EasyChair Preprint

№ 5138

Using Boolean Rings to Reconstruct the Hill Cipher Algorithm

Rishabh Malhotra, Girish Paliwal, S. Srinivasan and Narayanaswamy Chandramowliswaran

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

March 12, 2021

Using Boolean Rings to Reconstruct the Hill Cipher Algorithm

Rishabh Malhotra (✉)
Amity University Rajasthan, 303002
rish.malhotra1996@gmail.com

Girish Paliwal
Amity University Rajasthan, 303002

S. Srinivasan
Periyar Govt Arts and Science College Cuddalore, 607001

N. Chandramowliswaran
Amity University Haryana, 122413

Abstract — In the age of ever-growing technology, information transfer is becoming more and more vulnerable. Cryptography the key which ensures secure communication. In this paper, an attempt to recreate the Hill Cipher encryption scheme has been made where the key structure is based on a group algebra **G** over the boolean ring **R**. The key idea of the proposal is to overcome the currently existing vulnerabilities in the Hill Cipher. Developed by Lester S. Hill in 1929, the Hill Cipher encryption algorithm was a key invention in the field of Cryptography in the then era. However, changing worlds and developing technologies have made it necessary to make some amendments in the currently existing algorithm. Here, we use Boolean Rings as the key matrices to make the encryption scheme stronger and more secure.

Keywords — Cyber-Security, Cryptography, Hill Cipher, Encryption, Decryption, RSA Algorithm, Substitution Cipher

1 Introduction

In 1976, Whitefield Diffie and Martin Hellman published the first practical public key cryptosystem for secure data transmission [1]. The Diffie-Hellman Algorithm was based on the discrete log problem. Since then, many public key cryptography algorithms have been created. The RSA scheme [2] discovered in 1978 by Ron Rivest, A. Shamir and Adleman was based on the factorization problem of the modulus, factorizing of mod N is an impractical task if the integer N is sufficiently large, where N is the product of two distinct large primes. Since then, many developments have been made in the field of cryptography. Elliptic Curves Cryptography, which is based on the algebraic structure of elliptic curves over finite fields, has an advantage over the non-elliptic curve cryptography with the smaller key sizes [3][4].

The key idea of this encryption scheme is based on the pre-existing Hill Cipher [5] which is a polygraphic substitution cipher based on Linear Algebra. Here, Boolean Rings have been used to reconstruct the original message text over the group algebras.

Here, in this paper, we present some new techniques to encrypt and decrypt the messages. Some basic concepts of group algebra, and linear algebra have been used and applied to make a new algorithm. The RSA Algorithm [2] has been used as the basis of the cryptosystem.

2 Literature Review

In recent past many works have been done to improve the cryptosystems using the group algebra of commutative and non-commutative rings [6] [7]. More than just the encryption and decryption of data, the secure transmission of the private key(s) is a crucial part of a cryptosystem. The threshold schemes enable a group of users to share a secret by providing each user with a share [8]. It is necessary for a good cryptosystem to be practically impossible for the attacker to break [9]. A good cryptosystem would comparatively take more time while the attacker is trying to break into it. This can either be achieved by making a moderately longer key or by creating a more advance algorithm that would make the entire cryptosystem reluctant to any damage.

Sometimes, when the user has to upload the encrypted data at a public server, only the cipher with a public key won't be able to secure the data completely. Hence, in that case, the **homomorphic encryption** comes into picture. Here, encryption is performed on an already encrypted data at the server side [8].

$$\boldsymbol{Enc}(\ldots\boldsymbol{Enc}(\boldsymbol{Enc}(\boldsymbol{m}))\ldots),\text{ where m is the message.}$$

But, in order to recover the original message, the decipher key has to be applied only once to the homomorphically encrypted data.

When it comes to the speed in the computation, the homomorphic encryption has a constraint. To remove the limitation, a new latin-squares based technique for encryption has been derived. In this algorithm, all the encryption is done through Symmetric Key Cryptography. This procedure hence increases the security of the data manifolds and also the computation is comparatively complex.

