Journal of the Nigerian Mathematical Society
Vol. 39, Issue 2, pp. 269-285, 2020

RHOTRIX-MODULES AND THE MULTI-CIPHER HILL CIPHERS

S. M. TUDUNKAYA[1] AND S. USAINI

ABSTRACT. Now a days, Hill cipher is almost relegated. It is mostly referred to as a reference or rather history material. This is due to its weaknesses in terms of security, difficulty in both the multiplication and inverse computation of matrices. This paper presented a variant of the Hill Cipher that can be used to encrypt several ciphertexts together via the concept of rhotrices. In the proposed scheme, computation of products and inverses is easier and faster since computing products and inverses of rhotrices using heart based multiplication method is known to be easier than that of matrices. Also each plaintext rhotrix is indirectly encrypted by using its own key since it is presented in a row or column major similar to a plaintext block. Therefore, the presented scheme takes care of some of the drawbacks of the classical Hill cipher.

Keywords and phrases: Hill Cipher, Modular Arithmetic, Rhotrix, Heart based multiplication
2010 Mathematical Subject Classification: 11T71; 11E45

1. INTRODUCTION

Hill cipher is a symmetric cipher in which the sender and recipient share the same key proposed first in [14]. For the Hill cipher a plaintext (the message to be transmitted or stored) is represented as a row vector (column vector can be used as well) $X = (x_1, x_2, \cdots, x_n)$ of length $n \geq 2$, where each x_i is an integer (mod 26). This plaintext X is then converted to a ciphertext (the encrypted form of a message or data) Y which is a product of an $n \times n$ invertible key matrix K and X. In other words,

$$Y = XK \pmod{26}.$$

To retrieve the plaintext,

$$X = YK^{-1} \pmod{26}$$

Received by the editors May 21, 2018; Revised August 18, 2020 ; Accepted: August 18, 2020
www.nigerianmathematicalsociety.org; Journal available online at https://ojs.ictp.it/jnms/
[1]Corresponding author

is computed [1, 8, 9, 11, 12, 16, 21].

Cryptanalysis is a branch of cryptology that deals with the breaking of a cipher to recover information or forging encrypted information that will be accepted as authentic [22]. There are various types of cryptanalysis attacks including ciphertext-only attack, known-plaintext attack, chosen-plaintext attack and chosen-ciphertext attack. However, cryptanalysis of the Hill Cipher can be achieved by obtaining one or more ciphertexts or plaintexts [11, 12, 13, 16, 21]. The security of the Hill Cipher is measured by the number of operations to be performed and the length of time needed for an attack to succeed as implied in [11, 16, 21]. The most popular attack is the brute force attack, it is achieved by searching exhaustively through the key space until the key is found. If n or more plaintexts and their corresponding ciphertexts are obtained such that n of the plaintexts are linearly independent, the linearly independent plaintexts are considered as the rows of an $n \times n$ matrix L say. The corresponding ciphertexts are considered as the rows of another $n \times n$ matrix M, then

$$LK = M$$

which means

$$K = ML^{-1}$$

since the inverse of L exists.

Several variants of the Hill Cipher have been discussed in the literature. A scheme where random permutations of columns and rows of a matrix to form a different key for each data encryption was proposed in [21]. To overcome the drawbacks of this scheme, a more secure cryptosystem with a one-way hash function was presented in [7]. The effects of change in dimension and modulus on the order of the keyspace was analysed in [12]. Another scheme for encrypting grayscale images in an alphabet of 256 symbols based on adjusting the encryption key from one block to another was provided by Isma'il *et al.* in [11]. In a recent study a modified Hill cipher using randomized approach was discussed in [5]. In a similar note, an enhanced scheme of Hill cipher based on variable modulus and algebraic alphabet to protect software copy, which uses tridiagonal matrix was presented in [10]. The cipher is hard for an adversary to break since the modulus is not a fixed number and the algebraic alphabet depends on a variety of choices. All of the choices of the modulus, the algebraic alphabet and the key matrix depend on the

machine fingerprint of the buyer.

