v_n \quad v_{n-1} \quad v_1 \quad v_2 \quad \dots \quad v_{n-2}) \\ V_{n^2-3n+5} &= (v_n \quad v_1 \quad v_{n-1} \quad v_2 \quad \dots \quad v_{n-2}) \\ V_{n^2-3n+6} &= (v_n \quad v_1 \quad v_2 \quad v_{n-1} \quad v_3 \quad \dots \quad v_{n-2}) \\ &\vdots \end{aligned}$$

$$V_{n^2-2n+2} = (v_n \quad v_1 \quad v_2 \quad \dots \quad v_{n-1}).$$

Observe that $V_{n^2-3n+4}, V_{n^2-3n+5}, \dots, V_{n^2-2n+2}$ are distinct, for the location of $v_{n-1}$ in each $V_k$ varies. Therefore, we obtain $n-1$ distinct rows $V_k$ in the $(n-1)$th round.

Consider switching in the $n$th round. We obtain

$$\begin{aligned} V_{n^2-2n+3} &= (v_1 \quad v_n \quad v_2 \quad v_3 \quad \dots \quad v_{n-1}) \\ V_{n^2-2n+4} &= (v_1 \quad v_2 \quad v_n \quad v_3 \quad \dots \quad v_{n-1}) \\ V_{n^2-2n+5} &= (v_1 \quad v_2 \quad v_3 \quad v_n \quad v_4 \quad \dots \quad v_{n-1}) \\ &\vdots \\ V_{n^2-n+1} &= (v_1 \quad v_2 \quad v_3 \quad v_4 \quad \dots \quad v_n) = V_1. \end{aligned}$$

Observe that $V_{n^2-2n+3}, V_{n^2-2n+4}, \dots, V_{n^2-n+1}$ are distinct, for the location of $a_n$ in each $V_k$ varies. Therefore, we obtain $n-1$ distinct rows $V_k$ in the $n$th round.

Clearly all matrices $V_k$ generated by different rounds are completely distinct. Therefore, switching for $n$ rounds yields $(n^2-n+1)-1 = n^2-n = n(n-1)$ distinct matrices $V_i$. ❑

**Example 2.** Let $V = (1 \quad 3 \quad 6)$. Note that all entries of $V$ are distinct modulo 11. When switching column with steps as mentioned in Section 2.3, we obtain the following:

Row 1: $V_1 = (1 \quad 3 \quad 6)$.

Row 2: $V_2 = (3 \quad 1 \quad 6)$.

Row 3: $V_3 = (3 \quad 6 \quad 1)$.

Row 4: $V_4 = (6 \quad 3 \quad 1)$.

Row 5: $V_5 = (6 \quad 1 \quad 3)$.

Row 6: $V_6 = (1 \quad 6 \quad 3)$.

We can see that swapping elements of $V_6$ again yields $V_1$, so this process terminates. ❑

As there are $(n+1)^2$ different matrices $K_j$ generated by $K$ and there are $n(n-1)$ different row matrices $V_k$ generated by $V$, this provides double periodicity for encryption. In particular, our encryption will use the same pair of the keys $K_j, V_k$ after a certain number of blocks of plaintext. To find such number, the next lemma is required.

**Lemma 1.** *For all positive integers $n > 1$, we have*

$$\operatorname{lcm}\big((n+1)^2, n(n-1)\big) = \begin{cases} n(n-1)(n+1)^2 & \text{if } n \text{ is even}, \\ \dfrac{n(n-1)(n+1)^2}{2} & \text{if } n \equiv 3 \pmod 4, \\ \dfrac{n(n-1)(n+1)^2}{4} & \text{if } n \equiv 1 \pmod 4. \end{cases}$$

*Proof.* Let $d = \gcd(n+1, n)$. Then we have $d \mid ((n+1)-n)$, and so $d = 1$. It then follows that

$$\gcd((n+1)^2, n) = 1.$$

Moreover, by the Euclidean algorithm, one can see that $\gcd\big((n+1)^2,(n-1)\big)=\gcd(n-1,4)$. Now consider the following cases:

1. If $n$ is odd, then $n-1$ is even.

(a) If $4 \mid (n-1)$ (i.e., $n \equiv 1 \pmod 4$), then we obtain $\gcd(n-1,4)=4$.

