International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585
Volume 4, Issue 03, March-2018

# A STUDY ON DATA ENCRYPTION AND DECRYPTION USING HILL CIPHER ALGORITHM

D. MAHESWARI[1], A. KAUSHIKA[2], A. JENIFER[3]
[1]*Department of mathematics, Sri krishna arts and science college,*
[2]*Department of mathematics, Sri krishna arts and science college,*
[3]*Department of mathematics, Sri krishna arts and science college,*

***Abstract - In the recent years the need of security has increased many folds. Cryptography is used widely for the purpose of secure communication and password management. It comprises of two mechanisms namely encryption and decryption. Mathematical principles can be employed to encrypt and decrypt our message and to transmit them securely. In this paper we are using principles of hill cipher for developing an encryption and decryption algorithm to make transmission of messages secure from eavesdropping.***

***Keyword - Data encryption, decryption, ciphers, security, algorithm.***

## I. Introduction

Communication is the act of conveying intended meanings from one entity or group to another through the use of mutually understood signs. Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. A cryptographic algorithm works in combination with a **key**– a word, a number or a phrase to encrypt plain text. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

## II. Cryptography

The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fuelled the natural need of people to communicate secretly with selective recipients which in turn ensured the continuous evolution of cryptography as well[7]. The roots of cryptography are found in Roman and Egyptian civilizations.
Cryptography is the science of using mathematics to encrypt and decrypt data. Data encryption is known for protecting information from eavesdropping. It transforms data of a given format called the plain text, to another format called cipher text using an encryption key [1]. Decryption is the process of converting cipher text into a plain text with suitable key. This study is related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

## III. Basic terminology of cryptography

Cryptography is the transformation of understandable data into a form which cannot be understood in order to secure data.
The unencrypted data is called the **plain text**. That is it is the actual message which is to be transferred to the recipient. The plaintext is the message before encryption or it is the text at the receiver after decryption.
The encrypted data is called the **cipher text**. It is the text which is not understandable by others other than the recipient. Many algorithms are used to decipher the text back to plain text.
**Cipher** is the algorithm that is used to transform plain text into cipher text. The process of locking up information using cryptography is called **encryption**. Information that has been locked up this way is said to be encrypted. The process of unlocking encrypted information using cryptography is called **decryption**. A secret, like a password, which is used to encrypt and decrypt information is called a **key.**

## IV. Cryptography goals

Cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

A. *Confidentiality / Privacy*

It is the most important goal, that ensures that no one can read the message except the intended receiver.

B. *Authentication*
It is the process of proving one's identity. This means that the user or the system can prove their own identities to other parties who don't have personal knowledge of their identities.

C. *Data integrity*
It assures the receiver that the received message has not been altered in any way from the original. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it has been created, transmitted, or stored by an unauthorized user.

D. *Non – repudiation*
it is the mechanism to prove that the sender really sent this message and it was received by the specified recipient.

E. *Key exchange*
It is the method by which the sender and the receiver shares crypto keys.

## V. Data encryption

Encryption is based on the ancient art of cryptography. It uses mathematical algorithms to turn plain text into an unreadable, jumbled code called the cipher text [1]. To decrypt that cipher text into plain text we are in need of an encryption key. Only the intended recipient has the key in their possession. Cryptography uses two types of keys namely symmetric and asymmetric. Symmetric or secret key cryptography uses a single key for both the encryption and decryption of the cipher text. Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers [8]. Block ciphers process messages in blocks whereas stream cipher applies the key and algorithm one bit at a time.

## VI. Data decryption

Data decryption is the reverse process of encryption. It is the process of decoding the data which has been encrypted into a secret format, which means that it converts the unreadable cipher text into the plain text by using the suitable key[5]. An authorized user can only decrypt data decryption requires a secret key or password.

## VII. Symmetric key cryptography

Symmetric key cryptography also referred as secret key cryptography or private-key cryptography uses a single key to encrypt and decrypt the data. (or less commonly, in which their keys are different, but related in an easily computable way.) In this type both the sender and the receiver should have the copy of the key used to encrypt and decrypt the data [3].