In a recent development, a variant of Hill cipher via the concept of rhotrices was proposed in [20]. The proposed scheme ease the difficulties of computing inverses as rhotrix inverse computation is much easier than that of matrix [4, 19]. It also overcome the security flaw of the original Hill cipher where the same key matrix is used to encrypt all the plaintext blocks since each plaintext rhotrix is encrypted by using its own key. This is similar to the algorithm known as HillMRIV (abbreviation for Hill multiplying rows by initial vector) presented in [11], for which each plaintext block is encrypted by using its own key. The computation of such a unique key for each plaintext block requires a secret initial vector IV which is then multiplied with a randomly selected initial key and the multiplication results will be a unique key which can be used for encryption. The cipher provided in [20] was based on the set of integers $Z = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ and $Z_H = \{1, 2, \cdots, 26\}$ under the following assignment: $A = 1, B = 2, C = 3, \cdots, Y = 25, Z = 26$. Rhotrices with $t = 5$ entries were used there but the idea works for any t order of rhotrices. The plaintext was represented in column-major but row-major can also be used. Precisely, the whole idea was generalised as follows: denote by $RL(t, Z_m)$, the set of all invertible rhotrices over Z_m of order t. By the natural correspondence, a plaintext string over an alphabet of order m is represented as a vector over Z_m in either a column-major or a row-major. Such a vector is denoted as a rhotrix P of size t which is padded by zeros in the positions where there are no letters. Suppose a rhotrix $K \in RL(t, Z_m)$ is chosen to be the key rhotrix, compute $C = KP$ to encrypt. Then represent the product KP as a string over the same alphabet and either send or keep depending on the need. To decrypt, compute $K^{-1}C$.

In this paper, we extended the scheme presented in [20] by encrypting several messages together through the application of rhotrix-modules.

1.1 The concept of rhotrices

The concept of rhotrices was first introduced in [4]. A rhotrix is a rhomboid array of real numbers that are in some ways between

2×2 and 3×3 dimensional matrices. Thus,

$$A = \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle \tag{1}$$

where $a, b, h(A), d, e \in \mathbb{R}$, is a rhotrix. The entry at the centre of a rhotrix denoted by $h(A)$, is called heart. The sum of two rhotrices A and B is given by

$$\begin{aligned} A + B &= \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle + \left\langle \begin{array}{ccc} & f & \\ g & h(B) & j \\ & k & \end{array} \right\rangle \\ &= \left\langle \begin{array}{ccc} & a+f & \\ b+b & h(A)+h(B) & d+j \\ & e+k & \end{array} \right\rangle \end{aligned} \tag{2}$$

It can be observed that this addition is commutative. Let G be the set of all such A as defined in (1) above. Then the sum

$$\begin{aligned} A + (-A) &= \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle + \left\langle \begin{array}{ccc} & -a & \\ -b & -h(A) & -d \\ & -e & \end{array} \right\rangle \\ &= \left\langle \begin{array}{ccc} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{array} \right\rangle \end{aligned} \tag{3}$$

is the zero of G, meaning that $-A$ is the additive inverse of A. Let α be a scalar, the scalar multiplication was defined as

$$\alpha A = \alpha \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & \alpha a & \\ \alpha b & \alpha h(A) & \alpha d \\ & \alpha e & \end{array} \right\rangle. \tag{4}$$

The product of two rhotrices A and B is given by

$$\begin{aligned} A \bullet B &= \left\langle \begin{array}{ccc} & a & \\ b & h(A) & d \\ & e & \end{array} \right\rangle \bullet \left\langle \begin{array}{ccc} & f & \\ g & h(B) & j \\ & k & \end{array} \right\rangle \\ &= \left\langle \begin{array}{ccc} & ah(B)+fh(A) & \\ bh(B)+gh(A) & h(A)h(B) & dh(B)+jh(A) \\ & eh(B)+kh(A) & \end{array} \right\rangle. \end{aligned} \tag{5}$$

This multiplication is said to be "heart-oriented" and is also commutative. An alternative method for rhotrix multiplication known as "row-column multiplication" was proposed in [6]. But the former

multiplication method will be adopted through out this paper.

The identity of G with respect to heart-oriened multiplication method is given by

$$I = \left\langle \begin{array}{ccc} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{array} \right\rangle. \tag{6}$$

If

$$A \bullet B = \left\langle \begin{array}{ccc} & 0 & \\ 0 & 1 & 0 \\ & 0 & \end{array} \right\rangle, \tag{7}$$

then

$$B = A^{-1} = -\frac{1}{h(A)^2} \left\langle \begin{array}{ccc} & a & \\ b & -h(A) & d \\ & e & \end{array} \right\rangle \tag{8}$$

where $h(A) \neq 0$.
It can be observed that the operations were defined over base rhotrices (3-dimensional rhotrices) but these operations also hold on the set of general rhotrices. A general rhotrix is a rhotrix with t entries as defined in [3] as follows

