Cover Page

DOI: http://ijmer.in.doi./2023/12.05.20.2.2.3.2
www.ijmer.in

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:5(1), May: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd May 2023
Publication Date:1st June 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

CRYPTOGRAPHIC TECHNIQUES THROUGH MATRIX TRANSFORMATIONS AND APPLICATIONS

[1]Naidu Uma Devi and [2]Swathi Devi Medichalam
[1]MSc (Applied Mathematics),TS-AP SET 2014, CSIR UGC NET 2017
Mail id - umadevi134@gmail.com
[2]M Sc (Mathematics), TSSET-2017,Mail id -swathi.ragiphani06@gmail.com

ABSTRACT:

The practise and study of hiding information from everyone save those with the tools or keys to decipher the message is known as cryptography. Additionally, the field of cryptography uses a variety of techniques to convert regular data into an unintelligible format.

This article discusses a game that uses one of the ways used to demonstrate how matrices can be used in cryptography. In order to protect the communication with the aid of a key shared between the dispatcher and recipient, we have planned to utilise a linear matrix in this article to solve cryptographic algorithms, as well as a capable data encryption and data decryption method. In this post, we'll discuss data encryption and decryption using the Hill cypher technique.

KEYWORDS: Cryptography, Encryption, Decryption, Matrices.

INTRODUCTION:

It was invented roughly 4,000 years ago. The term "cryptography" comes from the Ancient Greek "kryptos," which means "hidden, secret," and "graphein," which means "to write." Today, "cryptography" permeates all aspects of our life without most of us being aware of it. The fundamental purpose of "cryptography," which is to conceal information in transit and make it available only to the intended recipients, has not changed over time.

Cryptography has emerged as one of the primary means of protection across all applications in the information era. Through the use of cryptography, people are able to transfer their sense of security from the physical world to the digital one. In the distant past, cryptography was employed to provide anonymity, allowing people to conduct business electronically without fear of fraud and deception. The integrity of the message and the sender's validity were often guaranteed via wax seals, signatures, and other physical procedures. The use of cryptography for integrity started to outpace its usage for secrecy when individuals started conducting business online and wanted to transfer money electronically. Every day, hundreds of thousands of individuals communicate electronically, whether through e-mail or e-commerce (online purchases).
Cryptography mainly consists of encryption and decryption.
Encryption and decryption require the use of some secret information, usually referred to as a key depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different.

Cryptanalysis: procedure of obtaining an original message from the encrypted message without knowing algorithms or keys

Cryptology: the art of encryption; combines cryptography and cryptanalysis ethics of Information Security

WHY CRYPTOGRAPHY?

The objectives of cryptography are centered around ensuring the confidentiality, integrity, authenticity, and availability of information in the presence of adversaries. These objectives are achieved through various cryptographic techniques and mechanisms. The primary objectives of cryptography include:

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:5(1), May: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd May 2023
Publication Date:1st June 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

DOI: http://ijmer.in.doi./2023/12.05.20.2.2.3.2
www.ijmer.in

1. Confidentiality: Information is intended to be hidden from unauthorised parties via cryptography. It involves encryption, which uses encryption keys and methods to convert plaintext into ciphertext. The ciphertext can only be converted to plaintext by authorised individuals who also possess the corresponding decryption keys.

2. Integrity: Data integrity is protected by cryptography, which can spot any unwanted updates or adjustments. In order to create fixed-length hash values (digests) from data, cryptographic hash functions are used. To check if the data has been altered, these hashes are compared.

3. Authentication: To confirm that entities (people, gadgets, or systems) are who they say they are, cryptography makes it easier to authenticate them. This is commonly accomplished through digital signatures, in which the sender creates a signature using their private key and the recipient uses the sender's public key to confirm the signature's legitimacy.

4. Availability: Cryptography helps ensure the availability of data and services. Denial of Service (DoS) attacks can disrupt availability, and cryptographic techniques can be used to defend against such attacks or to mitigate their impact.

5. Public Key Infrastructure (PKI): Cryptography provides the foundation for PKI, a framework that manages digital certificates and public-private key pairs. PKI enables secure communication and authentication over networks.

6. Data Privacy: In the context of sensitive personal information, cryptography helps protect individuals' privacy by ensuring that their data is not accessible to unauthorized parties.

7. Secure Transactions: Online transactions, such as e-commerce, online banking, and digital payments, require the use of cryptography to be secure. It makes sure that confidential financial information is kept private and that the parties are real.

8. Homomorphic Encryption: This advanced cryptographic concept allows computations to be performed on encrypted data without the need for decryption. This is particularly useful for privacy-preserving data analysis.

Overall, the main objectives of cryptography revolve around safeguarding sensitive information, verifying the authenticity of parties, and maintaining the integrity and availability of data and services in various digital environments.

