International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763
Issue 12, Volume 2 (December 2015) www.ijirae.com

ENCRYPTION USING LESTER HILL CIPHER ALGORITHM

Thangarasu.N
Research Scholar in Department of Computer Science
Bharathiar University,Coimbatore

Dr.Arul Lawrence SelvaKumar
Dean & Professor, Department of CSE
Rajiv Gandhi Institute of Technology,Bangalore

Abstract - The Hill cipher algorithm is one of the symmetrickey algorithms that have several advantages in data encryption as well as decryptions. But, the inverse of the key matrix used for encrypting the plaintext does not always exist. Then if the key matrix is not invertible, then encrypted text cannot be decrypted. In the Involuntary matrix generation method the key matrix used for the encryption is itself invertible. So, at the time of decryption we need not to find the inverse of the key matrix. The objective of this paper is to encrypt an text using a technique different from the conventional Hill Cipher.

Keyword - Encryption, Decryption, Key, Plain Text, Cipher Text, Hill Cipher

I. INTRODUCTION

Conventional Encryption is referred to as symmetric encryption or single key encryption. It was the only type of encryption in use prior to the development of public-key encryption. Conventional encryption can further be divided into the categories of classical and modern techniques. The information security is an increasingly important problem. Cryptography, the science of encryption, plays a central role in mobile phone communications, pay-TV, e-commerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords, and touches on many aspects of our daily lives. Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (cipher text) and then retransforming that message back to its original form. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, andengineering [1]

Substitution cipher is one of the basic components of classical ciphers. A substitution cipher is a method of encryption by which units of plaintext are substituted with cipher text according to a regular system; the units may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution [3]. The units of the plaintext are retained in the same sequence as in the cipher text, but the units themselves are altered. There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic.

In this paper, we have proposed aHill cipher algorithm which uses an involuntary key matrix for encryption. The objective of this paper is to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where we may not be able to decrypt the encrypted message, if the key matrix is not invertible. Also the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption, as we use involuntary key matrix for encryption. Using this key matrix we encrypted text. Our algorithm works well for all types of text except for the encrypted text as well as decrypt text.

II. HILL CIPHER

It is developed by the mathematician Lester Hill. The core of Hill cipher is matrix manipulations. For encryption, algorithm takes *m* successive plaintext letters and instead of that substitutes *m* cipher letters. In Hill cipher, each character is assigned a numerical value as reverse order like *a*= 25, *b*= 24, ..., z = 0[2][4]. The substitution of cipher text letters in the place of plaintext letters leads to *m* linear equation. The Hill Cipher is a linear algebra technique [6] but it relies on modular arithmetic. So we will give a quick reminder on modular calculations. Throughout the 0discussion we will let n be the modulus, so n will be an integer and $n \geq 2$.

Definition 1:
Let m and k be two integers, then we say that $m \equiv k \pmod n$, if $n \mid (m-k)$, that is, n divides the quantity m - k evenly.

Definition 2:
Let k be an integer, when we write k (mod n), we mean the number m that is in the range $25 \leq m < n$ such that $m \equiv k \pmod n$.

Arithmetic:
Addition, subtraction, and multiplication modulo a number are fairly straight forward. Simply does the addition, subtraction, or multiplication as usual then take the result mod the number [4]

Definition 3:
Let k be an integer, then k^{-1} (mod n) is the number m that is in the range $0 \leq m < n$ such that $m.k \pmod n \equiv 1$, if m exists. If no such number m exists then we say that k does not have an inverse modulo n or that k is not invertible mod n.

Theorem 1: *Let k be an integer, then k^{-1} (mod n) exists if and only if the greatest common divisor of k and n is 1, that is, gcd (k, n) = 1. Another way to say this is that k and n are relatively prime [1]*

Theorem 2: *Let A be an n * n integer matrix, then A^{-1} (mod n) exists if and only if det(A) is invertible modulo n. That is, if and only if $(det(A))^{-1}$ (mod n) exists.*

III. ENCRYPTION WITH THE HILL CIPHER

The Hill Cipher Encryption Algorithm

1. Find an n * n matrix E that is invertible modulo 26. This is actually the encryption key.
2. Take the message that is to be sent (the plaintext), remove all of the spaces and punctuation symbols, and convert the letters into all uppercase.
3. Convert each character to a number between 0 and 25. The usual way to do this is A = 25, B = 24, C = 23. . . Z = 0.

A	B	C	D	E	F	G	H	I	J	K	L	M
25	24	23	22	21	20	19	18	17	16	15	14	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12	11	10	9	8	7	6	5	4	3	2	1	0

As a historical note, Lester Hill [5] did not use this coding of letters to numbers; he simply mixed up the order. Mixing up the order does not make the method more secure, it simply combines the Hill cipher with a simple substitution cipher, which is easy to break.

