Non-singular Transformation Based Encryption Scheme

Sunil Kumar[1], Sandeep Kumar[1], Gaurav Mittal[1,2], Dharminder Dharminder[3], Shiv Narain[4]

[1] DRDO, India

[2] Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee, India

[3] Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Chennai

[4] Department of Mathematics Arya P.G. College Panipat, India

E-mail: sunilsangwan6174@gmail.com, sandeepkumar@hqr.drdo.in, gmittal@ma.iitr.ac.in, manndharminder999@gmail.com, math.shiv@gmail.com

Abstract: In this paper, we propose a novel variant of the Hill cipher based on vector spaces. In the classical Hill cipher, a non-singular matrix is used for encryption but it is well known that this cipher is vulnerable to the known-plaintext attack. In our proposed cryptosystem, we eradicate this problem by encrypting each plaintext block with a new invertible key matrix. This makes our scheme immune to all existing attacks in literature on this type of ciphers and so the resulting cipher can be used as other state-of-art block cipher. To generate the invertible matrices which serve as the dynamic keys, we make use of the vector spaces along with randomly generated basis and non-singular linear transformation. In addition to this, we also study the computational complexity of the proposed cryptosystem and compare this with the computational complexities of other schemes based on Hill cipher.

1. Introduction

There has been the requirement of secure communication since thousands of years which led the way for invention of cryptography[14, 19]. Cryptography enables two persons, let's say, Alice and Bob to communicate securely assuming the fact that channel between them is monitored by an adversary. Secure communication can be done by using the symmetric key cryptography or asymmetric key cryptography or combination of both known as hybrid cryptography [7]. In this paper, we restrict ourselves to symmetric key cryptography (in particular, Hill cipher) which involves prior sharing of a secret key between Alice and Bob. Hill cipher [9, 13]is one of the oldest known polyalphabetic cipher invented by Lester S. Hill [5], but it is well known that various attacks can be implemented on this cipher (e.g. known plaintext attack)[20]. Despite all these vulnerabilities, it is still gaining the attention of many researchers because of its simplicity, high speed, high throughput [21], ability to disguise the letter frequencies and importance in educational systems.

Now, let us mention some of the literature available in this direction. Yeh et al. [22] proposed an improvement of the Hill cipher by presenting a polygraph substitution algorithm. Although their algorithm is safe against the known-plaintext attack, but as discussed in [16], it is inefficient for bulk data and is time-consuming. Sadeenia [18] gave a way for enhancing the security of the Hill cipher by randomly permuting the rows and columns of a master key matrix and use them as a dynamic key matrix. In this scheme, both the encrypted permutation vector and encrypted plaintext are transmitted at the receiver end. Clearly, each plaintext is encrypted with the help of a new matrix but the known-plaintext attack can still be applied on the permutation vector [11], i.e. same vulnerability as in the Hill cipher. A modification of Hill cipher similar to [18] is proposed in [3]. This modification involves the use of a pseudo-random permutation generator by both the sides and sharing of necessary permutations with the receiver. Ismail et al. [6] gave *HillMRIV*, which is a variant of the Hill cipher. This variant uses a new key matrix for encrypting each plaintext block rather than using a single key matrix for the entire plaintext. This increases the security of the Hill cipher by thwarting the known-plaintext attack, but the encryption scheme has a severe issue regarding the invertibility of the key matrix [10] which is nowhere discussed in the paper. Mahmoud [12] gave a modification of the Hill cipher based on the generation of dynamic encryption key matrix by exponentiation with the help of eigenvalues. Further, circulant matrices have been employed in [16] to give another variant of Hill cipher and claimed to be secure against the chosen-plaintext

as well as known-plaintext attack. But, in [4] it has been shown that it is vulnerable to both the attacks. Acharya et al. [1] proposed an algorithm termed as AdvHill which make use of the involutory key matrix for both encryption and decryption. Since an involutory matrix is self invertible, so the computation involved in finding inverse of the key matrix is not required in this algorithm. Agrawal et al. [2] discussed a new encryption method in which the Hill cipher is generated with elliptic curves. This method increases the security but is inefficient because of the geometric structure of the elliptic curves. In this paper, we introduce a novel variant of the Hill cipher that conquers all the security snags. More specifically, we propose a vector space-based approach in which dynamic keys are produced with the help of a non-singular transformation and basis. We also show that the known-plaintext attack is no more a vulnerability in our proposed scheme. We also study the bit operation complexities of our scheme and make a comparison of the bit operations required for other variants of Hill cipher.