(b) If $4 \nmid (n-1)$ (i.e., $n \not\equiv 1 \pmod 4$), then we have $n \equiv 3 \pmod 4$ because $n$ is odd. Since $2 \mid (n-1)$, we obtain $\gcd(n-1,4)=2$.

2. If $n$ is even, then $n-1$ is odd. Thus, $\gcd(n-1,4)=1$.

In conclusion, we have

$$\gcd\big((n+1)^2,n(n-1)\big)=\begin{cases}1 & \text{if } n \text{ is even,}\\ 2 & \text{if } n \equiv 3 \pmod 4,\\ 4 & \text{if } n \equiv 1 \pmod 4.\end{cases}$$

The lemma then follows from the fact that

$$(n+1)^2 \cdot n(n-1)=\gcd\big((n+1)^2,n(n-1)\big)\cdot \operatorname{lcm}\big((n+1)^2,n(n-1)\big).$$

❑

**Theorem 3.** *Let $P(n)$ be the smallest number of $n$-blocks of plaintext required so that the same pair of the keys $(K_j,V_k)$ can be used. Then*

$$P(n)=\begin{cases}n(n-1)(n+1)^2+1 & \text{if } n \text{ is even,}\\ \dfrac{n(n-1)(n+1)^2}{2}+1 & \text{if } n \equiv 3 \pmod 4,\\ \dfrac{n(n-1)(n+1)^2}{4}+1 & \text{if } n \equiv 1 \pmod 4.\end{cases}$$

*Proof.* The theorem follows directly from Lemma 1 and the pigeonhole principle. ❑

**Theorem 4.** Let $\{a_1,a_2,\dots,a_s\}$ be the set of addenda as defined in Section 2.4. Then $a_1,a_2,\dots,a_s$ are incongruent modulo $m$.

*Proof.* Assume, to the contrary, that $a_i \equiv a_j \pmod m$ for some $i,j \in \{1,2,\dots,s\}$ with $i \neq j$. Then we have

$$i(v_1+v_2+\cdots+v_n) \equiv j(v_1+v_2+\cdots+v_n) \pmod m.$$

Since $\gcd(v_1+v_2+\cdots+v_n,m)=1$, this implies that $i \equiv j \pmod m$. But $1 \le i,j \le s < m$, this implies that $i=j$, a contradiction. ❑

The next example illustrates how encryption and decryption is done using our modified cipher.

**Example 3.** Choose $m = 39$, $n = 4$ and $s = 9$. Let

$$G' = \begin{pmatrix} 8 & 26 & 22 & 15 & 31 & 37 \\ 16 & 12 & 21 & 37 & 5 & 33 \\ 9 & 2 & 29 & 1 & 14 & 18 \\ 13 & 7 & 11 & 34 & 17 & 20 \\ 10 & 13 & 3 & 19 & 23 & 28 \end{pmatrix}$$

be one of the public key. One can verify that every square submatrices at the top-left corner of $G'$ is invertible modulo 39, so any one of them can be used as the key $G$. Here, as $n = 4$, we let

$$G = \begin{pmatrix} 8 & 26 & 22 & 15 \\ 16 & 12 & 21 & 37 \\ 9 & 2 & 29 & 1 \\ 13 & 7 & 11 & 34 \end{pmatrix}.$$

Let $V = (5 \quad 11 \quad 17 \quad 29)$ be one of the two secret keys. Then we let

$$K = K = (v_1 v_2 \cdots v_n)G = (5 \cdot 11 \cdot 17 \cdot 29)\begin{pmatrix} 8 & 26 & 22 & 15 \\ 16 & 12 & 21 & 37 \\ 9 & 2 & 29 & 1 \\ 13 & 7 & 11 & 34 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 26 & 25 & 33 \\ 4 & 3 & 15 & 19 \\ 12 & 20 & 17 & 10 \\ 13 & 31 & 32 & 28 \end{pmatrix} \bmod 39.$$

