"Development of Matrix for Cryptography"

Waghmare Shwetambari [1], Mali Ujwala [2]

Assistant professor[1], Assistant professor[2]

Applied Mathematics[1],Applied Mathematics[2]

[1] Bharati Vidyapeeth College of Engineering Sector 7 CBD Belpada Navi Mumbai Maharashtra,

[2] Bharati Vidyapeeth College of Enginearing Sector 7 CBD Belpada Navi Mumbai Maharashtra.

Abstract:

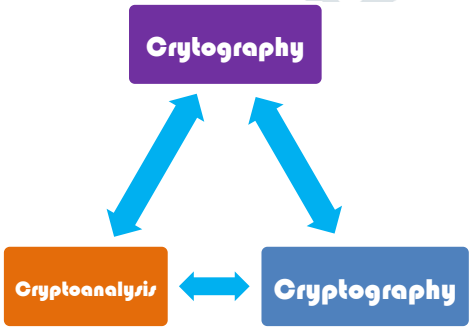
In this article, we have planned to use linear algebra/Matrix for solving cryptographic algorithm ,an capable data encryption and data decryption algorithm to protect the communication with the help of key passed between dispatcher and recipient. In this article we are using Hill cipher method to tackle encryption and decryption data.

Keywords: cryptography, Plaintext, cipher text, Encryption, Decryption

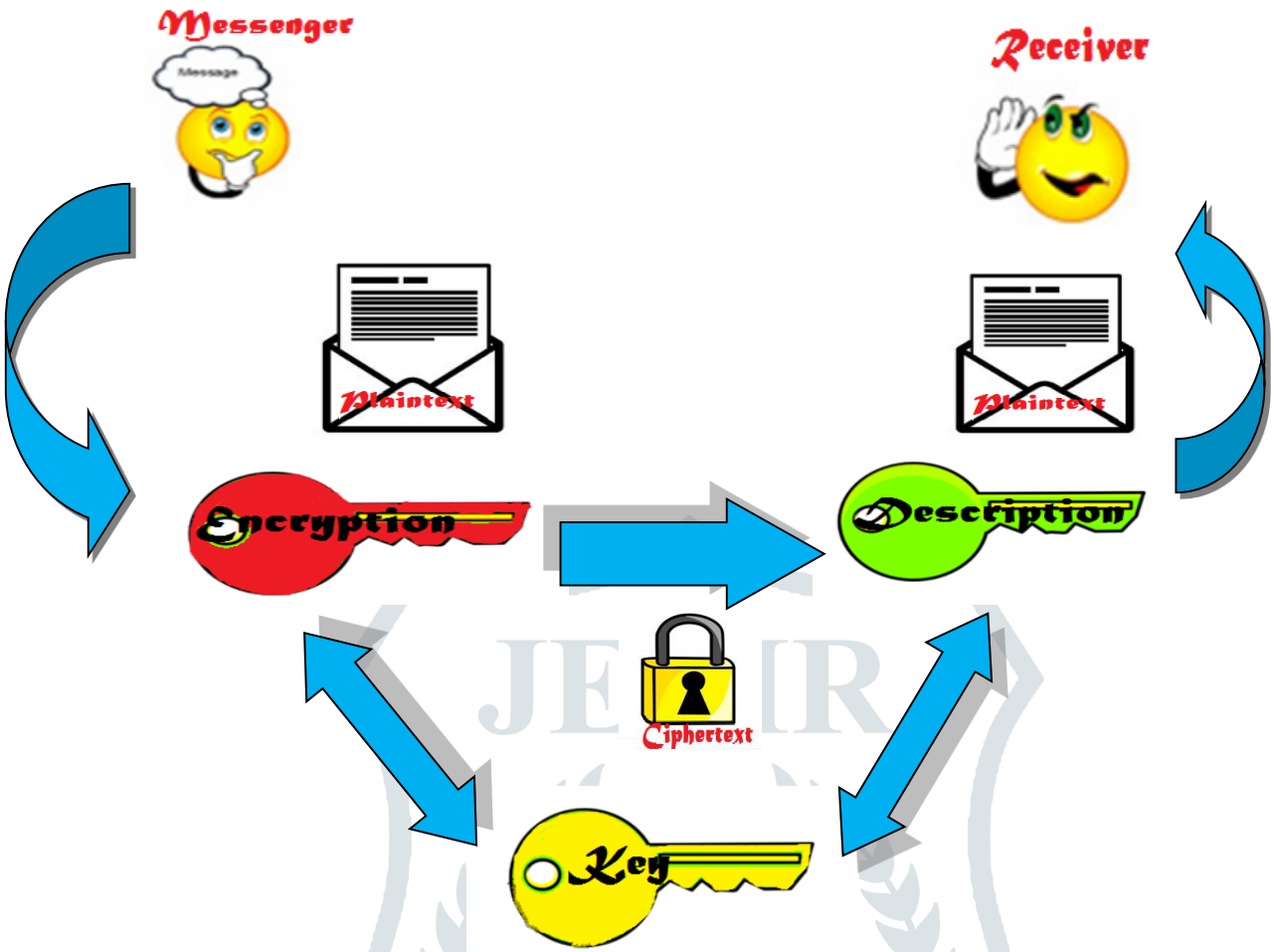
I INTRODUCTION: Cryptography originated about 4000 year ago. Cryptography an Ancient Greek translit "Kryptos" means " Hidden , secret" and graphein means "to write" [5]. Today 'Cryptography' is universal in our lives without most of us realizing it. The essential aspect of 'Cryptography' has remained same all the way through time which is to hide information in transit and make it presented only for the intended recipients [1]. The ***encoding*** of a note is the invention of the message. It is a system of coded meanings, and in order to create that, the sender needs to understand how the world is comprehensible to the members of the listeners[2]. The *decoding* of a note is how an listeners member is able to understand, and understand the message. It is a process of understanding and conversion of coded information into a understandable form. The messages are called **Plaintext[3].**