Paper Organisation : All the necessary definitions are presented in Section 2. Section 3 is devoted to the our novel scheme. Much required security analysis and computational costs of the scheme is discussed in Section 4 and 5, respectively. A toy example for the feel of the scheme is given in the last section.

2. Preliminaries

Definition 1. *Linear Transformation* [7]*: Let V1 and V2 be two vector spaces over the field F. A map T : V1 → V2 is termed as a linear transformation provided*

$$T(c_1\alpha_1 + c_2\alpha_2) = c_1 T(\alpha_1) + c_2 T(\alpha_2)$$

for all $\alpha_1, \alpha_2 \in V$ and $c_1, c_2 \in F$.

Definition 2. *Non-singular Linear Transformation*[7]*: A linear transformation $T : V \to V$ is non-singular, if for any $v \in V$, $T(v) = 0$ implies $v = 0$.*

Finally, let us end this section by recalling the well known classical Hill Cipher in the following subsection.

2.1. The Hill Cipher. In this cipher, before encryption, the plaintext is written into blocks of equal length say m. Then each plaintext block is encrypted using an invertible matrix of size m to obtain the corresponding ciphertext block of the same length. Decryption can be done simply by using the inverse of the matrix used for encryption.

Mathematically, encryption and decryption process in the Hill cipher are as follows: Define $P = C = (Z_{26})^m$ which means digits of the message and ciphertext are ranging from 0 to 25. Let

$$K = \{K \mid K \text{ is a inverible square matrix of order } m \text{ over } Z_{26}\}.$$

For a key $K \in K$, define the encryption and decryption functions

$$E : K \times P \to C : E(K, x) = xK,$$
$$D : K \times C \to P : D(K, y) = yK^{-1},$$

respectively, where all the calculations are performed in Z_{26}.

To make the decryption possible, it is important that the key matrix K must be invertible. But every square matrix over Z_{26} is not invertible. Further, if we consider the ring Z_p, for some prime p instead of Z_{26}, then this increases the probability of randomly choosing a matrix whose determinant is non-unit. This selection of ring also increases the size of key space [15]. If the adversary is available with ciphertexts only, then breaking the Hill cipher is an uphill task. However, the known plaintext attack still makes it most vulnerable [20]. To see this, suppose the attacker is in the possession of at least m different pairs $x_s = (x_{1s}, x_{2s}, x_{3s} \cdots, x_{ms})$ and $y_s = (y_{1s}, y_{2s}, y_{3s} \cdots, y_{ms})$, where ys are encryptions of x_s for $1 \le s \le m$. Using two square matrices $X = (x_{rs})$ and $Y = (y_{rs})$, a matrix equation $Y = XK$ can be formed, where the unknown square matrix K of order m is the key matrix. If X has inverse, then by premultiplying $Y = XK$ by X^{-1}, K can be recovered and the system will be broken. If X does not have inverse, then try another m plaintext-ciphertext pairs. This shows that the known plaintext attack can be implemented on the Hill cipher.

3. The Proposed Scheme

In this section, we introduce the novel variant of the Hill cipher based on vector spaces. Let *p* be a large prime and Fp be the corresponding field. Further let

$$V = (x_1, x_2, \cdots, x_n): x_i \in Fp, \text{ for } 1 \le i \le n,$$

be a n−dimensional vector space over the field *Fp* and $T : V \to V$ be a non-singular transformation. Since every non-singular linear transformation corresponds to a non-singular matrix over the field Fp, *T* can be seen as an element

of *GL(n, Fp)*, which is a group of all non-singular matrices of order n over the field Fp. We choose one such *T* whose order is large in *GL(n, Fp)*. Rationale behind choosing this *T* is discussed later on.