Consider the plaintext

$$P = (9 \quad 26 \quad 27 \quad 13 \quad 1 \quad 21 \quad 1 \quad 11 \quad 5 \quad 24 \quad 36 \quad 16 \quad 18 \quad 7 \quad 23 \quad 19).$$

As mentioned earlier, our procedures can generate $(4+1)^2 = 25$ different matrices $K_j$ and $4(4-1) = 12$ different matrices $V_k$. Here, since there are only 4 blocks of plaintext (each of length 4), we only need $K_1, \ldots, K_4$ and $V_1, \ldots, V_4$ for encryption.

Encrypting each block of plaintext, we obtain

$$C_1 = K_1 P_1^{\mathrm{T}} + V_1^{\mathrm{T}} = \begin{pmatrix} 2 & 26 & 25 & 33 \\ 4 & 3 & 15 & 19 \\ 12 & 20 & 17 & 10 \\ 13 & 31 & 32 & 28 \end{pmatrix}\begin{pmatrix} 9 \\ 26 \\ 27 \\ 13 \end{pmatrix} + \begin{pmatrix} 5 \\ 11 \\ 17 \\ 29 \end{pmatrix} \equiv \begin{pmatrix} 9 \\ 36 \\ 25 \\ 35 \end{pmatrix} \pmod{39}$$

$$C_2 = K_2 P_2^{\mathrm{T}} + V_2^{\mathrm{T}} = \begin{pmatrix} 26 & 2 & 25 & 33 \\ 3 & 4 & 15 & 19 \\ 20 & 12 & 17 & 10 \\ 31 & 13 & 32 & 28 \end{pmatrix}\begin{pmatrix} 1 \\ 21 \\ 1 \\ 11 \end{pmatrix} + \begin{pmatrix} 11 \\ 5 \\ 17 \\ 29 \end{pmatrix} \equiv \begin{pmatrix} 38 \\ 4 \\ 26 \\ 10 \end{pmatrix} \pmod{39}$$

$$C_3 = K_3 P_3^{\mathrm{T}} + V_3^{\mathrm{T}} = \begin{pmatrix} 26 & 25 & 2 & 33 \\ 3 & 15 & 4 & 19 \\ 20 & 17 & 12 & 10 \\ 31 & 32 & 13 & 28 \end{pmatrix}\begin{pmatrix} 5 \\ 24 \\ 36 \\ 16 \end{pmatrix} + \begin{pmatrix} 11 \\ 17 \\ 5 \\ 29 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 21 \\ 13 \\ 35 \end{pmatrix} \pmod{39}$$

$$C_4 = K_4 P_4^{\mathrm{T}} + V_4^{\mathrm{T}} = \begin{pmatrix} 26 & 25 & 33 & 2 \\ 3 & 15 & 19 & 4 \\ 20 & 17 & 10 & 12 \\ 31 & 32 & 28 & 13 \end{pmatrix}\begin{pmatrix} 18 \\ 7 \\ 23 \\ 19 \end{pmatrix} + \begin{pmatrix} 11 \\ 17 \\ 29 \\ 5 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 26 \\ 30 \\ 1 \end{pmatrix} \pmod{39}.$$

Therefore, the ciphertext is

$$C = (9 \quad 36 \quad 25 \quad 35 \quad 38 \quad 4 \quad 26 \quad 10 \quad 15 \quad 21 \quad 13 \quad 35 \quad 8 \quad 26 \quad 30 \quad 1).$$

Define the set of addenda $A = \{a_1, a_2, \ldots, a_s\}$ where $a_i = i(v_1 + v_2 + \cdots + v_n) \bmod m$. We have

$$\begin{aligned}
a_1 &= 1(5+11+17+29) = 23 \mod 39\\
a_2 &= 2(5+11+17+29) = 7 \mod 39\\
a_3 &= 3(5+11+17+29) = 30 \mod 39\\
a_4 &= 4(5+11+17+29) = 14 \mod 39\\
a_5 &= 5(5+11+17+29) = 37 \mod 39\\
a_6 &= 6(5+11+17+29) = 21 \mod 39\\
a_7 &= 7(5+11+17+29) = 5 \mod 39\\
a_8 &= 8(5+11+17+29) = 28 \mod 39\\
a_9 &= 9(5+11+17+29) = 12 \mod 39.
\end{aligned}$$

Therefore, we have $A = \{23,\ 7,\ 30,\ 14,\ 37,\ 21,\ 5,\ 28,\ 12\}$.