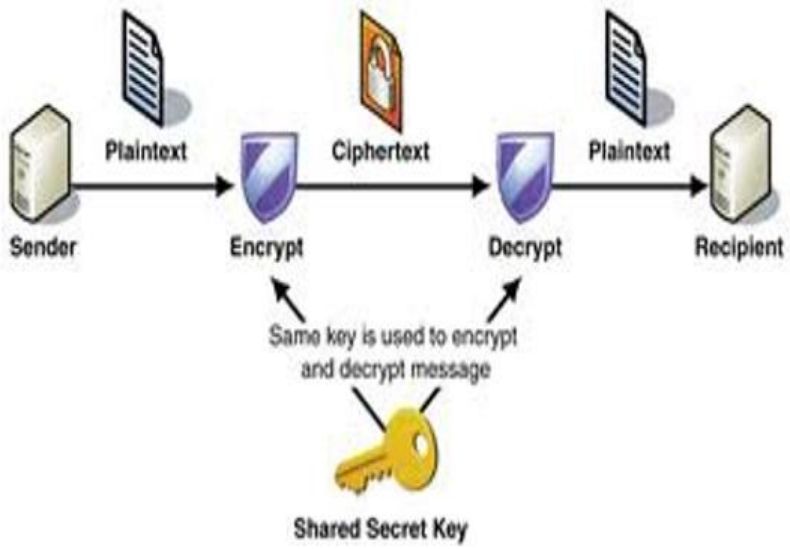


Fig. 1 Diagrammatic representation of symmetric key cryptography.

## VIII. Asymmetric key cryptography

Asymmetric cryptography also referred to as public key cryptography uses two different keys for encryption and decryption.. In this type of cryptography, one key is used to encrypt, and a matching key is used to decrypt. These two

keys together are called a key pair. One of these keys is called the secret key or private key, and should be kept secure and the other is called the public key.

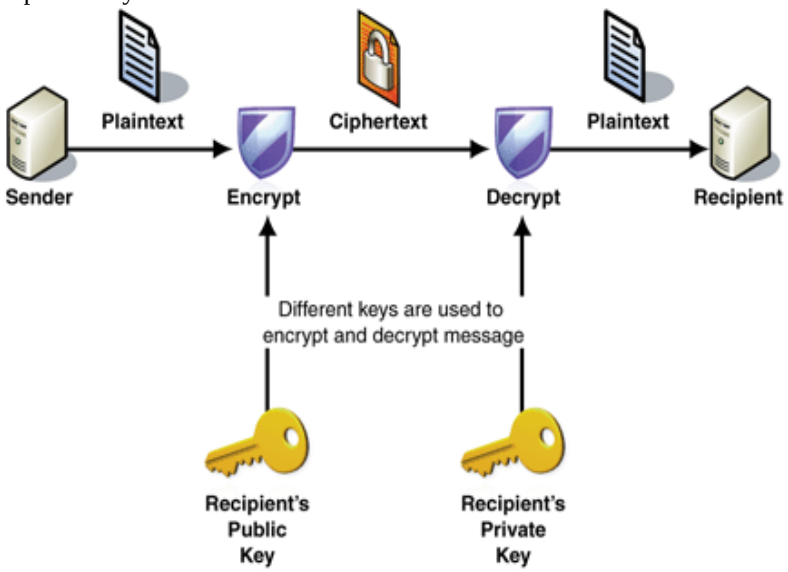


Fig. 2 diagrammatic representation of asymmetric key cryptography.