$$A(n) = \left\langle \begin{array}{ccccccc} & & & a_1 & & & \\ & & a_2 & a_3 & a_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ a_{\left\{\frac{t+1}{2}\right\}-n\backslash 2} & \cdots & \cdots & a_{\left\{\frac{t+1}{2}\right\}} & \cdots & \cdots & a_{\left\{\frac{t+1}{2}\right\}+n\backslash 2} \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & a_{t-3} & a_{t-2} & a_{t-1} & & \\ & & & a_t & & & \end{array} \right\rangle \tag{9}$$

where $t = \frac{1}{2}(n^2+1)$, $\quad n \in 2Z^+ + 1$ and $n\backslash 2$ is the integer value upon division of n by 2.
In a similar note, modular arithmetic with respect to addition and multiplication of rhotrices modulo n was presented in [18]. Thus, a rhotrix

$$M = \left\langle \begin{array}{ccccccc} & & & m_1 & & & \\ & & m_2 & m_3 & m_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ m_\alpha & \cdots & \cdots & m_\beta & \cdots & \cdots & m_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & m_{t-3} & m_{t-2} & m_{t-1} & & \\ & & & m_t & & & \end{array} \right\rangle \tag{10}$$

where $\alpha = \frac{n^2-2n+5}{4}$, $\beta = \frac{1}{4}(n^2+3)$, $\pi = \frac{n^2+2n+1}{4}$ for which addition $(+)$ and multiplication $(\bullet)$ of such rhotrices are done modulo n was defined as a modulo rhotrix in [18]. If the set of all such M is denoted by S, then the zero element of S is

$$0 = \left\langle \begin{array}{ccccccc} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0_\alpha & \cdots & \cdots & 0_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & 0_t & & & \end{array} \right\rangle \tag{11}$$

and the multiplicative identity is

$$I = \left\langle \begin{array}{ccccccc} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0_\alpha & \cdots & \cdots & 1_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & 0_t & & & \end{array} \right\rangle. \tag{12}$$

But, if $n = p$, the multiplicative inverse of

$$A = \left\langle \begin{array}{ccccccc} & & & a_1 & & & \\ & & a_2 & a_3 & a_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ a_\alpha & \cdots & \cdots & a_\beta & \cdots & \cdots & a_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & a_{t-3} & a_{t-2} & a_{t-1} & & \\ & & & a_t & & & \end{array} \right\rangle \tag{13}$$

will be

$$B = \left\langle \begin{array}{ccccccc} & & & b_1 & & & \\ & & b_2 & b_3 & b_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ b_\alpha & \cdots & \cdots & b_\beta & \cdots & \cdots & b_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & b_{t-3} & b_{t-2} & b_{t-1} & & \\ & & & b_t & & & \end{array} \right\rangle \tag{14}$$

such that for each i, $i = 1, 2, \cdots, t$

$$a_i b_\beta + b_i a_\beta \equiv 0 \quad mod \quad p \tag{15}$$

except where $i = \beta$ which is

$$a_\beta b_\beta \equiv 1 \quad mod \quad p. \tag{16}$$

The idea of defining a rhotrix whose entries are also rhotrices was presented first in [19]. Suppose $R_1, \ldots, R_t$ are rhotrices of the same size, then

$$\alpha_t = \left\langle \begin{array}{ccccccc} & & & R_1 & & & \\ & & R_2 & R_3 & R_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ R_\alpha & \cdots & \cdots & R_\beta & \cdots & \cdots & R_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & R_{t-3} & R_{t-2} & R_{t-1} & & \\ & & & R_t & & & \end{array} \right\rangle \tag{17}$$

is called a rhotrix rhotrix. The addition of two rhotrix-rhotrices α_t and

$$\beta_t = \left\langle \begin{array}{ccccccc} & & & B_1 & & & \\ & & B_2 & B_3 & B_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ B_\alpha & \cdots & \cdots & B_\beta & \cdots & \cdots & B_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & B_{t-3} & B_{t-2} & B_{t-1} & & \\ & & & B_t & & & \end{array} \right\rangle \tag{18}$$

is done component wise as indicated in (2) above. The additive identity of the set $R_t[R]$ of all rhotrix-rhotrices of size t is

$$0_A = \left\langle \begin{array}{ccccccc} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0_\alpha & \cdots & \cdots & 0_\beta & \cdots & \cdots & 0_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & 0_t & & & \end{array} \right\rangle \tag{19}$$

where for each i, 0_i is the zero rhotrix. The inverse of α_t with respect to addition is

$$-\alpha_t = \left\langle \begin{array}{ccccccccc} & & & & -R_1 & & & & \\ & & & -R_2 & -R_3 & -R_4 & & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & \\ -R_\alpha & \cdots & \cdots & & -R_\beta & \cdots & \cdots & -R_\pi & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & & & \\ & & -R_{t-3} & -R_{t-2} & -R_{t-1} & & & & \\ & & & & -R_t & & & & \end{array} \right\rangle. \tag{20}$$