Basically, our scheme involves the following main points which will be discussed in the following subsections:

(1) Construction of a linear transformation *T* .
(2) How to write the plaintext in blocks?
(3) Whitening process before encryption.
(4) How to generate the dynamic keys?
(5) Encryption and decryption algorithms. To start with, first of all, we discuss how to select a non-singular linear transformation.

3.1. How to construct T . It is well known that the vector space of all square matrices of order n (i.e. $M(n, F)$ over a field F is isomorphic to the vector space $\text{Hom}_F(V, V)$, of all linear transformations on an n-dimensional vector space V over F [7]. Mathematically, we can write

$$M(n, F) \cong \text{Hom}_F(V, V),$$
$$M(n, \text{F}) \text{ HomF}(V, V).$$

This means, any invertible matrix in $M(n, F)$ can be seen as a non-singular linear transformation.

Example 1. *Let* $A = \begin{bmatrix} 4 & 2 \\ 0 & 3 \end{bmatrix}$ *be a 2x2 non-singular matrix over the field F5. Then the 03 transformation T on* $2-$*dimensional vector space V defined by*

$$T(a, b) = [a \ b] \begin{bmatrix} 4 & 2 \\ 0 & 3 \end{bmatrix} = (4a, 2a + 3b),$$

is an invertible transformation.

3.2. Way of writing the plaintext. Write the plaintext message in blocks of length n, where n is some positive integer (add padding if required), i.e. $m = m_1 m_2 \cdots$, where $m_i = (m_i^1, m_i^2, \dots m_i^n)$ is i^{th} message block of length n with $m_i^j \in F_p$ for all $1 \leq j \leq n$.

3.3. Whitening process. Choose a random $1 \times n$ non zero vector $I_1 = (I_1^1, I_1^2, \dots I_1^n)$ with $I_1^i \in F_p$, $1 \leq i \leq n$. This vector is used for whitening of the first message block. For this, simply add I_1 and m_1 modulo p. Let

$$m_1' = m_1 \oplus_p I_1$$

For the whitening of subsequent blocks, we make the use of the non-singular linear transformation *T* in the following manner: Let m_i be the ith, $i \geq 2$ message block and

$$Ii = T(I_{i-1}) = (I_i^1, I_i^2, \cdots, I_i^n) \ (mod \ p), \text{ for } i \geq 2,$$

i.e. I_i is obtained from I_{i-1} by applying *T* on it. Now the ith, $i \geq 2$ whitened message block is

$$m_1' = m_1 \oplus_p I_i$$

This process is included as a part of encryption to overcome the problem of a message block with all entries 0. Fig. 1, represents this process schematically, where $\oplus p$ is the same as the addition modulo *p*.
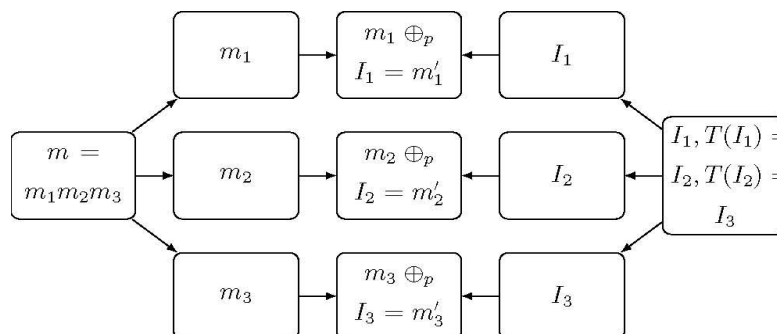