Hill Cipher sees its applications in image encryptions as well [10]. For grayscale images, the modulus will be 256 (the number of levels is considered as the number of alphabets). In the case of colour images, the image is first decomposed (R-G-B) components. Then, each component is encrypted separately. Finally, in order to get the encrypted colour image, each encrypted component is concatenated. The image encryption technique has also been proposed combining Hill Cipher with Elliptic Curve Techniques [11]. This method removes the requirement of the key matrix in inverse hence increasing the decryption speed. In Hill Cipher, the construction of keys plays an important part. Many methods to construct the keys have been made using both Classical Cipher [12] and Genetic Algorithms [13]. However, it is vulnerable to known plaintext attack. Another setback is that an invertible key matrix is needed for decryption and it is not suitable for encrypting a plaintext consisting of zeroes. [14]

.

3 Proposed Algorithm

The currently existing hill cipher has several advantages in cryptography however, it encrypts plaintext blocks to identical ciphertext blocks making it difficult to properly hide the patterns of the plain text. The proposed technique adjusts the encryption key to form a different key for each block encryption. Taking into consideration the more complex computations using the boolean rings as the base of the structure, we certainly observe a higher work factor and the examples show that this encryption scheme prevents Single Letter Frequency Distribution.

Def 1. Boolean Ring [15]

Let $\boldsymbol{X}$ be any given finite set (non-empty). Consider $\boldsymbol{\mathcal{P}}(\boldsymbol{X}) = \{\boldsymbol{set\ of\ ALL\ subsets\ of\ X}\}$

Define $\oplus$ and $\cdot$ on $\boldsymbol{\mathcal{P}}(\boldsymbol{X})$ as follows:

$$\boldsymbol{A \oplus B} = (\boldsymbol{A} - \boldsymbol{B}) \cup (\boldsymbol{B} - \boldsymbol{A})$$

$$\boldsymbol{A} \cdot \boldsymbol{B} = \boldsymbol{A} \cap \boldsymbol{B}, \qquad \boldsymbol{where\ A, B} \in \boldsymbol{\mathcal{P}}(\boldsymbol{X})$$

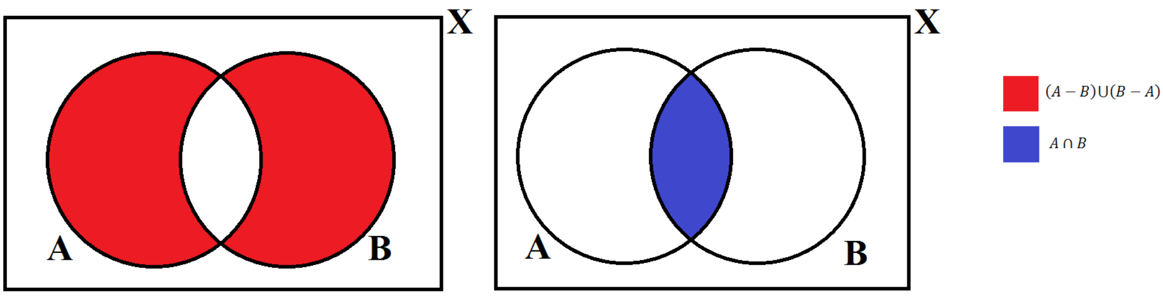

Figure 1 : Boolean Ring

This ring is:

a) Commutative

$\boldsymbol{A \oplus B = B \oplus A}$

$\boldsymbol{A \cdot B = B \cdot A}$, where $\boldsymbol{A, B} \in \boldsymbol{\mathcal{P}(X)}$

b) Associative

$\boldsymbol{A \oplus (B \oplus C) = (A \oplus B) \oplus C}$

$\boldsymbol{A \cdot (B \cdot C) = (A \cdot B) \cdot C}$, where $\boldsymbol{A, B, C} \in \boldsymbol{\mathcal{P}(X)}$

c) Distributive

$\boldsymbol{(A \oplus B) \cdot C = (A \cdot C) \oplus (B \cdot C)}$

$\boldsymbol{(A \cdot B) \oplus C = (A \oplus C) \cdot (B \oplus C)}$, where $\boldsymbol{A, B, C} \in \boldsymbol{\mathcal{P}(X)}$

The empty set ($\boldsymbol{\phi}$) is the zero of the ring.

The finite set $\boldsymbol{X}$ is the one of the ring.

Hence, $(\boldsymbol{\mathcal{P}(X)}, \oplus, \cdot, \boldsymbol{\phi}, \boldsymbol{X})$ forms a Boolean Ring.