The pair $(R_t[R], +)$ consisting of the set $R_t[R]$ together with the operation $(+)$ of rhotrix rhotrix addition is a group. The product of two rhotrix-rhotrices α_t and β_t is given by

$$\alpha_t \bullet \beta_t = \left\langle \begin{array}{ccccccccc} & & & & C_1 & & & & \\ & & & C_2 & C_3 & C_4 & & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & \\ C_\alpha & \cdots & \cdots & & C_\beta & \cdots & \cdots & C_\pi & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & & & \\ & & C_{t-3} & C_{t-2} & C_{t-1} & & & & \\ & & & & C_t & & & & \end{array} \right\rangle \tag{21}$$

such that when $i = \beta$

$$R_\beta B_\beta = C_\beta$$

and for each $i \neq \beta$

$$R_i B_\beta + B_i R_\beta = C_i.$$

If k is a scalar, the scalar multiplication of k and α_t is

$$k\alpha_t = \left\langle \begin{array}{ccccccccc} & & & & kR_1 & & & & \\ & & & kR_2 & kR_3 & kR_4 & & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & & \\ kR_\alpha & \cdots & \cdots & & kR_\beta & \cdots & \cdots & kR_\pi & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & & & \\ & & kR_{t-3} & kR_{t-2} & kR_{t-1} & & & & \\ & & & & kR_t & & & & \end{array} \right\rangle. \tag{22}$$

Also, if A is a rhotrix, the scalar multiplication of A and α_t is

$$A\alpha_t = \left\langle \begin{array}{ccccccc} & & & AR_1 & & & \\ & & AR_2 & AR_3 & AR_4 & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ AR_\alpha \cdots & \cdots & & AR_\beta & \cdots & \cdots & AR_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots & & \\ & & AR_{t-3} & AR_{t-2} & AR_{t-1} & & \\ & & & AR_t & & & \end{array} \right\rangle. \quad (23)$$

The multiplicative identity of a rhotrix rhotrix of size t is a rhotrix rhotrix of the form

$$I_{rr} = \left\langle \begin{array}{ccccccc} & & & 0_1 & & & \\ & & 0_2 & 0_3 & 0_4 & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0_\alpha \cdots & \cdots & & I_\beta & \cdots & \cdots & 0_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots & & \\ & & 0_{t-3} & 0_{t-2} & 0_{t-1} & & \\ & & & 0_t & & & \end{array} \right\rangle \quad (24)$$

such that for each $i \neq \beta$, 0_i is the zero rhotrix and when $i = \beta$, I_i is the identity rhotrix. The set $R_t[R]$ together with the operations $(+)$ and $(\bullet)$ of rhotrix-rhotrices is a commutative ring with identity. The multiplicative inverse of α_t is

$$\alpha_t^{-1} = -R_\beta^{-2} \left\langle \begin{array}{ccccccc} & & & R_1 & & & \\ & & R_2 & R_3 & R_4 & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ R_\alpha \cdots & \cdots & & R_\beta & \cdots & \cdots & R_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots & & \\ & & R_{t-3} & R_{t-2} & R_{t-1} & & \\ & & & R_t & & & \end{array} \right\rangle. \quad (25)$$

Lemma 1.1: Let A be a rhotrix, then by [2] for any integer m

$$A^m = (h(A))^{m-1} \left\langle \begin{array}{ccc} & ma & \\ mb & h(A) & md \\ & me & \end{array} \right\rangle \quad (26)$$

Let m and n be integers, then the following properties of rhotrix exponent rules hold for any rhotrix R as presented in [2].

(a) $R^m \circ R^n = R^{m+n}$,
(b) $\frac{R^m}{R^n} = R^{m-n}$, provided $h(R) \neq 0$,
(c) $(R^m)^{1/n} = R^{\frac{m}{n}}$,
(d) $(R^m)^n = R^{mn}$
(e) $(kR)^m = k^m R^m$, (where k is a scalar)

(f) $R^0 = I$, (where I is the identity of R),
(g) $R^{-1} = \frac{I}{R} = I \circ R^{-1}$, provided $h(R) \neq 0$,
(h) $R^m = 0$, provided $h(R) = 0$ and $m \geq 2$.

The remaining part of the paper was organised as follows: We introduced some preliminary results in Section 2. In Section 3 the proposed scheme was presented and its advantages in comparison to the original Hill cipher were discussed. Also, an illustrative example was provided in order to test our proposition. In Section 4, we gave a concluding remark.