## IX. Types of ciphers

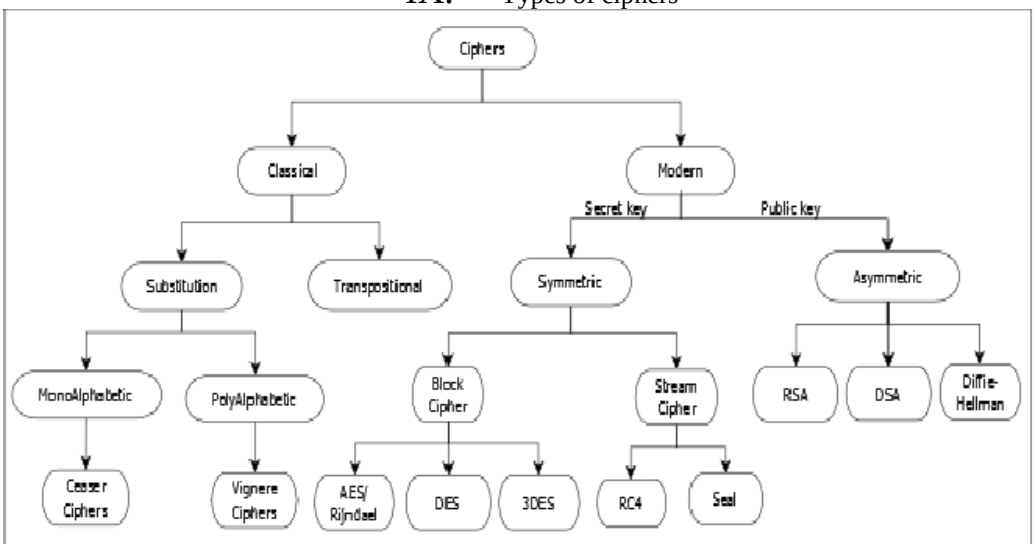


Fig. 3 tree diagram for types of ciphers.

Now we consider hill cipher which is one of the substitution ciphers.

## X. Hill cipher

One of the ways in which a Plain text message can be codified to obtain the corresponding cipher text using linear algebra is HILL CIPHER which belongs to a category of ciphers called block ciphers. HILL CIPHER is developed by the Mathematician LESTER S. HILL in 1929 [6]. In this cipher the plain text is divided into equal size blocks. The blocks are encrypted one at a time in such a way that each character in the block contributes to the encryption of other characters in the block.

## XI. Algorithm for encryption

**Cipher text = (plain text * key) mod 26**

**Step 1:** Obtain a plain text message to encode in standard English with no punctuation.
**Step 2:** Create an n*n secret matrix which contains numbers from 0 to 25 such that its determinant does not factor by 2 or 13.
**Step 3:** Group the plaintext into n-letter blocks. If we have an odd number of letters, repeat the last letter [2].
**Step 4:** Replace each letter by the number corresponding to its position in the alphabet i.e) A=1, B=2, C=3..., Z=0.

**Step 5:** Convert each block of letters into plaintext vectors.
**Step 6:** Convert the plain text vectors into cipher text vectors by multiplying the secret matrix by each plaintext vector and replace each new vector by its residue modulo 26 if possible.
**Step 7:** Convert each entry in the cipher text vector into its corresponding position in the alphabet.
**Step 8:** Align the letters in a single line without spaces. The message is now enciphered[4].

## XII. Algorithm for decryption

**Plain text = (cipher text * $key^{-1}$) mod 26**
**$key^{-1}$ = $(determinant\ of\ key)^{-1}$ * adjoint (key)**

**Step 1:** Obtain a plaintext message to encode in standard English with no punctuation.
**Step 2:** Group the cipher text into n-blocks.
**Step 3:** Replace each letter by the number corresponding to its position in the alphabet i.e) A=1, B=2, C=3, ... ,Z=0.
**Step 4:** Convert each block of letters into cipher text vectors.
**Step 5:** Find the inverse of the enciphering matrix.
i) Find the determinant of the enciphering matrix and then find the determinant's reciprocal modulo 26 i.e)

| | | | | | |
|---|---|---|---|---|---|
| 1 | 3 | 5 | 7 | 9 | 11 |
| 1 | 9 | 21 | 15 | 5 | 19 |

| | | | | |
|---|---|---|---|---|
| 15 | 17 | 21 | 23 | 25 |
| 7 | 23 | 5 | 17 | 25 |

These are the only multipliers that can be used because they are the only integers that have inverses modulo 26.
ii) Multiply the reciprocal modulo 26 by the secret matrix.
iii) Find the residue modulo 26 of the new matrix. This gives the deciphering matrix.
**Step 6:** Convert the cipher text vectors into plain text vectors.
i) Multiply the deciphering matrix by each cipher text vector.
ii) Replace each new vector by its residue modulo 26 if possible.
**Step 7:** Convert each entry in the cipher text vector into its corresponding position in the alphabet.
**Step 8:** Align the letters in a single line without spaces.