Def 2. Multiplication of Boolean Rings

Let $\boldsymbol{\mathcal{U}} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{bmatrix}, \boldsymbol{\mathcal{V}} = \begin{bmatrix} \boldsymbol{E} & \boldsymbol{F} \\ \boldsymbol{G} & \boldsymbol{H} \end{bmatrix}$,

then the matrix multiplication is defined as follows:

$$\boldsymbol{\mathcal{U} \cdot \mathcal{V}} = \begin{bmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{E} & \boldsymbol{F} \\ \boldsymbol{G} & \boldsymbol{H} \end{bmatrix} = \begin{bmatrix} \boldsymbol{AE \oplus BG} & \boldsymbol{AF \oplus BH} \\ \boldsymbol{CE \oplus DG} & \boldsymbol{CF \oplus DH} \end{bmatrix} \qquad \langle \boldsymbol{AB = A \cdot B} \rangle$$

$$\boldsymbol{where}, \boldsymbol{A, B, C, D, E, F, G, H} \in \boldsymbol{\mathcal{P}(X)}$$

Note: While decrypting the message, the invertibility of the latin square, formed over the boolean ring R, is a necessary condition.

3.1 Encryption and Decryption Algorithm

Let $\boldsymbol{\mathcal{M}} = \begin{bmatrix} \boldsymbol{Y_1} \\ \boldsymbol{Y_2} \\ \boldsymbol{Y_3} \end{bmatrix}$ be the message that we have to encrypt.

To encrypt the message, we need a key.

Let $\boldsymbol{\mathcal{K}} = \begin{bmatrix} \boldsymbol{X \oplus AE \oplus BF} & \boldsymbol{A \oplus BG} & \boldsymbol{B} \\ \boldsymbol{E \oplus CF} & \boldsymbol{X \oplus CG} & \boldsymbol{C} \\ \boldsymbol{F} & \boldsymbol{G} & \boldsymbol{X} \end{bmatrix}$ be the Encryption key, $\boldsymbol{Det(\mathcal{K}) = X}$.

$\boldsymbol{where, A, B, C, E, F, G \in \mathcal{P}(X)}$

Define $\boldsymbol{Enc(\mathcal{M}) = \mathcal{K} \cdot \mathcal{M}}$

$$= \begin{bmatrix} \boldsymbol{X \oplus AE \oplus BF} & \boldsymbol{A \oplus BG} & \boldsymbol{B} \\ \boldsymbol{E \oplus CF} & \boldsymbol{X \oplus CG} & \boldsymbol{C} \\ \boldsymbol{F} & \boldsymbol{G} & \boldsymbol{X} \end{bmatrix} \cdot \begin{bmatrix} \boldsymbol{Y_1} \\ \boldsymbol{Y_2} \\ \boldsymbol{Y_3} \end{bmatrix} = \begin{bmatrix} \boldsymbol{Y'_1} \\ \boldsymbol{Y'_2} \\ \boldsymbol{Y'_3} \end{bmatrix} \ \boldsymbol{(say)}$$

$$= \begin{bmatrix} \boldsymbol{Y_1 \oplus BFY_1 \oplus AY_2 \oplus BGY_2 \oplus BY_3} \\ \boldsymbol{EY_1 \oplus CFY_1 \oplus Y_2 \oplus CGY_2 \oplus CY_3} \\ \boldsymbol{FY_1 \oplus GY_2 \oplus Y_3} \end{bmatrix} = \begin{bmatrix} \boldsymbol{Y'_1} \\ \boldsymbol{Y'_2} \\ \boldsymbol{Y'_3} \end{bmatrix}$$

Here,

$\boldsymbol{Y'_1} = \boldsymbol{Y_1 \oplus BFY_1 \oplus AY_2 \oplus BGY_2 \oplus BY_3}$

$\boldsymbol{Y'_2} = \boldsymbol{EY_1 \oplus CFY_1 \oplus Y_2 \oplus CGY_2 \oplus CY_3}$