Fig. 1. Whitening Process for a Message of Three Blocks

3.4. Key Generation Scheme. Choose a random basis of V. For that, we need a non-singular square matrix over Fp. Let P be the probability of a randomly selected square matrix of order n to be non-singular over modulo p. Then we have

$$P = \frac{(p^n - 1)(p^n - p) \dots (p^n - P^{n-1})}{p^{n^2}} = \frac{p^{n^2}\left(1 - \frac{1}{p^n}\right)\left(1 - \frac{1}{p^{n-1}}\right) \dots \left(1 - \frac{1}{p}\right)}{p^{n^2}}$$

$$= \left(1 - \frac{1}{p^n}\right)\left(1 - \frac{1}{p^{n-1}}\right) \dots \left(1 - \frac{1}{p}\right)$$

which is approximately 1 for large p and finite n. Therefore, any randomly selected square matrix of order n over F_p is probably non-singular (i.e. invertible). If not, choose another random matrix. Within a few choices, we get the non-singular matrix. So, let A_1 be the chosen non-singular matrix, i.e. $A_1 \in GL(n, F_p)$. This is the key matrix for encrypting first whitened block and the set of all rows (let's say B_1) of A_1 serves the purpose of a random basis. Since T is a non-singular linear transformation, it maps basis to basis [7] and therefore by giving a random basis as a seed, it will generate a sequence of basis $\{B_2, B_3, \cdots, \}$. From this sequence of basis, we obtain a sequence of matrices in $GL(n, F_p)$ by putting the elements of Bi as the rows of Ai for $i \geq 2$ and these matrices serve as dynamic keys for the proposed algorithm. Fig. 2, represents this scheme schematically.

3.5. Encryption Algorithm. First, encrypt m$_1$ with the key matrix A$_1$ by simply multiplying both modulo p. This yields ciphertext

$$c_1 = m_1' \otimes_p A_1$$

For encrypting i^{th} ,$i \geq 2$ message block, we use the key matrix Ai defined in Subsection 3.4. Corresponding ciphertext is
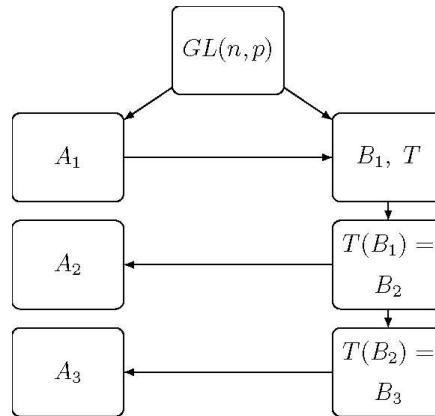
$$c_1 = m_i' \otimes_p A_i$$

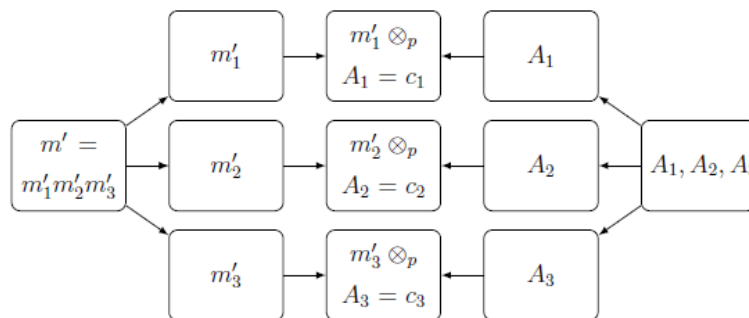Fig. 2. Key Generation Process for a Message of Three Blocks

Fig. 3. Encryption Process for a Message of Three Blocks

Fig. 3, represents this scheme schematically, where $\otimes p$ represents multiplication modulo p.

3.6. Symmetric key. Since Hill cipher is a symmetric encryption algorithm, the following three things need to be shared with the decryptor in the beginning:

(1) Initial vector.
(2) Non-singular linear transformation.
(3) Basis of the vector space.