2. PRELIMINARY

We introduce the following important notations before presenting the scheme.

(1) Let B be a rhotrix, then
  (i) $B^m = B \times B \times B \cdots \ m - times$
  (ii) If A and B^m are rhotrices of the same size then $\frac{A}{B^m} = AB^{-m}$ where

$$B^{-m} = B^{-1(m)} = (B^m)^{-1}.$$

(2) For $a, b \in Z_{26}$, $\frac{a}{b} = a\frac{1}{b} = ab^{-1} \ mod \ 26$.

Definition 1: A multicipher Hill cipher is defined as a Hill Cipher that contains a collection of various cipher texts to be encrypted by a collection of different keys.

3. THE PROPOSED SCHEME

The proposed scheme was presented in the following theorem.

Theorem 1: (Multi-cipher Hill Cipher) Let $P_1, P_2, ..., P_t \in P$ be different plaintexts rhotrices of the same size $t = \frac{1}{2}(n^2 + 1), \quad n \in 2Z^+ + 1$ such that the plaintexts are represented in the column major and each entry along the column major of each P_i is a numerical representation of an English alphabet, unoccupied positions in each P_i are padded with zero. Let $K_1, K_2, ..., K_t \in K$ be unique key rhotrices such that $(h(K_\beta), 26) = 1$, then if the cipher text is given by $C = KP \bmod 26$, the plaintext is given by $P = K^{-1}C$.

Proof: Let $\alpha = \frac{n^2-2n+5}{4}$, $\beta = \frac{1}{4}(n^2+3)$ and $\pi = \frac{n^2+2n+1}{4}$ such that

$$P = \left\langle \begin{array}{ccccccc} & & & P_1 & & & \\ & & P_2 & P_3 & P_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ P_\alpha & \cdots & \cdots & P_\beta & \cdots & \cdots & P_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & P_{t-3} & P_{t-2} & P_{t-1} & & \\ & & & P_t & & & \end{array} \right\rangle \tag{27}$$

$$K = \left\langle \begin{array}{ccccccc} & & & K_1 & & & \\ & & K_2 & K_3 & K_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ K_\alpha & \cdots & \cdots & K_\beta & \cdots & \cdots & K_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & K_{t-3} & K_{t-2} & K_{t-1} & & \\ & & & K_t & & & \end{array} \right\rangle \tag{28}$$

where $P_1, P_2, ..., P_t$ are plaintext rhotrices of the same size and $K_1, K_2, ..., K_t$ are unique key rhotrices of the same size such that $(h(K_\beta), 26) = 1$.

Let the cipher text be given by

$$C = KP = \left\langle \begin{array}{ccccccc} & & & K_1 & & & \\ & & K_2 & K_3 & K_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ K_\alpha & \cdots & \cdots & K_\beta & \cdots & \cdots & K_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & K_{t-3} & K_{t-2} & K_{t-1} & & \\ & & & K_t & & & \end{array} \right\rangle$$

$$\bullet \left\langle \begin{array}{ccccccc} & & & P_1 & & & \\ & & P_2 & P_3 & P_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ P_\alpha & \cdots & \cdots & P_\beta & \cdots & \cdots & P_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & P_{t-3} & P_{t-2} & P_{t-1} & & \\ & & & P_t & & & \end{array} \right\rangle \tag{29}$$

$$= \left\langle \begin{array}{ccccccc} & & & C_1 & & & \\ & & C_2 & C_3 & C_4 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ C_\alpha & \cdots & \cdots & CP_\beta & \cdots & \cdots & C_\pi \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & C_{t-3} & C_{t-2} & C_{t-1} & & \\ & & & C_t & & & \end{array} \right\rangle \ mod\ 26$$

such that for each i, $i = 1, 2, \cdots, t$

$$C_i = P_i K_\beta + K_i P_\beta \; mod \; 26 \tag{30}$$

except for

$$C_\beta = P_\beta K_\beta \; mod \; 26 \tag{31}$$

Now by (8) above,

$$K^{-1} = K_\beta^{-2} \left\langle \begin{array}{ccccccc} & & & -K_1 & & & \\ & & -K_2 & -K_3 & -K_4 & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ -K_\alpha & \cdots & \cdots & K_\beta & \cdots & \cdots & -K_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & -K_{t-3} & -K_{t-2} & -K_{t-1} & & \\ & & & -K_t & & & \end{array} \right\rangle \; mod \; 26 \tag{32}$$