Extending the ciphertext using the set $A$, first we obtain

$$C' = (9\ \ 7\ \ 36\ \ 23\ \ 28\ \ 25\ \ 14\ \ 35\ \ 38\ \ 21\ \ 37\ \ 26\ \ 10\ \ 15\ \ 5\ \ 21\ \ 37\ \ 13\ \ 35\ \ 8\ \ 26\ \ 30\ \ 23\ \ 1\ \ 5)$$

as one of possible results after insertion. Suppose that $\alpha = 7$ is chosen as another secret key. Then the extended ciphertext is

$$C^{\text{ext}} = \alpha C' = (24\ \ 10\ \ 18\ \ 5\ \ 1\ \ 19\ \ 20\ \ 11\ \ 32\ \ 30\ \ 25\ \ 28\ \ 26\ \ 31\ \ 27\ \ 35\ \ 30\ \ 25\ \ 13\ \ 11\ \ 17\ \ 26\ \ 15\ \ 5\ \ 7\ \ 35) \bmod 39,$$

which is sent to the recipient.

For the recipient, in order to decrypt the message, the extended ciphertext needs to be reduced first. Multiplying $C^{\text{ext}}$ by $\alpha^{-1} = 28$, we obtain

$$\alpha^{-1}C^{\text{ext}} = C' = (9\ \ 7\ \ 36\ \ 23\ \ 28\ \ 25\ \ 14\ \ 35\ \ 38\ \ 21\ \ 37\ \ 26\ \ 10\ \ 15\ \ 5\ \ 21\ \ 37\ \ 13\ \ 35\ \ 8\ \ 26\ \ 30\ \ 23\ \ 1\ \ 5) \bmod 39.$$

After eliminating all addenda, we finally have

$$C^{\text{rdc}} = (9\ \ 36\ \ 25\ \ 35\ \ 38\ \ 4\ \ 26\ \ 10\ \ 15\ \ 21\ \ 13\ \ 35\ \ 8\ \ 26\ \ 30\ \ 1) = C,$$

i.e., the true ciphertext is obtained.

Decrypting each block of ciphertext, we have

$$P_1 = K_1^{-1}(C_1^{\mathrm{T}} - V_1^{\mathrm{T}}) = \begin{pmatrix} 32 & 34 & 30 & 26 \\ 17 & 1 & 25 & 1 \\ 5 & 2 & 31 & 36 \\ 1 & 24 & 33 & 7 \end{pmatrix} \left( \begin{pmatrix} 9 \\ 36 \\ 25 \\ 35 \end{pmatrix} - \begin{pmatrix} 5 \\ 11 \\ 17 \\ 29 \end{pmatrix} \right) \equiv \begin{pmatrix} 9 \\ 26 \\ 27 \\ 13 \end{pmatrix} \pmod{39}$$

$$P_2 = K_2^{-1}(C_2^{\mathrm{T}} - V_2^{\mathrm{T}}) = \begin{pmatrix} 17 & 1 & 25 & 1 \\ 32 & 34 & 30 & 26 \\ 5 & 2 & 31 & 36 \\ 1 & 24 & 33 & 7 \end{pmatrix} \left( \begin{pmatrix} 38 \\ 4 \\ 26 \\ 10 \end{pmatrix} - \begin{pmatrix} 11 \\ 5 \\ 17 \\ 29 \end{pmatrix} \right) \equiv \begin{pmatrix} 1 \\ 21 \\ 1 \\ 11 \end{pmatrix} \pmod{39}$$