$\boldsymbol{Y'_3} = \boldsymbol{FY_1 \oplus GY_2 \oplus Y_3}$

To decrypt this message,

$$\boldsymbol{D_n(\mathcal{M}) = \mathcal{K}^{-1}}$$

$$= \frac{\boldsymbol{1}}{\boldsymbol{X}} \begin{bmatrix} \boldsymbol{X} & \boldsymbol{A} & \boldsymbol{AC \oplus B} \\ \boldsymbol{E} & \boldsymbol{X \oplus AE} & \boldsymbol{C \oplus CAE \oplus BE} \\ \boldsymbol{F} & \boldsymbol{G \oplus GAE \oplus AF} & \boldsymbol{X \oplus BF \oplus CG \oplus EBG \oplus CGAE} \end{bmatrix}$$

$$= \begin{bmatrix} \boldsymbol{X} & \boldsymbol{A} & \boldsymbol{AC \oplus B} \\ \boldsymbol{E} & \boldsymbol{X \oplus AE} & \boldsymbol{C \oplus CAE \oplus BE} \\ \boldsymbol{F} & \boldsymbol{G \oplus GAE \oplus AF} & \boldsymbol{X \oplus BF \oplus CG \oplus EBG \oplus CGAE} \end{bmatrix} \qquad |\because \boldsymbol{X\ is\ the\ one\ in\ the\ ring\ \mathcal{P}(X)}|$$

Here, as mentioned, that in a Boolean Ring, the one $(\mathbf{1})$ of the ring is the finite set $\boldsymbol{X}$. In order to maintain the invertibility of the matrix, it is important that such a matrix is constructed with determinant $= \boldsymbol{X}$. This determinant being equal to the one of the finite ring ensures the invertibility and hence the decryption is possible without the loss of data.

Some of the methods to construct such matrices have been discussed below.

3.2 To Construct a square matrix with determinant = X using triangular matrices

Let X be any given finite set (non-empty).
Consider $\mathcal{P}(X) = \{set\ of\ ALL\ subsets\ of\ X\}$
Define $\oplus$ and $\cdot$ on $\mathcal{P}(X)$ as follows:

$$A \oplus B = (A - B) \cup (B - A) = B \oplus A$$
$$A \cdot B = A \cap B = B \cdot A, \qquad where\ A, B \in \mathcal{P}(X)$$

Define two square matrices $\boldsymbol{\mathcal{U}}$ and $\boldsymbol{\mathcal{V}}$

$$\boldsymbol{\mathcal{U}} = \begin{bmatrix} X & A & B \\ \phi & X & C \\ \phi & \phi & X \end{bmatrix}; \ \boldsymbol{\mathcal{V}} = \begin{bmatrix} X & \phi & \phi \\ E & X & \phi \\ F & G & X \end{bmatrix} \ where\ A, B, C, E, F, G \in \mathcal{P}(X)$$

$$\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}} = \begin{bmatrix} X \oplus AE \oplus BF & \phi \oplus AX \oplus BG & \phi \oplus BX \\ \phi \oplus E \oplus CF & \phi \oplus X \oplus CG & \phi \oplus \phi \oplus C \\ \phi \oplus XF & \phi \oplus G & X \end{bmatrix}$$

$$\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}} = \begin{bmatrix} X \oplus AE \oplus BF & A \oplus BG & B \\ E \oplus CF & X \oplus CG & C \\ F & G & X \end{bmatrix} \qquad \rightarrow (\boldsymbol{K})$$

$\det(\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}})$

$$= [(X \oplus AE \oplus BF)(X \oplus CG \oplus CG)] \oplus [(A \oplus BG)(E \oplus CF \oplus CF)] \oplus [B(EG \oplus CFG \oplus F \oplus CGF)]$$
$$= X \oplus AE \oplus BF \oplus AE \oplus BGE \oplus BEG \oplus BF$$
$$= X$$

Example:
Assume $X = \{1,2,3,4,5\}$ and $\mathcal{P}(X)$ *be the power set of* X

$$\boldsymbol{\mathcal{U}} = \begin{bmatrix} X & \{1,2\} & \{2,3\} \\ \phi & X & \{1,2,3\} \\ \phi & \phi & X \end{bmatrix}; \ \boldsymbol{\mathcal{V}} = \begin{bmatrix} X & \phi & \phi \\ \{1,3\} & X & \phi \\ \{1,2\} & \{3,4\} & X \end{bmatrix}$$

$$\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}} = \begin{bmatrix} \{3,4,5\} & \{1,2,3\} & \{2,3\} \\ \{2,3\} & \{1,2,4,5\} & \{1,2,3\} \\ \{1,2\} & \{3,4\} & X \end{bmatrix}$$

here, $\det(\boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}}) = X$

Similarly, using different finite non-empty sets "X" and taking different elements from their power set, we can obtain infinite number of square matrices of any order.