3.7. Decryption Algorithm. Since the initial vector I_1, non-singular linear transformation T and invertible matrix A_1 are known at the receiver (say Bob) end, he calculates all the required keys and whitening vectors. To get the *i-th* plaintext block, following operation is needed to perform by the receiver:

$$m_i = \left(c_i \otimes_p A_i^{-1}\right) \ominus_p I_i,$$

where $\ominus_p$ represents subtraction modulo p.

3.8. Rationale behind choosing T. We have chosen the non-singular linear transformation T over the vector space of dimension n having large order t (by order, we mean the order of T in $GL(n, Fp)$. If this is not the case, then the key matrices may start repeating themselves before encryption of $t - 1$ blocks. To avoid this, we have chosen the non-singular transformation of large order.

4. Security Analysis

In this section, we discuss the security analysis of the proposed scheme. Our encryption scheme is such that the key matrix used to encrypt any whitened message block is invertible. In this scheme, message block with all zero entries is not encrypted to the same block because of whitening. Further, change in one entry of initial vector changes the entire ciphertext and this highlights the importance of the initial vector. Brute force complexity and resistance with various attacks are discussed in subsequent subsections.

4.1. Brute force attack. Let V be the same n-dimensional vector space over Fp considered in Section 3. Then number of basis of V are

$$N = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}).$$

Due to whitening process and dynamic key for each block, brute force complexity of the proposed scheme has enhanced considerably. In order to mount brute force attack an adversary should have knowledge of prime number p and block size n. Assuming availability of these two parameters to an adversary he needs a triplet (I, B, T), where $I \in V$ and $B, T \in GL(n, Fp)$. Thus, the total number of triplets required for brute force attack are $L = p^n \cdot N^2$. If both p and n are large, then this is very large number and makes the brute force infeasible, e.g. if $n = 128$ and $p = 29$, then $L > 2^{877}$ which is cryptographically secure even with the best available computation facility. This shows that brute force complexity of this cipher is greater than that of the classical Hill cipher.

4.2. Security against known-plaintext attack. In classical Hill cipher same matrix is used for encrypting all the blocks of a message. This causes a consequential weakness, as because of this, a system of n^2 linear equation with n^2−unknown is formed and can be solved uniquely with the help of Gauss elimination method and Cramer's rule, if coefficient matrix is non-singular. Now, we show that this type of approach is not applicable in our proposed scheme.

Suppose the attacker is available with plaintext-ciphertext pairs (m_j, c_j), $j \in J$, where J is some index set. Since different keys are used for encrypting different message blocks, so to find the key matrix used for encrypting j^{th} message block, an attacker can incorporate only one plaintext-ciphertext pair (m_j, c_j) provided corresponding initial vector is known to the attacker which itself is a difficult task. This gives the linear system of n equations with n^2 unknowns and solving this system yields infinitely many solutions. Therefore, our proposed scheme thwarts the known-plaintext attack and similarly it is secure against choosen-plaintext attack.

4.3. Completeness effect. Each letter of ciphertext block in this scheme depends on all letters of corresponding plain text block. So our proposed scheme has completeness effect.

5. Computational Costs

The total time taken by a computer for a specific task, fundamentally depends on the number of bits operations used for its execution and further, number of bits operations depend on the algorithms. But to analyze the worst case scenario, in the proposed scheme, conventional method bit operation complexity is considered which can, however, be further reduced by employing efficient algorithms [8]. Now, whenever we add, divide and multiply two numbers, then

the total numbers of bit operations depend on the bit size of these numbers. In our proposed algorithm, every number is between 0 and $p - 1$, but for worst case situation every numbers in the process will be considered of $\lfloor \log_2(p - 1) \rfloor + 1$ bits.