$$P_3 = K_3^{-1}(C_3^{\mathrm{T}} - V_3^{\mathrm{T}}) = \begin{pmatrix} 17 & 1 & 25 & 1 \\ 5 & 2 & 31 & 36 \\ 32 & 34 & 30 & 26 \\ 1 & 24 & 33 & 7 \end{pmatrix} \left( \begin{pmatrix} 15 \\ 21 \\ 13 \\ 35 \end{pmatrix} - \begin{pmatrix} 11 \\ 17 \\ 5 \\ 29 \end{pmatrix} \right) \equiv \begin{pmatrix} 5 \\ 24 \\ 36 \\ 16 \end{pmatrix} \pmod{39}$$

$$P_4 = K_4^{-1}(C_4^{\mathrm{T}} - V_4^{\mathrm{T}}) = \begin{pmatrix} 17 & 1 & 25 & 1 \\ 5 & 2 & 31 & 36 \\ 1 & 24 & 33 & 7 \\ 32 & 34 & 30 & 26 \end{pmatrix} \left( \begin{pmatrix} 8 \\ 26 \\ 30 \\ 1 \end{pmatrix} - \begin{pmatrix} 11 \\ 17 \\ 29 \\ 5 \end{pmatrix} \right) \equiv \begin{pmatrix} 18 \\ 7 \\ 23 \\ 19 \end{pmatrix} \pmod{39}.$$

Therefore, we again obtain the plaintext

$$P = (9 \quad 26 \quad 27 \quad 13 \quad 1 \quad 21 \quad 1 \quad 11 \quad 5 \quad 24 \quad 36 \quad 16 \quad 18 \quad 7 \quad 23 \quad 19).$$

❑

## 4. DISCUSSION

In this section, we will discuss some benefits provided by our modified Hill cipher towards certain cryptological aspects.

### 4.1 Frequency analysis

By calculating the frequency of each digit in the plaintext $P$, ciphertext $C$ and the extended ciphertext $C^{\mathrm{ext}}$ illustrated in Example 3, we find that our modified Hill cipher can manipulate all digits so that the frequency of each digit in the plaintext, ciphertext and extended ciphertext cannot be mutually compared (see Figure 3). Hence, our modified Hill cipher is resistant to frequency analysis attack similarly to the original Hill cipher.