CRYPTOGRAPHIC TECHNIQUES:

The usage of matrices in various cryptographic systems has a big impact on how secure communications and data protection are. The following are some applications of matrices in cryptography:

Hill Cipher: The Hill cipher is a symmetric key encryption technique that uses matrices for encryption and decryption. The plaintext is divided into blocks and represented as vectors. These vectors are then multiplied by a matrix modulo some value to produce the ciphertext. The inverse of the matrix is used for decryption.

Linear Feedback Shift Registers (LFSRs): LFSRs are used in stream ciphers, a type of symmetric key encryption. They use matrices to perform operations on the binary sequence to generate a pseudorandom bit stream, which is then combined with the plaintext to produce the ciphertext.

Matrix-based Transposition Ciphers: Transposition ciphers involve rearranging the order of characters in a message. Matrices are used to define the specific transposition pattern applied to the plaintext.

Public Key Cryptography: In some cases, matrices are used in the mathematical operations underlying public key cryptography algorithms. For example, in the RSA algorithm, modular exponentiation involves matrix-like calculations with large numbers.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:5(1), May: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd May 2023
Publication Date:1st June 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

DOI: http://ijmer.in.doi./2023/12.05.20.2.2.3.2
www.ijmer.in

Error-Correcting Codes: Matrices are used in coding theory to design error-correcting codes. Parity-check matrices and generator matrices are employed to encode data in a way that can recover from errors during transmission.

Elliptic Curve Cryptography (ECC): ECC is a public key cryptography technique that involves mathematical operations on points of an elliptic curve. These points form a group, and matrix operations are used to manipulate these points, providing the basis for encryption and digital signatures.

Homomorphic Encryption: Matrices can be used in some homomorphic encryption schemes, which allow computation on encrypted data without decrypting it first. Matrices enable certain operations to be performed on ciphertexts while preserving their security.

These are just a few examples of how matrices are used in the field of cryptography. Matrices provide a mathematical foundation for many encryption and decryption processes, helping to ensure the confidentiality and integrity of sensitive information.

HILL CIPHER TECHNIQUE:

The Hill cipher technique plays the most significant role in the development of cryptography.
A cryptographic algorithm for encryption and decoding is called The Hill Cipher. It belongs to the class of substitution cyphers, which change letters in plaintext into ciphertext by performing a mathematical operation. The Hill Cipher uses matrix operations for its encryption and decryption processes, which sets it apart from simpler substitution cyphers.
The Hill Cipher's use of matrix operations gives it greater resistance to simple frequency analysis attacks than simpler cyphers like the Caesar Cipher or the simple substitution cypher, which are susceptible to such attacks.
The Hill Cipher has restrictions, though. Larger key matrices can become computationally expensive and are required to be invertible. Furthermore, the key matrix choice affects the Hill Cipher's security, and some key matrix choices can result in flaws.
Due to their higher security and versatility, modern cryptographic methods like block cyphers and public-key cryptography have essentially replaced traditional techniques like the Hill Cipher. However, the Hill Cipher continues to be a significant historical turning point in the evolution of cryptographic methods.

IMPLEMENTATION OF HILL CIPHER:

A cryptogram is a message written according to a secret code. Below, I will illustrate one method of using matrix multiplication to encode and decode a message. By assigning a number to each letter in the alphabet (0 assigned to a blank space) as follows,

Alphabet	A	B	C	D	E	F	G	H	I	J
Assigned number	0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:5(1), May: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd May 2023
Publication Date:1st June 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

DOI: http://ijmer.in.doi./2023/12.05.20.2.2.3.2
www.ijmer.in

Steps involved in the Hill Cypher Technique:

Key Generation: A key matrix is generated by selecting a square matrix of a certain size (usually 2x2 or 3x3) with elements from a defined set (often the alphabet's letters mapped to numbers). This matrix serves as the encryption and decryption key.

Encryption: The plaintext message is divided into blocks of the same size as the key matrix. Each block is then represented as a column vector, and matrix multiplication is performed between the key matrix and the column vector to obtain the corresponding ciphertext vector. The resulting vector is then converted back to letters or symbols.

Decryption: The ciphertext is divided into blocks again, and matrix multiplication is done between the modular inverse of the key matrix (which exists only if the key matrix is invertible) and the ciphertext vector to obtain the original plaintext vector. The vector is then converted back to the original message.

KEY GENERATION:

A key(C) is a matrix which has the same size as of k

Which has a set of unique numbers which can be used for decryption and encryption of the message

For this exercise, we will use the following key.

$$C= \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$$

ENCRYPTION

Encryption is a process of encoding a message which can only be read after decrypting with the key (C)

$$C(K, P) = (K*P) \bmod$$

The Hill Cipher formula for encrypting any given message

K is a 3x3 matrix

C and P are the vectors

C1 = (K11 P1 + K12 P2 + K13 P3) mod 26.