The messages after coading are called **cipher text.** The process of converting from plain text to coading message is called **enciphering(encoding)**.it is reverse process of getting plain text from cipher text is called **deciphering(decoding) [4].**

- **Cryptography**: procedure of making and using codes to secure broadcast of information[6]
- **Encryption**: converting original message into a form unreadable by unauthorized individuals[6]
- **Cryptanalysis**: procedure of obtaining original message from encrypted message without knowing algorithms or keys[6]
- **Cryptology**: art of encryption; combines cryptography and cryptanalysis ethics of Information Security[6]



It is the practice and study of hiding information. In this type of Encryption, a pair of keys known as Public Key and Private Key is used. As name indicates, Public Key is shared and identified to everyone where as Private Key is With the person himself [7,6].



II OBJECTIVES OF CRYPTOGRAPHY:

Confidentiality: the information cannot be known by anyone for whom it was unexpected[5].

Integrity: the information cannot be altered in storage or transfer between dispatcher and intended receiver without the modification being detected[5]

Non-repudiation: the originator of the information cannot reject at later stage his or her intentions in the making or broadcast of the information[5]

Authentication: he dispatcher and recipient can verify each other's identity band source/destination of the information.

All are needed in various application such as Military communications, Radio communication, telephonic communication, Network communication, Mobile communication and internet[5,6].

III RESEARCH METHODOLOGY

Hill cipher is a polygraphic substitution cipher that is based on linear algebra .It is the first polygraphic cipher that's able to work on more than three symbols at once[5,13]

3.1 A history of hill cipher

It was invented by Lester S. Hill in 1929.Hill cipher is an example of block cipher that acts on groups of letters[11]. It can work on any sized block ,including digraphs & triagraphs. The ability to extendable to work with different sized blocks of letters is main advantage of this cipher[5,6].

3.2 Method to encrypt using Hill cipher

To encrypt you must change your keyword into a key matrix, 2 by 2 for digraphs or 3 by 3 for trigtaphs[12].Then turn the plaintext into digraphs or trigraphs & each of these into column vector. Then perform matrix multiplication modulo the length of alphabet on each vector .Then finally convert these vectors back into letters to produce the cibhertext[5,6].