Let T_{Enct} and T_{Dect} signify the time taken by the proposed algorithms for encrypting and decrypting t^{th} block (with $t > 1$) of the plaintext and ciphertext, respectively. Assuming $(t - 1)^{th}$ block encryption matrix and the corresponding initial vector are given, then on neglecting the followings:

   (1) Time required for 'bookkeeping' or logical steps other than the bit operations.
   (2) Computational cost of introduced protocol,

we have:

$$T_{Enct} \approx (n^3 + n^2 - n)T^{+p} + (n^3 + 2n^2)T^{\times p}. \tag{5.1}$$

$$T_{Dect} \approx (3n^3 - n^2 - n)T^{+p} + (3n^3 + 2n^2)T^{\times p} + nT^{-1p} \tag{5.2}$$

where inverse of dynamic key matrices has been calculated using method of Gauss elimination and the time required for addition, multiplication and inverse in the finite field Fp are denoted by T^{+p}, $T^{\times p}$ and T^{-1p}, respectively. Let λ be number of bits in $p - 1$, i.e. $\lambda = \lfloor \log_2(p - 1) \rfloor + 1$. Then according to conventional method [17], we have

$$T^{+p} = O(\lambda). \tag{5.3}$$

$$T^{\times p} = O(\lambda^2) \tag{5.4}$$

$$T^{-1p} = O(\lambda^3) \tag{5.5}$$

Thus, from equations 5.1 to 5.5, it is clear that running time for encryption and decryption explicitly depend on λ (bit length of $p - 1$) and n (block size).

Let $\wp$ denotes plaintext length. Then overall time taken for encryption of the entire plaintext message is

$$T_{Total\_Enc} \approx n^2 T^{+p} + n^2 T^{\times p} + \left(\left\lceil \frac{\wp}{n} \right\rceil - 1 \right)(n^3 + n^2 - n)T^{+p} + (n^3 + 2n^2)T^{\times p} \tag{5.6}$$

Similarly, time taken for decryption of the entire ciphertext is:

$$T_{Total\_Dec} \approx n^2(2n - 1)T^{+p} + n^2(2n + 1)T^{\times p} + nT^{-1p} + \left(\left\lceil \frac{\wp}{n} \right\rceil - 1 \right) \times$$
$$\left((3n^3 - n^2 - n)T^{+p} + (3n^3 + 2n^2)T^{\times p} + nT^{-1p} \right) \tag{5.7}$$

The computational cost for encrypting/decrypting the whole plaintext/ciphertext message under the proposed scheme can be calculated by employing equations 5.1 to 5.5 in equation 5.6 and 5.7, respectively. The comparison of operations required for encryption/decryption of each plaintext/ciphertext block between our scheme and the other schemes based on the Hill cipher is given below in Table 1. It reflects that the number of operations in our proposed scheme are greater than from others schemes based on the Hill cipher.

6. Example

In this section, we discuss a toy example for the feel of our scheme. We restrain ourselves to a key matrices of order 3 and prime number $p = 29$, so that the calculations can be performed manually.

Example 2. *Let $V = \{(v_1, v_2, v_3): v_i \in F_{29}$ for $1 \leq i \leq 3\}$. Clearly $F = F_{29}$ and length of the message block to be encrypted is 3. Further, consider the non-singular linear transformation $T : V \rightarrow V$ defined by*

$$T(v_1, v_2, v_{3,}) = (v_1 + v_2, 3v_2 + v_3, v_1 - v_2 + v_3)$$

initial vector $I_1 = (2, 1, 5)$ and the random basis

$$B_1 = \{(1, 2, 0), (3, 1, 0), (1, 28, 4)\}$$

Let $m = m_1 m_2 m_3 m_4 m_5 m_6$, where

$$m_1 = (12, 0, 17), \ m_2 = (2, 7, 5), \ m_3 = (14, 17, 22)$$
$$m_4 = (0, 17, 3), \ m_5 = (0, 19, 5), \ m_6 = (8, 21, 4)$$

is the message. Initial whitening of the message yields $m_1 m_2 m_3 m_4 m_5 m_6$, where

$$m_1' = (14, 1, 22), \ m_2' = (5, 15, 11), \ m_3' = (25, 18, 23)$$
$$m_4' = (12, 21, 14), \ m_5' = (16, 13, 24), m_6' = (18, 22, 16)$$