C2 = (K21 P1 + K22 P2 + K23 P3) mod 26.

C3 = (K31 P1 + K32 P2 + K33 P3) mod 26.

$$\begin{bmatrix} C1 \\ C2 \\ C3 \end{bmatrix} = \begin{bmatrix} P1 & P2 & P3 \end{bmatrix} * \begin{bmatrix} K11 & K12 & K13 \\ K21 & K22 & K23 \\ K31 & K32 & K33 \end{bmatrix} \bmod 26$$

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:5(1), May: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd May 2023
Publication Date:1st June 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

DOI: http://ijmer.in.doi./2023/12.05.20.2.2.3.2
www.ijmer.in

Our message to encrypt is **VANDE MATARAM**

Word	V	A	N	D	E	M	A	T	A	R	A	M
Assigned number	21	0	13	3	4	12	0	19	0	17	0	12

Applying the Hill Cipher formula for the given word

Take 3 alphabets at a time only

$$C_{van} = [21\ 0\ 13] \text{ X } \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \text{Mod } 26$$

$$=[86 \quad 120 \quad 63] \text{Mod } 26$$

$$= [8\ 16\ 11] = [\text{I Q L}]$$

$$C_{dem} = [3\ 4\ 12] \text{ X} \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \text{Mod } 26$$

$$=[63 \quad 82 \quad 25] \text{Mod } 26$$

$$= [11\ 4\ 25] = [\text{L E Z}]$$

$$C_{ata} = [0\ 19\ 0] \text{ X } \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \text{Mod } 26$$

$$=[0 \quad 19 \quad 76] \text{Mod } 26$$

$$= [0\ 19\ 24] = [\text{A T Y}]$$

$$C_{ram} = [17\ 0\ 12] \text{ X } \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \text{Mod } 26$$

$$=[77 \quad 106 \quad 51] \text{Mod } 26$$

$$= [25\ 2\ 25] = [\text{Z C Z}]$$

Cipher Text = [IQL LEZ ATY ZCZ]

DECRYPTION

$P = K^{-1} C \bmod 26$

$= K^{-1} (KP) = P$

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881; IMPACT FACTOR :8.017(2023); IC VALUE:5.16; ISI VALUE:2.286
Peer Reviewed and Refereed Journal: VOLUME:12, ISSUE:5(1), May: 2023
Online Copy of Article Publication Available (2023 Issues)
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: 2nd May 2023
Publication Date:1st June 2023
Publisher: Sucharitha Publication, India
Digital Certificate of Publication: www.ijmer.in/pdf/e-CertificateofPublication-IJMER.pdf

DOI: http://ijmer.in.doi./2023/12.05.20.2.2.3.2
www.ijmer.in

(C=KP mod 26)

$$K = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}$$

Applying mod 26 to remove negative values

$$K^{-1} \bmod 26 = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix}$$

$P = K^{-1} C \bmod 26$

$$P_1 = [8 \quad 16 \quad 11] \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} Mod\ 26 = [567 \quad 364 \quad 403] Mod\ 26 = [21 \quad 0 \quad 13] = (VAN)$$

$$P_2 = [11 \quad 4 \quad 25] \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} Mod\ 26 = [627 \quad 342 \quad 168] Mod\ 26 = [3 \quad 4 \quad 12] = (DEM)$$

$$P_3 = [0 \quad 19 \quad 24] \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} Mod\ 26 = [884 \quad 305 \quad 442] Mod\ 26 = [0 \quad 19 \quad 0] = (ATA)$$

$$P_4 = [25 \quad 2 \quad 25] \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} Mod\ 26 = [615 \quad 572 \quad 194] Mod\ 26 = [17 \quad 0 \quad 12] = (RAM)$$

VANDE MATARAM

Hence message decryption is successful.

REFERENCES:

1. Khan F. H., Shams R., “Hill Cipher Key Generation Algorithm by using Orthogonal Matrix”, International Journal of Innovative Science and Modern Engineering (IJISME), Volume-3 Issue-3, 2015.
2. Gomes, J.; Velho, L. Image Processing for Computer Graphics and Vision. Springer-Verlag, 2008.
3. Gonzalez, R. C.; Woods, R. E. Digital Image Processing. Third Edition. Prentice Hall, 2007
4. K Thiagarajan et al 2018 J. Phys.: Conf. Ser. 1000 012148 Encryption and decryption algorithm using algebraic matrix approach National Conference on Mathematical Techniques and its Applications (NCMTA 18) IOP Publishing.
5. P. Zimmerman, "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.
6. www.google.com
7. Vasta B.S, Vasta Suchi., Theory of matrices., Third Edition., new Agt international, india 2010.
8. J. Callas, "The Future of Cryptography," Information Systems Security, vol. 16, no. 1, pp. 15-22, 2007.