Encryption [10]

Cipher Text = (plain Text X key) mod 26

E.g. C =AB(mod 26)

Description[9]

Plain Text = (Cipher Text X Key $^{-1}$) mod 26

E.g. B =A^{-1} C (mod 26)

3.3 Example of hill cipher encryption using 3 by 3 matrix [8]

Step I

Encryption

.Message: ATTACK IS TONIGHT

$$\text{Key} = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$$

Step 2

Encryption

Message:: ATTACK IS TONIGHT

Assign: A-Z 0-25

$$\begin{bmatrix} A & T & T \\ A & C & K \\ I & S & T \\ O & N & I \\ G & H & T \end{bmatrix} = \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix}$$

Step 3

…….Encryption

Message: ATTACK IS TONIGHT

Cipher Text = (Plain Text X key) Mod 26

$$= \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} \text{X} \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \text{ mod } 26$$

Step 4

……Encryption

$$= \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} \text{X} \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \text{ mod } 26$$

C_{11} = 0*3 + 19 * 20 + 19*9 = 551 Mod 26 = 05

C_{12} = 0* 10 + 19*9 + 19 * 4 = 247 mod 26 = 13

C_{13} = 0 *20 + 19*17 + 19*17 = 646 mod 26 =22

C21= 0*3 + 2*20+10*9=130 Mod 26=0

C22=0*10+2*9+10*4=58 Mod 26=6

C23=0*20+2*17+10*17=204 mod 26=22

C31= 8*3 +18*20+19*9=555mod26=9

C32=8*10+18*9+19*4=318 mod26=6

C33=8*20+18*17+19*17=789 mod 26=9

C41=14*3+13*20+8*9=374 mod 26=10

C42=14*10+13*9+8*4=289 mod 26 =3

C43=14*20+13*17+8*17=697 mod 26 = 13

C51=6*3+7*20+19*9=329 mod 26 = 17

C52=6*10 +7*9+19*4=199 mod 26= 17

C53 = 6*20+7*17+19*17= 562 mod 16=16

ATTACK IS TONIGHT --> FNDAGW JG JKDNRRQ

Cipher Text = $\begin{bmatrix} 5 & 13 & 22 \\ 0 & 6 & 22 \\ 9 & 6 & 9 \\ 10 & 3 & 13 \\ 17 & 17 & 16 \end{bmatrix}$

Decryption

Key = $\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$

Det Key= $\begin{vmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{vmatrix}$ mod 26 =-1635 mod 26=-23 mod 26=03

$\{\text{Det (key)}\}^{-1}=(03)^{-1}$mod 26=09

Transpose of key = $\begin{bmatrix} 3 & 20 & 9 \\ 10 & 9 & 4 \\ 20 & 17 & 17 \end{bmatrix}$

Minor of Transpose of key = $\begin{bmatrix} 85 & 90 & -10 \\ 187 & -129 & -349 \\ -1 & -78 & -173 \end{bmatrix}$

Cofactor Matrix of Transpose of key = $\begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix}$

$(key)^{-1}=(\text{Det Key})^{-1}$ X Adj Key$=\left\{09 * \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix}\right\}$mod 26

$$=\begin{bmatrix} 765 & -810 & -90 \\ -1683 & -1161 & 3141 \\ -9 & 702 & -1557 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{bmatrix}$$

Plain text = (Cipher Text X key^{-1})mod 26

$$=\left\{\begin{bmatrix} 5 & 13 & 22 \\ 0 & 6 & 22 \\ 9 & 6 & 9 \\ 10 & 3 & 13 \\ 17 & 17 & 16 \end{bmatrix} * \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{bmatrix}\right\} * \text{mod} 26$$

$$=\begin{bmatrix} 520 & 227 & 409 \\ 416 & 54 & 192 \\ 294 & 252 & 279 \\ 352 & 247 & 242 \\ 578 & 527 & 643 \end{bmatrix} \text{mod } 26 == \begin{bmatrix} 0 & 19 & 19 \\ 0 & 2 & 10 \\ 8 & 18 & 19 \\ 14 & 13 & 8 \\ 6 & 7 & 19 \end{bmatrix} = \textbf{ATTACK IS TONIGHT}^{5}$$

Likewise we tackle encryption and decryption of our cryptography examples. This methodology is very helpful to solve crypto problems.

IV. Applications of Cryptography:

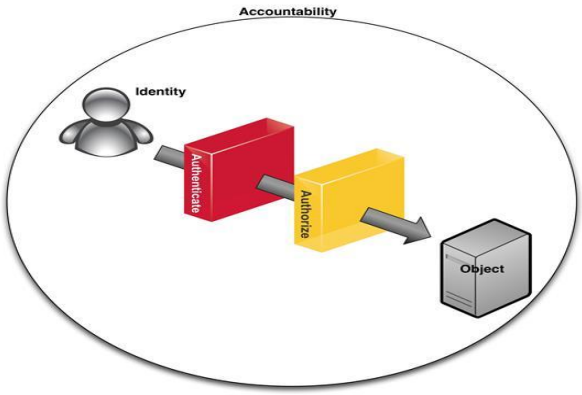
- **Secure communication:**

  To stop listen in-war time communication and commerce transaction.