Similarly, we can create a 4-square matrix by multiplying

$$\boldsymbol{\mathcal{U}} = \begin{bmatrix} X & A & B & C \\ \phi & X & D & E \\ \phi & \phi & X & F \\ \phi & \phi & \phi & X \end{bmatrix} \text{ and } \boldsymbol{\mathcal{V}} = \begin{bmatrix} X & \phi & \phi & \phi \\ G & X & \phi & \phi \\ H & I & X & \phi \\ J & K & L & X \end{bmatrix}$$

in order to get a 4-sqaure matrix $\boldsymbol{\mathcal{D}} = \boldsymbol{\mathcal{U}} \cdot \boldsymbol{\mathcal{V}}$ whose determinant $= X$.

$$\mathcal{D} = \mathcal{U} \cdot \mathcal{V} = \begin{bmatrix} X \oplus AG \oplus BH \oplus CJ & A \oplus BI \oplus CK & B \oplus CL & C \\ G \oplus DH \oplus EJ & X \oplus DI \oplus EK & D \oplus EL & E \\ H \oplus FJ & I \oplus FK & X \oplus FL & F \\ J & K & L & X \end{bmatrix}$$ where $A, B, C, D, E, F, G, H, I, J, K, L \in \mathcal{P}(X)$.

3.3 To construct a square matrix with determinant = X using square tridiagonal matrices

Let X be any given finite set (non-empty).
Consider $\mathcal{P}(X) = \{set\ of\ ALL\ subsets\ of\ X\}$
Let $\mathcal{U} = \begin{bmatrix} X & A & \phi \\ B & X & A \\ \phi & B & X \end{bmatrix}$ and $\mathcal{V} = \begin{bmatrix} X & C & \phi \\ D & X & C \\ \phi & D & X \end{bmatrix}$, we have $Det(\mathcal{U}) = Det(\mathcal{V}) = X$.
Here, $A, B, C, D \in \mathcal{P}(X)$

$$\mathcal{U} \cdot \mathcal{V} = \begin{bmatrix} X \oplus AD & C \oplus A & CA \\ B \oplus D & X \oplus BC \oplus AD & C \oplus A \\ BD & B \oplus D & X \oplus BC \end{bmatrix},$$

$$Det(\mathcal{U} \cdot \mathcal{V}) = Det(\mathcal{U}) \cdot Det(\mathcal{V}) = X \cdot X = X$$

3.4 To construct a square matrix with determinant = X using partitions of a set

Let "X" be a non-empty finite set,

$$X = \{a_1, a_2, a_3, \ldots, a_n\}$$

Define $A_1, A_2, A_3, \ldots, A_n$ as the partitions of the set X.

$$X = \bigcup_{i=1}^{n} A_i\ ;\ A_i \cap A_j = \phi\ \forall\ i \neq j.$$

Create a matrix "$\mathcal{U}$" using the $A_i s$ as latin square.

$$Det(\mathcal{U}) = A_1 \oplus A_2 \oplus A_3 \oplus \ldots \oplus A_n = X$$

4 Analysis

Let `M = ABC` be the plain text. The message corresponds to $\{0, 1, 2\}$.
Considering $K = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$ as the secret key and encrypting the message with Hill Cipher we get `M' = YRM` as the encrypted text. The same text when encrypted with the developed Hill Cipher using
$K = \begin{bmatrix} \phi & \{1,\ 2,\ 3\} & \phi \\ \phi & \{4,\ 5\} & \{1,\ 2,\ 3\} \\ \{1,\ 3\} & \{1,\ 2,\ 3,\ 4\} & \{4,\ 5\} \end{bmatrix}$ as the secret key gives `M' = BCB` as the encrypted text.

The above example is evident to the fact that the proposed algorithm overcomes the single letter frequency distribution problem making the encryption more strong and secure

5 Conclusion

The Hill cipher is the first polygraph cipher which has some advantages in symmetric data encryption. However, many studies and experiments show that Hill Cipher is vulnerable to known plaintext attack. The known-plaintext attack (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext, and the corresponding encrypted version through which other encrypted texts can be decoded. The reason for such a drawback is the linear calculations which the algorithm uses. Applying a brute force attack on any hill cipher encrypted text would lead to the plain text in fewer number of permutations. Less work factor on brute force attacks is another vulnerability observed in Hill Cipher Algorithm.