Dynamic keys for the encryption are

$$A_1 = \begin{bmatrix} 1 & 2 & 0 \\ 3 & 1 & 0 \\ 1 & -1 & 4 \end{bmatrix} \quad A_2 = \begin{bmatrix} 3 & 6 & -1 \\ 4 & 3 & 2 \\ 0 & 1 & 6 \end{bmatrix} \quad A_3 = \begin{bmatrix} 9 & 17 & -4 \\ 7 & 11 & 3 \\ 1 & 8 & 5 \end{bmatrix}$$

$$A_4 = \begin{bmatrix} 26 & 18 & -12 \\ 18 & 7 & -1 \\ 10 & 3 & -3 \end{bmatrix} \quad A_5 = \begin{bmatrix} 15 & 13 & -4 \\ 25 & 20 & 10 \\ 13 & 6 & 4 \end{bmatrix} \quad A_6 = \begin{bmatrix} -1 & 6 & -2 \\ 16 & 12 & 15 \\ 19 & 22 & 11 \end{bmatrix}$$

Corresponding ciphertext is $c_1 c_2 c_3 c_4 c_5 c_6$ with

$$c_1 = (10, 7, 1), c_2 = (17, 28, 4), c_3 = (26, 26, 11),$$
$$c_4 = (18, 28, 25), c_5 = (7, 3, 17), c_6 = (0, 28, 6)$$

where all the operations are performed under modulo 29. Decryption can be performed easily by computing the inverses of key matrices and knowledge of initial vector.

Table 1. Bit operation comparison per block among the schemes based on the Hill cipher

Distinct Schemes	Operation	T_{Mul}	T_{Add}	T_{Inv}
Original Hill Cipher	Encryption	n^2	$n^2 - 1$	-
	Decryption	n^2	$n^2 - 1$	-
Affine Hill Cipher	Encryption	n^2	n^2	-
	Decryption	n^2	n^2	-
Lin et al.'s Scheme [11]	Encryption	$n^2 + n + 3$	$n^2 + 4$	-
	Decryption	$n^2 + n + 3$	$n^2 + 4$	1
M. Toorani and A. Falahati [21]	Encryption	$n^2 + 2n$	$n^2 + n + 1$	-
	Decryption	$n^2 + 2n$	$n^2 + n + 1$	1
Proposed Scheme	Encryption (first block)	n^2	n^2	-
	Encryption (block =1)	$n^3 + 2n^2$	$n^3 + n^2 - n$	-
	Decryption (first block)	$n^2(2n + 1)$	$n^2(2n - 1)$	n
	Decryption (block =1)	$3n^3 + 2n^2$	$3n^3 - n^2 - n$	n

7. Conclusion

In this paper, we have pointed the traditional Hill cipher algorithm and its drawbacks. To overcome the issues, we have introduced a new variant of Hill cipher. More specifically, we propose a vector space-based approach in which dynamic keys are produced with the help of a non-singular transformation and basis. This scheme is secure against the known-plaintext attack and a Brute Force attack requires $\left((p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) \right)^2$ number of key pairs generations other than initial vector or with assumption that initial vector is known to adversary, where n is the order of key matrix. Moreover, proposed framework uses linear operations i.e. matrix additions and multiplications which makes it more efficient. Thus proposed scheme advances the matrix based encryption scheme from the present state of knowledge.

References

[1]   B. Acharya, S. K. Panigrahy, S. K. Patra, and G. Panda. Image encryption using advanced hill cipher algorithm. International Journal of Recent Trends in Engineering, 1(1):663–667, 2009.

[2]   K. Agrawal and A. Gera. Elliptic curve cryptography with hill cipher generation for secure text cryptosystem. International journal of computer applications, 106(1), 2014.

[3]   A. Chefranov, A. Elci, B. Ors, and B. Preneel. Secure hill cipher modification shcm. In Proc. Of the First International Conference on Security of Information and Network, pages 34–37, 2008.