4. Divide this string of numbers up into blocks of size n. Note that if E is an n * n Matrix then the block size is n. Another note, if the message does not break evenly into blocks of size n we pad the ending of the message with characters, this can be done at random.
5. Write each block as a column vector of size n. At this point the message is a sequence of n-dimensional vectors, v1, v2,.....,vt.
6. Take each of the vectors and multiply them by the encryption matrix E, so
   Ev1 = V1
   Ev2 = V2
   Ev3 = V3
   …
   Evt = Vt
7. Take the vectors v1, v2,.....,vt., write the entries of the vectors in order, convert the numbers back to characters and you have your cipher text. One note about this algorithm is that we can do step 6 with a single matrix multiplication.If we let the message matrix M and E there for EM=C

EXAMPLE:

Say Alice wants to send Bob the message “SRIROSAN IS A GOOD BOY”

1. Alice chooses the block size n = 3 and chooses the encryption matrix E to be

$$E = \begin{vmatrix} 2 & 4 & 5 \\ 2 & 7 & 8 \\ 4 & 6 & 2 \end{vmatrix}$$

   Since det(E) (mod 26) = 12, and 12 is invertible modulo 26, the matrix E is also invertible modulo 26.

2. The message that is to be sent is “SRIROSAN ISAGOODBOY ", removing the spaces and 0punctuation symbols, and convert the letters into all uppercase gives
   SRIROSAN ISAGOODBOY

3. Conversion to numbers using A = 25, B = 24, C = 23, . . . , Z = 0, gives
   7 8 17 8 11 7 25 12 17 7 25 19 11 11 22 24 11 1
   So no padding is needed here.

4. Dividing this string of numbers up into blocks of size 3.

   7 8 17 8 11 7 25 12 17 7 25 19 11 11 22 24 11 1

   so no padding is needed here.

5. Converting these blocks into a message matrix M gives,

$$M = \begin{vmatrix} 7 & 8 & 17 & 8 & 11 & 7 \\ 25 & 12 & 17 & 7 & 25 & 19 \\ 11 & 11 & 22 & 24 & 11 & 1 \end{vmatrix}$$

6. Multiply by the encryption matrix E,

$$E = \begin{vmatrix} 2 & 4 & 5 \\ 2 & 7 & 8 \\ 4 & 6 & 2 \end{vmatrix}$$

$$M = \begin{vmatrix} 7 & 8 & 17 & 8 & 11 & 7 \\ 25 & 12 & 17 & 7 & 25 & 19 \\ 11 & 11 & 22 & 24 & 11 & 1 \end{vmatrix}$$

   Therefore EM = C

$$C = \begin{vmatrix} 20 & 23 & 21 & 16 & 6 & 24 \\ 17 & 6 & 17 & 23 & 25 & 25 \\ 18 & 22 & 6 & 18 & 8 & 14 \end{vmatrix}$$

7. Convert C into the cipher text.

20	23	21	16	6	24		F	C	E	J	T	B
17	6	17	23	25	25		I	T	I	C	A	A
18	22	6	18	8	14		H	D	T	H	R	L

   FCEJTBITICAAHDTHRL

So Alice will send “FCEJTBITICAAHDTHRL" to Bob.

Since this is a symmetric cipher, Alice and Bob would have to share this key with each other. They obviously could not simply call or text each other with this information since Eve could easily intercept that call or text and would know the key[9].

So either Alice or Bob would have to meet in person, in a secure location, and exchange the key or they would need some other trusted person to deliver the key from Alice to Bob. This difficulty in exchanging the key securely gave rise to the creation of public-key systems which are comm. only used today, for more information on public-key systems please see the references [4].

IV. DECRYPTION WITH THE HILL CIPHER

Now that Bob has the encrypted message and the encryption key he can decrypt the message that Alice had sent to him. The decryption algorithm is essentially the same as the encryption algorithm, except that we use E□1 in place of E.

Since EM = C, and E is invertible we can calculate $M = E^{-1}C$. We will call $D = E^{-1}$ the decryption matrix, so DC = M. Remember that this inverse is the inverse modulo 26 [8].

THE HILL CIPHER DECRYPTION ALGORITHM

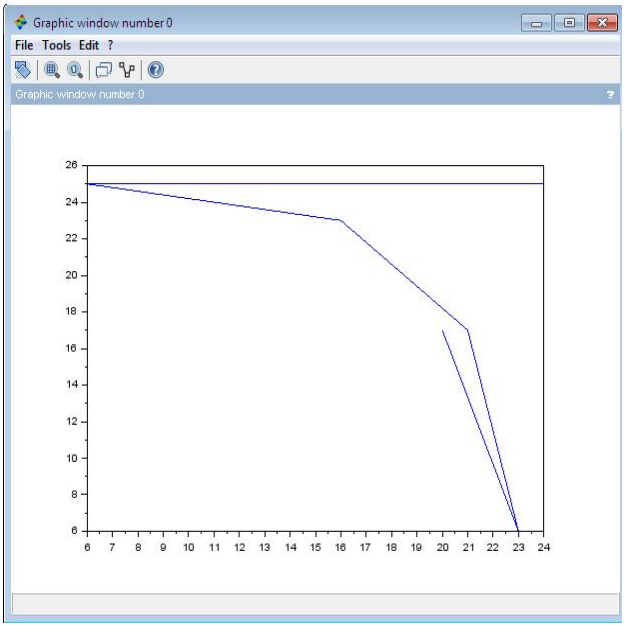
1. Find $D = E^{-1} \pmod{26}$. This is the decryption key.
2. Take the cipher text and convert it to the matrix C.
3. Calculate DC = M.
4. Convert the matrix M to the plaintext message. You may need to insert the appropriate spaces and punctuation symbols since these were removed.