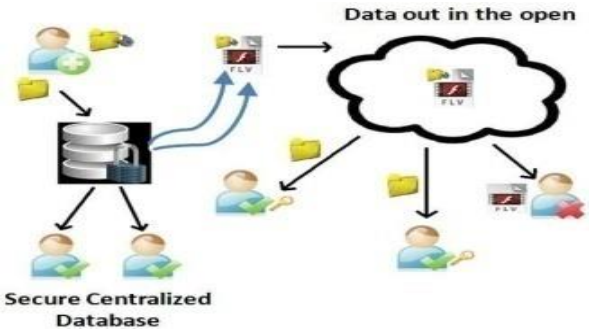
Military communications[5].

- **Identification & Authentication:**

  Checking the integrity[5]



- **Secret sharing/ data hiding:**
  Secrete something that has been written[5].



- **E-commerce/ E-payment:**

- **Certification:**
  Certification is a system by which trusted agents such s certifying authorities assurance for Unidentified agents, such as users[5].

V Conclusion:

In this article, we have planned to use linear algebra/Matrix for solving cryptographic algorithm, an capable data encryption and data decryption algorithm to protect the communication with the help of key passed between dispatcher and recipient. Also communication with any number of words having any digit of character can is encrypts and decrypt by dispatcher and recipient. With data encryption, data owner can use the benefits of communication splitting to digit of words such that to decrease storage and computational overheads. The hill cipher methodology can be used to tackle crypto problem, using matrices it is possible to solve encryption and decryption problem.

VI References:

1.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.

2. P. Zimmerman, "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.

3. C. Shannon, “Communication Theory of Secrecy Systems”, Bell Systems Technical Journal, MD Computing, vol. 15, pp. 57-64, 1998.

4. H. Mohan, and R. Raji. "Performance Analysis of AES and MARS Encryption Algorithms".
International Journal of Computer Science Issues (IJCSI), Vol. 8, issue 4. 2011.

5. www.google .com

6.Book of Applied Mathematics-I Tech max publications ,pune written by Dr.N.R Dasre,S.R Mitkari, M.V Ghotkar, B.B Gadekar.

7. Kalaichelvi V, Manimozhi K, Meenakshi P, Rajakumar B, Vimaladevi P A New variant of Hill Cipher Algorithm for Data Security , International Journal of Pure and Applied Mathematics, Volume 117 No. 15 2017, 581-588 ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version) url: http://www.ijpam.eu

8. Ismail I A, Amin Mohammed, Diab Hossam, How to Repair the Hill Cipher, Journal of Zhejiang University Science, 7(12), pp. 2022-2030, 2006.

9. A. H. Rushdi and F. Mousa, “Design of a Robust Cryptosystem Algorithm for Noninvertible Matrices Based on Hill Cipher ”Intl Journal of Computer Science and Network Security , vol.9, no.5, 2009 pp. 11-16 10. Yeh YS, Wu TC, Chang CC, Yang WC. “A New Cryptosystem Using Matrix Transformation”. 25th IEEE International Carnahan Conference on Security Technology 1991: 131-138

11. Chefranov A. G., “Secure Hill Cipher Modification SHC-M” Proc. Of the First International Conference on Security of Information and Network (SIN2007) 7-10 May 2007, Gazimagusa (TRNC) North Cyprus, Elci, A., Ors, B., and Preneel, B (Eds) Trafford Publishing, Canada, 2008: pp 34-37, 2007

12. Y. Mahmoud Ahmed, Chefranov A. G., “ Hill Cipher Modification Based on Pseudo-Random Eigen values HCM-PRE” Submitted to Turkish Journal of Electrical Engineering & Computer Science on 2-03-2010

13. William Stallings, “Cryptography and Network Security”, 5th Edition. 7. Bruce Schneier, "Applied Cryptography" , John Wiley & Sons, Inc 1996 8. Richard Smith "Internet Cryptography",Pearson Edn Pvt.Ltd