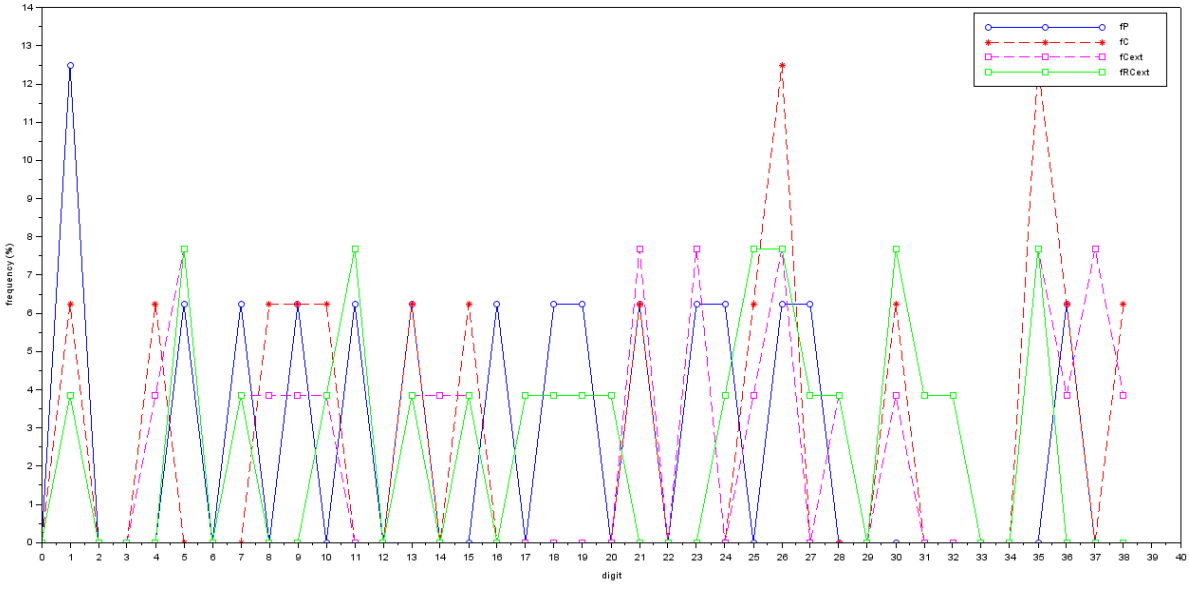


**Figure 3** Frequency analysis of digits in $P$ (blue), $C$ (red), $C'$ (magenta) and $C^{\mathrm{ext}}$ (green)

**4.2 Determining the length of plaintext block**

Although the square matrix $G$ used to generate the initial key $K$ is a submatrix of the public key $G'$, we can choose $G'$ so that there can be several possibilities for such $G$, as illustrated in Example 3. This therefore prevents an opponent from knowing the exact value of $n$ (the dimension of $G$, the length of $V$, the length of plaintext block and the length of ciphertext block), and so finding the initial matrices $K$ and $V$ by brute force is impossible. Even if the entire extended ciphertext is intercepted, its length still depends on the choice of extended ciphertext made by the sender. Hence, the dimension $n$ cannot be determined immediately as a factor of the length of extended ciphertext unless the extended ciphertext is correctly reduced.

**4.3 Determining the ciphertext**

In order to obtain the correct ciphertext, the set $A$ of addenda must be correctly determined first. As $s$ (the size of $A$) is known publicly, the opponent may carry frequency analysis to determine all $s$ most frequently seen digits in the extended ciphertext (see Figure 4). Nevertheless, to obtain all correct addenda, the secret key $\alpha$ is required. Note that $\gcd(\alpha, m) = 1$, so there are $\phi(m)$ (the Euler's phi function of $m$) possible values which can be chosen as $\alpha$. Moreover, since the secret key $V$ is unknown to the opponent, generating the set $A$ directly from $V$ is impossible.