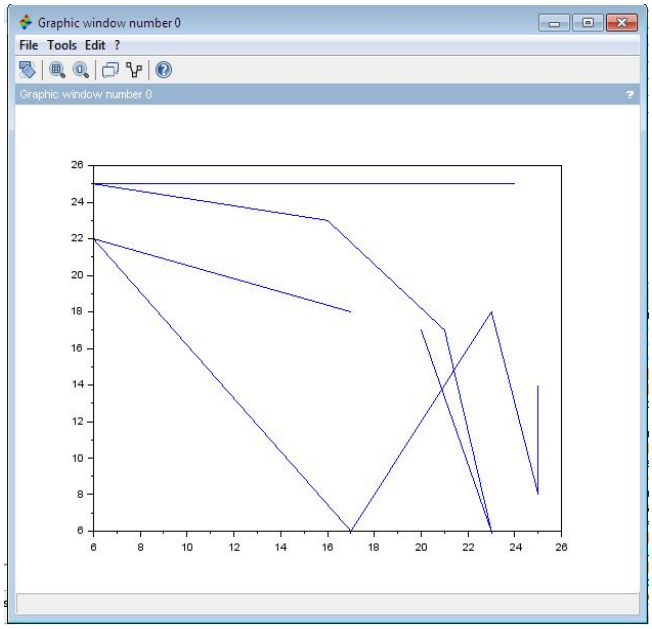
CRYPTOGRAPHIC SYSTEMS ARE GENERALLY CLASSIFIED ALONG THREE INDEPENDENT DIMENSIONS:

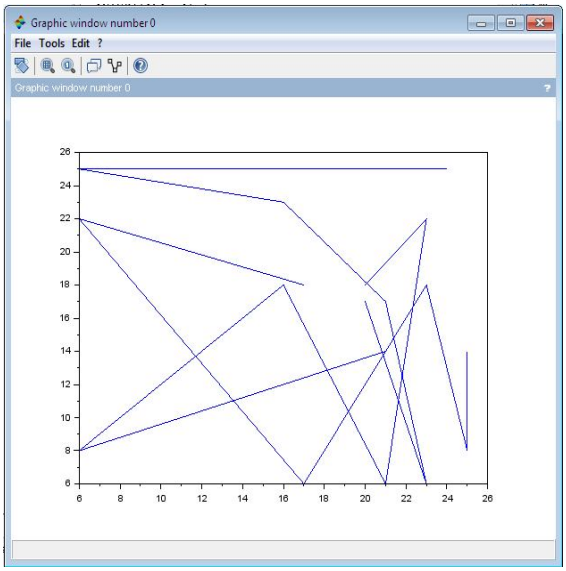
1. Type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles.

2. Those are substitution, in which each element in the plain text is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition [2].
3. The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption [3].
4. The way in which the plaintext is processed: A block cipher processes the input on block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along [4].

V. IMPLEMENTATION FOR THE PROBLEM IN SCILAB USING CIPHER TEXT







VI. CONCLUSION

We have given formulae for the numbers of n*n invertible and involuntary matrices mod m. We note that, while involuntary matrices may save decryption time, requiring that key matrices be involuntary significantly reduces the size of the key. We have also observed that, while increasing the dimension of key matrices leads to a larger key, increasing the modulus (i.e., the size of the alphabet) may not.

When. Thus, the largest key spaces result from a large matrix dimension and an alphabet of prime order. This significantly increased the resistance of the algorithm to the known plaintext attack. Hill also implements an involuntary key generation algorithmwhere the same matrix key can be used for both encryption and decryption.

REFERENCE

[1]. Bidhudendra Acharya, GirijaSankarRath, Sarat Kumar Patra, Saroj Kumar Panigraphy 2007. Novel Methods of generating Self-Invertible Matrix for hill Cipher Algorithm, International Journal of Security, Volume 1, Issue 1,2007, PP.14-21.
[2]. Menezes, A.J.,P.C. Van Oorschot, S.A.Van Stone.1996. Handbook of applied Cryptography. CRC press.
[3]. Saeednia, S., 2000.How to make the Hill Cipher secure. Cryptologia,24(4):353-360.
[4]. Stallings, W. Cryptography and Network Security, 2005. 4th edition, Prentice Hall.
[5]. Lester S. Hill. Cryptography in an Algebraic Alphabet. Amer. Math.
[6]. David Lay. Linear Algebra and its Applications. Pearson, Boston, 3rd edition, 2006.
[7]. Maxima Computer Algebra System. http://maxima.sourceforge.net/, 2013.
[8]. D. Luciano and G. Prichett, “From Caesar Ciphers to Public-Key Cryptosystem”,.
[9]. M. Toorani and A. Falahati, “A Secure Variant of the Hill Cipher”, in Proc. www.**scilab**.org/download/latest