The algorithm to use Boolean Rings solves the above-mentioned problems in the Hill Cipher. The non-linear key calculations increase the complexity in key formation. Hence, now more work factor would be required while applying Brute force attack. And, it is not just the complexity in key formations, but this algorithm also removes the single letter frequency attack which increases the number of permutations while performing the brute force attack.

Another key feature of this proposed algorithm lies in what we call the 'Discrete Matrix Problem' derived from the term 'Discrete Log Problem'. Let G be a finite group and g be an element of G. Given $a \in G$ find an integer x such that $gx = a$. This corresponds to the logarithm problem for the positive reals, that is the same problem but with x a real number. The finiteness of the group and the type of solution sought account for the discrete in the name. Similarly, in the proposed algorithm; it is not possible to trace back the key from the given decrypted text. Hence, preventing the known-plaintext attack.

6 References

[1] W. Diffie and M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976), 644-654.

[2] R.L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM 21 (1978), pp. 120126.

[3] K. Komaya, U. Maurer, T. Okamoto and S. Vanston, Newpublic-key schemes bases on elliptic curves over the ring Zn, In J. Feigenbaum (Ed.): Crypto'91, LNCS 576, Springer-Verlag (1992), pp. 252-266.

[4] Koblitz, N. (1987). "Elliptic curve cryptosystems". Mathematics of Computation. 48 (177): 203–209. doi:10.2307/2007884

[5] Lester S. Hill (1929); Cryptography in An Algebraic Alphabet, The American Mathematical Monthly, 36:6, 306-312

[6] N. Chandramowliswaran, P. Muralikrishna and S. Srinivasan, Key Exchange and Encryption Schemes Based on commutative rings

[7] Zhenfu Cao, Xiaolei Dong and Licheng Wang, (2007) New Public Key Cryptosystems Using Polynomials over Non-commutative Rings, International Association for Cryptologic Research (009)

[8] N. Chandramowliswaran, S. Srinivasan & P. Muralikrishna (2015) Authenticated key distribution using given set of primes for secret sharing, Systems Science & Control Engineering, 3:1, 106-112, DOI: 10.1080/21642583.2014.985803

[9] Christof Paar, Jan Pelzl, Understanding Cryptography, Springer (2010)

[10] Ismail, I. A., Mohammed Amin, and Hossam Diab. "How to repair the Hill cipher." Journal of Zhejiang University-Science A 7.12 (2006): 2022-2030.

[11] Dawahdeh, Ziad E., Shahrul N. Yaakob, and Rozmie Razif bin Othman. "A new image encryption technique combining Elliptic Curve Cryptosys-tem with Hill Cipher." Journal of King Saud University-Computer and Information Sciences 30.3 (2018): 349-355.

[12] Mahendran, R., and K. Mani. "Generation of key matrix for hill cipher encryption using classical cipher." 2017 World Congress on Computing and Communication Technologies (WCCCT). IEEE, 2017.

[13] Putera, Andysah, Utama Siahaan, and Robbi Rahim. "Dynamic Key Ma-trix of Hill Cipher Using Genetic Algorithm." Int. J. Secur. Its Appl 10.8 (2016): 173-180.

[14] Rahman, M. Nordin A., et al. "Cryptography: A new approach of classical Hill cipher." International Journal of Security and Its Applications 7.2 (2013): 179-190.

[15] Herstein, I. N. (1975), Topics In Algebra (2nd ed.), John Wiley & Sons

7 Authors

1. **Rishabh Malhotra** is a student of Cyber Security at Amity University Rajasthan. He has completed his graduation in Mathematics.
2. **Dr. Girish Paliwal** is an Assistant Professor at Amity Institute of Information Technology at Amity University Rajasthan. His previous works include various studies on Wireless Networking, Computer Networking and Security. (gpaliwal@jpr.amity.edu)
3. **Dr. S Srinivasan** is an Assistant Professor of Mathematics at Periyar Govt Arts and Science College Cuddalore. (smrail@gmail.com)
4. **Dr. N. Chandramowliswaran** is a Professor of Mathematics at Amity University Haryana. He earned his PhD from IIT Delhi in 1995. His previous works include various research on Discrete Mathematics, Mathematical Aspects of Cryptography and Linear Algebra. (ncmowli@hotmail.com)