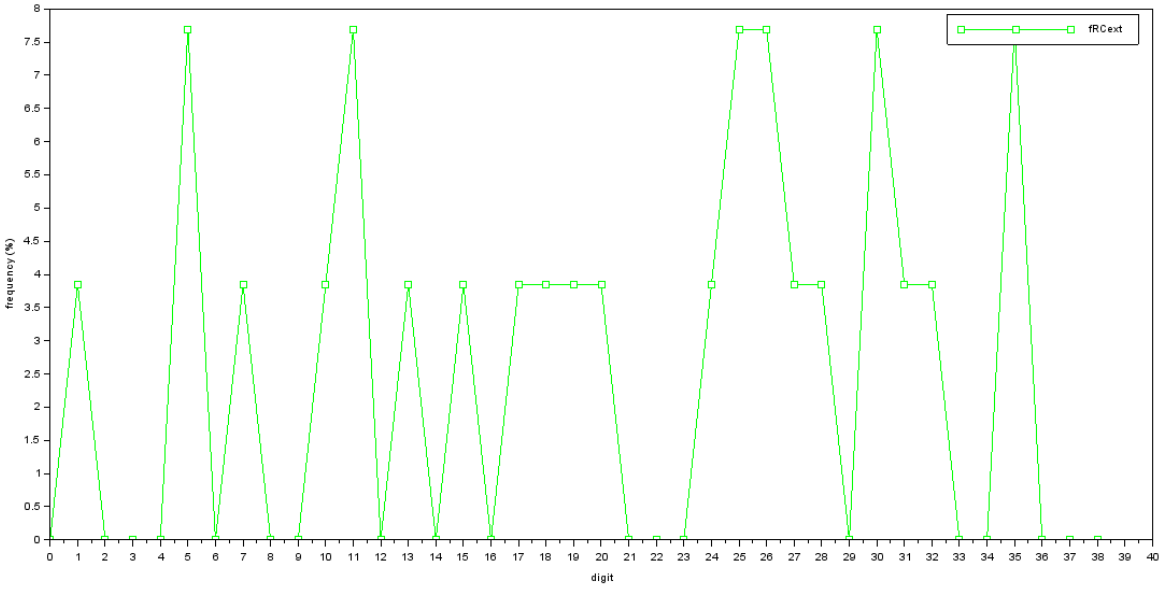


**Figure 4** Frequency analysis of digits in the extended ciphertext $C^{\text{ext}}$

**4.4 Determining $K$ and $V$**

If somehow the opponent can determine $\alpha$, $n$ and the set $A$ of addenda successfully, then the extended ciphertext can be reduced to the ciphertext and there might be an attempt to determine the secret key $V$, which in turn would yield the key $K$. However, successful determination of $A$ will only yield the sum $v_1 + v_2 + \cdots + v_n$, and there are $m^{n-1}$ matrices $(v_1 \quad v_2 \quad \cdots \quad v_n)$ resulting in this sum. Thus, the secret key $V$ cannot be determined exactly. Furthermore, since $K = (v_1 v_2 \cdots v_n)G$ but $V$ is unknown to the opponent, the key $K$ also cannot be determined exactly.

**4.5 Ciphertext-only attack**

Ciphertext-only attack is an attack where the opponent knows only the encryption algorithm and the ciphertext, and so it is the easiest attack to defend against (Stallings, 2011).

Suppose that the opponent can successfully reduce the extended ciphertext to the ciphertext. If the opponent attempts to attack using only the knowledge of a ciphertext block, say, $C_1$, then from the encryption algorithm, we have

$$C_1 = K_1 P_1 + V_1^{\mathrm{T}} = KP_1 + V^{\mathrm{T}} = (v_1 v_2 \cdots v_n)GP_1 + \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \bmod m. \tag{1}$$

Since the opponent cannot determine $V$ successfully and the plaintext block $P_1$ (of length $n$) is unknown, this yields a system of $n$ linear congruences with $2n$ variables (provided that $v_1 v_2 \cdots v_n$ is regarded as a variable). Such system cannot have a unique solution; thus, the opponent cannot obtain the plaintext in this way.

Alternatively, the opponent may ease the attack by using the fact that some blocks of plaintext are encrypted using the same pair of the keys $(K_j, V_k)$. By Theorem 3, this situation can occur only when at least $\frac{n(n-1)(n+1)^2}{4} + 1$, $\frac{n(n-1)(n+1)^2}{2} + 1$, or $n(n-1)(n+1)^2 + 1$ blocks of ciphertext are intercepted, depending on $n$. In contrast, the modified Hill cipher proposed by Adinarayana Reddy et al. (2012), which uses the encryption algorithm

$$C_i = KP_i + V_i^{\mathrm{T}} \bmod m$$

where $K$ is a common key used by every plaintext block and $V_i$ is of length $n$, will be compromised when only $n$ blocks of ciphertext are intercepted. Hence, our modified Hill cipher provides higher security against ciphertext-only attack than the one of Adinarayana Reddy et al. (2012).

**4.6 Known-plaintext attack**

Known-plaintext attack is an attack where the opponent knows encryption algorithm, ciphertext, and one or more plaintext-ciphertext pairs formed with the secret key (Stallings, 2011).

Suppose that the opponent can successfully reduce the extended ciphertext to the ciphertext. If the opponent attempts to attack using the knowledge of a plaintext-ciphertext pair, say, $(P_1, C_1)$, then from the encryption algorithm (1), we will obtain a system of $n$ linear congruences with $n+1$ variables (provided that $v_1 v_2 \cdots v_n$ is regarded as a variable). Again, such system cannot have a unique solution; thus, the opponent still cannot obtain the plaintext.