If

$$K^{-1}C = \left\langle \begin{array}{ccccccc} & & & P_1 & & & \\ & & P_2 & P_3 & P_4 & & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ P_\alpha & \cdots & \cdots & P_\beta & \cdots & \cdots & P_\pi \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & P_{t-3} & P_{t-2} & P_{t-1} & & \\ & & & P_t & & & \end{array} \right\rangle = P \; mod \; 26 \tag{33}$$

then for each i, $i = 1, 2, \cdots, t$

$$P_i = \frac{-K_i}{K_\beta^2}(P_\beta K_\beta) + (P_i K_\beta^2 + K_i P_\beta)\frac{K_\beta}{K_\beta^2} \; mod \; 26 \tag{34}$$

except for β where

$$P_\beta = \frac{(P_\beta K_\beta)K_\beta}{K_\beta^2} \; mod \; 26 \tag{35}$$

This proves the theorem.

3.1 Keyspace of the scheme

Definition 3.1: Consider the ring Z_n for an integer n. Let R_{Z_n} be the set of all rhotrices of the same size t defined on Z_n under the addition and multiplication of rhotrices mod n. Then R_{Z_n} is called a rhotrix-module such that the addition is defined by

$$R_{Z_n} \times R_{Z_n} \to R_{Z_n} : (r_1, r_2) \to r_1 + r_2$$

and the multiplication by

$$R_{Z_n} \times R_{Z_n} \to R_{Z_n} : (n, r) \to nr.$$

The ideas provided in [17] were also found very important for the development of the following results:

Theorem 3.1: Let $R_{z_{26}}$ be the set of all rhotrices of the same size t defined over Z_{26}, then the triple $(R_{z_{26}}, +, \cdot)$ where $(+)$ and $(\cdot)$ denote the addition and multiplication of rhotrices mod 26 is a commutative ring with identity.

Proof: The proof follows from equations $(2-5, 10-12)$ and the discussions corresponding to them. Moreover, the closure with respect to addition and multiplication mod 26 reveals that distributive property holds.

Theorem 3.2: Let $M_{z_{26}}$ be the set of all rhotrix-modules defined over $R_{z_{26}}$ such that for all $\lambda, \mu \in M_{z_{26}}$ and $J, K \in R_{z_{26}}$ where $(+)$ and $(\cdot)$ denote the addition and multiplication of rhotrices mod 26

(i) $(M_{z_{26}}, +)$ is an abelian group,
(ii) $(J+K)\cdot\lambda = J\cdot\lambda + K\cdot\lambda$ and $J\cdot(\lambda+\mu) = J\cdot\lambda + J\cdot\mu$,
(iii) $(J\cdot K)\cdot\lambda = J\cdot(K\cdot\lambda)$,
(iv) $1\lambda = \lambda$.

Clearly this result holds by the discussions provided in section one above. More precisely, the proof follows from equations (2), (5) and $(18-24)$.

This means $M_{z_{26}}$ is an $R_{z_{26}}$-module. Without going into the details of the Mathematics but assuming all properties of a module, it can be seen clearly that Z_{26} is embedded in $R_{z_{26}}$ and for each t the key space is abundantly rich.

3.2 Advantages

The variant of the Hill Cipher presented here offers some improvements over that where matrices are used (easier computation of products and inverses etc). The proposed scheme provides the possibility of encrypting several ciphertexts together. As a result of difficulties in the computation of inverses for matrices, the idea of using involutory rhotrices was suggested in [15], this in turn reduces the size of the keyspace. But for this method, computation of products and that of inverses is easier [16], while factorization is expected to be more difficult than that of matrices. It has a richer keyspace since $M_{z_{26}}$ is an $R_{z_{26}}$-module and the multiplication here is commutative.

3.3 Illustrative example

The set

$$Z_{26} = \{0, 1, 2, 3, ..., 25\}$$

with the following assignment:

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

is used. Also, all additions and multiplications are those of rhotrices modulo 26.

Note that the choice of the order t of rhotrices depends on the length and amount of messages under consideration. The plaintext is represented in the column major throughout but row major can as well be used. The position that is not occupied is padded with either 0 or a zero rhotrix depending on the nature of the position.