**Step 9:** Use logic and phonetics to determine individual words. The message is now deciphered.

## XIII. EXAMPLE

To encrypt the word MATHEMATORES using HILL CIPHER algorithm we have the formula [10].
**Cipher text = (plain text * key) mod 26**

Let the key matrix be $\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$

Determinant of the matrix be -1635. Separate the word MATHAMATORES into equal blocks
MAT HAM ATO RES. Now to replace each letter by the number corresponding to its position in the alphabet. The corresponding value for each alphabet is given in the table below:

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

The next step is to convert each block into plain text vectors

MAT = $\begin{bmatrix} 12 \\ 0 \\ 19 \end{bmatrix}$ Multiply the plain text vectors by the secret matrix to get the cipher text matrix

$$\text{MAT} = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} * \begin{bmatrix} 12 \\ 0 \\ 9 \end{bmatrix} = \begin{bmatrix} 416 \\ 563 \\ 431 \end{bmatrix}$$

Replacing new vector by its residue modulo 26 we get,

$$\text{MAT} = \begin{bmatrix} 416 \\ 563 \\ 431 \end{bmatrix} \pmod{26} = \begin{bmatrix} 0 \\ 17 \\ 15 \end{bmatrix}$$

Converting the entry in the cipher text vector into its corresponding position in the alphabet we get,

$$\begin{bmatrix} 0 \\ 17 \\ 15 \end{bmatrix} = \text{ARP}$$

Continuing the same process for other block of letters we get the enciphered text as ARPBGHCTCJGH. Now to decipher the enciphered text into the actual text we have the formula

**Plain text = (cipher text * $key^{-1}$) mod 26**

**$key^{-1}$ = ($determinant\ of\ key$)$^{-1}$ * adjoint (key)**

Group the cipher text into n-blocks ARP BGH CTC JGH. Replacing each letter by the number corresponding to its position in the alphabet i.e) A=1, B=2, C=3, ... ,Z=0 and converting each block of letters into cipher text vectors we get,

$$\text{ARP} = \begin{bmatrix} 0 \\ 17 \\ 15 \end{bmatrix}$$ To find the $key^{-1}$ we have to find the inverse of the determinant of the key

$$\text{Determinant of the key} = \begin{vmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{vmatrix} = 3$$

$(determinant\ of\ key)^{-1} = 3^{-1} \pmod{26} = 9$

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

$$key^{-1} = 9 * \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix} = \begin{bmatrix} 11 & 22 & 14 \\ 7 & 9 & 21 \\ 17 & 0 & 3 \end{bmatrix}$$

To convert the cipher text vectors into plain text vectors, we multiply the deciphering matrix ($key^{-1}$matrix) by each cipher text vector and replace each new vector by its residue modulo 26.

$$\text{ARP} = \begin{bmatrix} 584 \\ 468 \\ 45 \end{bmatrix} \pmod{26} = \begin{bmatrix} 12 \\ 0 \\ 19 \end{bmatrix}$$ Converting each entry in the cipher text vector into its corresponding position in the alphabet we get,

$$\begin{bmatrix} 12 \\ 0 \\ 19 \end{bmatrix} = \text{MAT}$$

Continuing the same process of deciphering for other block of letters we get the actual text as MATHAMATORES.

## XIV. SUMMARY

Data security is an essential component of an organization in order to keep the information or data safe from various competitors. It helps to ensure the privacy of a user's personal information from others. Cryptography ensures that the contents of a message are confidentially transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and the data cannot be changed means the original information cannot be changed. Strong encryption algorithms and optimized key management techniques always help in achieving confidentiality, authentication, and integrity of data and reduce the overheads of the system**.**

## XV. REFERENCE

[1] Vikasagarwal, Shruti Agarwal, Rajesh Deshmukh, "Analysis and review of encryption and decryption for secure communication", *IJSER* , vol.2 , no.2, February 2014, ISSN 2347-3848.

[2] Brown Lawrie, Steflik Dick, "Symmetric encryption algorithms", *CS-480b* Lecture slides.

[3] Preeti Singh, Praveen Shende, "Symmetric key cryptography: Current Trends", *IJCSMC,* Vol. 3, no. 12, pp. 410-415, December 2014, ISSN 2320-088X.

[4] Vishwa Gupta, GajendraSingh,Ravindra Gupta, "Advance cryptography algorithm to improve data security" , IJARCSSE, vol. 2, no. 1, January 2012, ISSN 2277-128X.

[5]https://www.technopedia.com/definition/1773/decryption

[6] Hill cipher and modular linear algebra,[online] Available:http://apprendre-en-ligne.net/crypto/hill/hillciph.pdf

[7]https://en.wikipedia.org/wiki/cryptography

[8]https://www.technopedia.com/definition/25403/encryption-key

[9]http://resources.infosecinstitute.com/basics-of-cryptography-the-practical-application-and-use-of-cryptography/#gref

[10] https://www.cybrary.it/0p3n/learn-hill-cipher-3*3-matrix-multiplicative-inverse-example/