[4]   A. A. ElHabshy. Augmented hill cipher. International Journal of Network Security, 2019.

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

[6]   I. Ismail, M. Amin, and H. Diab. How to repair the hill cipher. Journal of Zhejiang University-Science A, 7(12):2022–2030, 2006.

[7]   J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. Handbook of applied cryptography. CRC press, 1996.

[8]   D. Knuth. The art of computer programming vol. 2: Seminumerical methods, 1981.

[9]   A. Krishna and K. Madhuravani. A modified hill cipher using randomized approach. International Journal of Computer Network and Information Security, 4(5):56–62, 2012.

[10] C.-q. Li, D. Zhang, and G.-r. Chen. Cryptanalysis of an image encryption scheme based on the hill cipher. Journal of Zhejiang University-Science A, 9(8):1118–1123, 2008.

[11] C.-H. Lin, C.-Y. Lee, and C.-Y. Lee. Comments on saeednia's improved scheme for the hill cipher. Journal of the Chinese institute of engineers, 27(5):743–746, 2004.

[12] A. Y. Mahmoud and A. G. Chefranov. Hill cipher modification based on eigenvalues hcm-ee. In Proceedings of the 2nd international conference on Security of information and networks, pages 164–167. ACM, 2009.

[13] A. Y. Mahmoud and A. G. Chefranov. A hill cipher modification based on eigenvalues extension with dynamic key size hcm-exdks. International Journal of Computer Network & Information Security(IJCNIS), 6(5), 2014.

[14] H. M. Mousa. Bat-genetic encryption technique. *International Journal of Intelligent Systems and Applications(IJISA)*, 11(11):1, 2019.

[15] J. Overbey, W. Traves, and J. Wojdylo. On the keyspace of the hill cipher. Cryptologia, 29(1):59–72, 2005.

[16] K. A. Reddy, B. Vishnuvardhan, A. Krishna, et al. A modified hill cipher based on circulant matrices. Procedia Technology, 4:114–118, 2012.

[17] K. H. Rosen. Elementary number theory and its applications. addision-wesley. Reading, MA, 1988.

[18] S. Saeednia. How to make the hill cipher secure. Cryptologia, 24(4):353–360, 2000.

[19] R. G. Sharma, H. Garg, and P. Dimri. An efficient (n, n) visual secret image sharing using random grids with xor recovery. International Journal of Computer Network and Information Security, 11(11):14.

[20] D. R. Stinson. Cryptography: theory and practice. Chapman and Hall/CRC, 2005.

[21] M. Toorani and A. Falahati. A secure variant of the hill cipher. In 2009 IEEE Symposium on Computers and Communications, pages 313–316. IEEE, 2009.

[22] Y.-S. Yeh, T.-C. Wu, C.-C. Chang, and W.-C. Yang. A new cryptosystem using matrix transformation. In Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology, pages 131–138. IEEE, 1991.

Authors' Profiles

Sunil Kumar is Scientist at Defence research and development organization (DRDO), Delhi, India. His research interests are cryptography, signcryption, and group rings based cryptography.

Sandeep Kumar is Scientist at Defence research and development organization, Delhi, India. He has more than six years of teaching experience in Institute of National Importance. His research area of interest are public key cryptography based on Group Rings, code based cryptography and symmetric key cryptography.

Gaurav Mittal is Scientist at Defence research and development organization, Delhi, India and Ph.D. candidate at IIT Roorkee. His research interests are algebra, cryptography, and inverse problems.

Dr. Dharminder Dharminder is working as Assistant Professor in the Department of Mathematics at Amrita Vishwa Vidyapeetham, Chennai, India. His research interests are cryptography, elliptic curve, and signcryption.

Shiv Narain received his Ph.D. from Kurukshetra University Kurukshetra, India and currently working as Assistant Professor, Post Graduate Department Of Mathematics Arya P.G. College ,Panipat India. His research interests are Group Theory, Fuzzy Set Theory, Cryptography and Fractional Calculus.