For $t = 5$, suppose

$$P_5 = \left\langle \left\langle \begin{matrix} 0 & \begin{matrix} P \\ U \\ T \end{matrix} & 0 \end{matrix} \right\rangle \quad \begin{matrix} \left\langle \begin{matrix} 0 & \begin{matrix} N \\ O \\ T \end{matrix} & 0 \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & \begin{matrix} U \\ S \\ E \end{matrix} & 0 \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} & 0 \end{matrix} \right\rangle \end{matrix} \quad \left\langle \begin{matrix} 0 & \begin{matrix} T \\ A \\ P \end{matrix} & 0 \end{matrix} \right\rangle \right\rangle, \tag{36}$$

then by the above assignment

$$P_5 = \left\langle \left\langle \begin{matrix} 0 & \begin{matrix} 16 \\ 21 \\ 20 \end{matrix} & 0 \end{matrix} \right\rangle \quad \begin{matrix} \left\langle \begin{matrix} 0 & \begin{matrix} 14 \\ 15 \\ 20 \end{matrix} & 0 \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & \begin{matrix} 21 \\ 19 \\ 5 \end{matrix} & 0 \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} & 0 \end{matrix} \right\rangle \end{matrix} \quad \left\langle \begin{matrix} 0 & \begin{matrix} 20 \\ 1 \\ 16 \end{matrix} & 0 \end{matrix} \right\rangle \right\rangle. \tag{37}$$

If

$$K = \left\langle \left\langle \begin{matrix} 11 & \begin{matrix} 4 \\ 5 \\ 2 \end{matrix} & 1 \end{matrix} \right\rangle \quad \begin{matrix} \left\langle \begin{matrix} 7 & \begin{matrix} 8 \\ 3 \\ 4 \end{matrix} & 9 \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 2 & \begin{matrix} 3 \\ 11 \\ 9 \end{matrix} & 3 \end{matrix} \right\rangle \\ \left\langle \begin{matrix} 0 & \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} & 0 \end{matrix} \right\rangle \end{matrix} \quad \left\langle \begin{matrix} 4 & \begin{matrix} 12 \\ 7 \\ 6 \end{matrix} & 15 \end{matrix} \right\rangle \right\rangle. \tag{38}$$

Then

$$C = KP_5 = \left\langle \left\langle \begin{matrix} 17 & \begin{matrix}4\\14\\4\end{matrix} & 4 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 12 & \begin{matrix}2\\1\\18\end{matrix} & 5 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 0 & \begin{matrix}0\\14\\22\end{matrix} & 2 \end{matrix} \right\rangle \right\rangle \left\langle \begin{matrix} 0 & \begin{matrix}0\\0\\0\end{matrix} & 0 \end{matrix} \right\rangle$$
$$= \left\langle \left\langle \begin{matrix} Q & \begin{matrix}D\\N\\D\end{matrix} & D \end{matrix} \right\rangle \quad \left\langle \begin{matrix} L & \begin{matrix}B\\A\\R\end{matrix} & E \end{matrix} \right\rangle \quad \left\langle \begin{matrix} Z & \begin{matrix}Z\\N\\V\end{matrix} & B \end{matrix} \right\rangle \right\rangle. \tag{39}$$

Going by the above discussions we got

$$K^{-1} = \left\langle \left\langle \begin{matrix} 11 & \begin{matrix}18\\15\\24\end{matrix} & 9 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 6 & \begin{matrix}9\\19\\1\end{matrix} & 9 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 2 & \begin{matrix}8\\21\\12\end{matrix} & 17 \end{matrix} \right\rangle \right\rangle \left\langle \begin{matrix} 0 & \begin{matrix}0\\0\\0\end{matrix} & 0 \end{matrix} \right\rangle. \tag{40}$$

Hence,

$$K^{-1}C = \left\langle \left\langle \begin{matrix} 0 & \begin{matrix}16\\21\\20\end{matrix} & 0 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 0 & \begin{matrix}21\\19\\5\end{matrix} & 0 \end{matrix} \right\rangle \quad \left\langle \begin{matrix} 0 & \begin{matrix}20\\1\\16\end{matrix} & 0 \end{matrix} \right\rangle \right\rangle \left\langle \begin{matrix} 0 & \begin{matrix}0\\0\\0\end{matrix} & 0 \end{matrix} \right\rangle = P_5. \tag{41}$$

4. CONCLUDING REMARKS

In this paper, we proposed a variant of the Hill cipher via the concept of rhotrices as presented in Theorem 1. More precisely, certain modules (Rhotrix-Modules) were used in the implementation of the proposed scheme which is a process of sending several messages together. The scheme posseses a rich keyspace (Theorems 2 and Theorem 3 and as a plaintext could be presented in either row major or column major) and in each case there are a variety of choices for the appropriate associated key.

It is well known that computing products and inverses of rhotrices using heart-oriented multiplication method is easier than that of matrices [4, 19]. Thus the proposed scheme provides easier way of computing inverses. The rhotrix factorization problem is expected to be difficult, an important problem we intend to address in the near future. In order to confirm the proposal, advantages

of the proposed algorithm over that of the classical Hill cipher are discussed and an illustrative example of the scheme was provided.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers and the handling Editor whose constructive comments and suggestions enhanced the original version of the paper.