Similarly to the case of ciphertext-only attack, if the opponent attempts to ease the attack using the same pair of the keys $(K_j, V_k)$, then our modified Hill cipher is more resistant to this attack than the one of Adinarayana Reddy et al. (2012), for ours will take considerably larger period for the same pair of the keys $(K_j, V_k)$ to be re-used.

**4.7 The size of secret keys**

Suppose that each block of plaintext has length $n$. The classical Hill cipher uses an $n \times n$ matrix as the secret key, and so there are $n^2$ integers for the secret key. On the other hand, the modified Hill cipher proposed by Adinarayana Reddy et al. (2012) only requires $n$ integers for the secret key. Although our modified Hill cipher requires $n+1$ integers for the secret keys (which is slightly less economical than the one of Adinarayana Reddy et al. (2012)), it can provide additional securities in several aspects, as mentioned earlier.

## 5. CONCLUSIONS

In this research, we propose a new modification of the Hill cipher using doubly periodic encryption and length variation. Our modified cipher uses the matrix $G'$ and the positive integer $s$ as the public keys, and uses the matrix $V$ and the positive integer $\alpha$ as the secret keys. Thus, our modified cipher only requires $n+1$ integers for the secret key; this is more economical than the classical Hill cipher, but is slightly less economical than the modified Hill cipher proposed by Adinarayana Reddy et al. (2012).

Combination of the secret key $V$ and the public key $G'$ provides two initial keys $K$ and $V$, both of which are then used to generate different keys $K_j$ and $V_k$ for each round of encryption. Our procedures ensure that both types of keys have different periodicity, which leads to larger period for the same pair of the keys $(K_j, V_k)$ to be re-used in encryption, and in turn minimizes the risk of ciphertext-only and known-plaintext attacks.

In addition, our modified Hill cipher introduces a method to extend the ciphertext so that there can be many possible extended ciphertexts obtained from the same ciphertext, whereas reducing any one of those extended ciphertexts always yields the same ciphertext. This procedure can disguise the length $n$, and so determination of the secret keys by brute force is thwarted. It also results in variation of the frequency of each digit, which prevents the opponent from frequency analysis attack.

## 6. ACKNOWLEDGEMENTS

The authors are grateful to Department of Mathematics, Faculty of Science, Khon Kaen University, for supporting facilities towards this research.

## 7. REFERENCES

Acharya, B., Patra, S.K. and Panda, G. (2009). Involutory permuted and reiterative key matrix generation methods for Hill cipher system. International Journal of Recent Trends in Engineering 1(4): 106-108.

Acharya, B., Shukla, S.K., Panigrahy, S.K., Patra, S.K. and Panda, G. (2009). H-S-X cryptosystem and its application to image encryption. In: Proceedings of the 2009 International Conference on Advances in Computing, Control and Telecommunication Technologies (ACT 2009), 28-29 December 2009, Trivandrum, Kerala, India. Guerrero, J.E. (ed.). IEEE Computer Society, Los Alamitos. 720-724.

Adinarayana Reddy, K., Vishnuvardhan, B., Madhuviswanatham, V. and Krishna, A.V.N. (2012). A modified Hill cipher based on circulant matrices. Procedia Technology 4: 114-118.

Hill, L.S. (1929). Cryptography in an algebraic alphabet. The American Mathematical Monthly 36(6): 306-312.

Krishna, A.V.N. and Madhuravani, K. (2012). A modified Hill cipher using randomized approach. International Journal of Computer Network and Information Security 4(5): 56-62.

Magamba, K., Kadaleka, S. and Kasambara, A. (2012). Variable-length Hill cipher with MDS key matrix. International Journal of Computer Applications 57(13): 43-45.

Stallings, W. (2011). Cryptography and Network Security: Principles and Practice. (5th ed.). Upper Saddle River: Pearson Education. pp. 60-72.

Toorani, M. and Falahati, A. (2009). A secure variant of the Hill cipher. In: Proceedings of the 14th IEEE Symposium on Computers and Communications (ISCC 2009), 5-9 July 2009, Sousse, Tunisia. Elmaghraby, A. (ed.). IEEE Computer Society, Los Alamitos. 313-316.

❑❑❑❑❑