REFERENCES

[1] A. J. Menezes, P. C. Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, Boca Raton, CRC Press, 1997.

[2] A. Mohammed, *A Note on Rhotrix Exponent Rule and it's Application to Special Series and Polynomial Equations Defined over Rhotrices*, Notes Num. Theo. Discrete Math., **13** 1-15, 2007.

[3] A. Mohammed, *Theoretical Development and Application of Rhotrices*, PhD Dissertation, University of Ilorin, Ilorin, Kwara State, Nigeria, 2011.

[4] A. O. Ajibade, *The Concept of Rhotrix in Mathematical Enrichment*, Int. J. Math. Educ. Sci. Technol., **34** 175-179, 2003.

[5] A. V. N. Krishna and K. Madhuravani, *A Modified Hill Cipher using Randomized Approach*, Int. J. Comp. Netw. Inform. Sec., **5** 56-62, 2012. DOI: 10.5815/ijcnis.2012.05.07

[6] B. Sani, *An Alternative Method for Multiplication of Rhotrices*, Int. J. Math. Educ. Sci. Tech., **35** 777-781, 2004.

[7] C. H. Lin, and C. Y. Lee, *Comments on Saeednias improved scheme for the Hill cipher*, J. Chinese Inst. Eng., **27** 743-746, 2004.

[8] C. Li, D. Zhang and G. Chen, *Cryptanalysis of an Image Encryption Scheme based on the Hill Cipher*, J. Zhejiang Uni., SCIENCE A, **9** (08) 1118-1123, 2008. DOI: 10.1631/jzus.A0720102

[9] D. R. Stinson, *Cryptography: Theory and Practice*, (fourth edition), Boca Raton, Chapman and Hall/CRC Press, 2006.

[10] H. Ning, *An Enhanced Hill Cipher and Its Application in Software Copy Protection*, J. Networks, **9** (10), 2014. DOI: 10.4304/jnw.9.10.2582-2590

[11] I. A. Ismail, M. Amin, and H. Diab, *How to Repair the Hill Cipher*, J. Zhejiang Uni., SCIENCE A, **7** (12), 2022-2030, 2006.

[12] J. Overbey, W. Traves and J. Wojdylo, *On the Keyspace of the Hill Cipher*, Cryptologia., **29** (1) 59-72, 2005. DOI: 10.1080/0161-110591893771

[13] L. Keliher, *Cryptanalysis of a Modified Hill Cipher*, Int. J. Comp. Network Sec., **2** (7) 122-126, 2010.

[14] L. S. Hill, *Cryptography in an Algebraic Alphabet*, Am. Math. Mon., **36** 306-312, 1929. https://doi.org/10.1080/00029890.1929.11986963

[15] L. S. Hill, *Concerning Certain Linear Transformation Apparatus of Cryptography*, Am. Math. Mon., **38** 135-154, 1931.

[16] M. Toorani and A. Falahati, *Secure Variant of the Hill Cipher*, Proc. IEEE Symp. Comp. Comm., Susse, Tunisia 313-316, 2009. DOI 10.1109/ISCC.2009.5202241

[17] S. Lang, *Algebra: Graduate Texts in Mathematics*, (fourth edition), New York, Springer-Verlag.

[18] S. M. Tudunkaya and S. O. Makanjuola, *Certain Construction of Finite Fields*, J. Nig. Math. Phy., **22** 95-104, 2012.

[19] S. M. Tudunkaya and S. O. Makanjuola, *On the Structure of Rhotrix Rhotrices*, J. Nig. Math. Phy., **23** 41-50, 2013.
[20] S. M. Tudunkaya, On the Hill Ciphers of Rhotrices, Afr. J. Comp. ICT, **8** (2) 109-114, 2015.
[21] S. Saeedinia, *How to make the Hill Cipher Secure*, Cryptologia, **24** (4) 353-360, 2000. https://doi.org/10.1080/01611190008984253
[22] W. Stallings, *Cryptography and Network Security: Principles and Practice* (fifth edition), Boston, Practice Hall, 2011.

DEPARTMENT OF MATHEMATICS, AHMADU BELLO UNIVERSITY, ZARIA, NIGERIA
E-mail address: tudunkayaunique@yahoo.com

DEPARTMENT OF MATHEMATICs, KANO UNIVERSITY OF SCIENCE AND TECHNOLOGY, WUDIL, NIGERIA
E-mail address: salisu.usaini@kustwudil.edu.ng