Enhancement of Arithmetic operators in Hill Cipher algorithm of Encipher & Decipher

Mohammad Rafeek Khan[1] , Md Imran Alam[2]

Lecturer,Department of Computer Engineering & Networks, Jazan University, Jazan Saudi Arabia

rafeek04@gmail.com, imran.amu2008@gmail.com

Abstract— **Nowadays abundant of data are transferred through networks, the complete dominancy of Internet in every sphere of life has made life easy, transferring of data over internet is on fingertip or just one click away, but in course of transferring such heavy of data over internet causes the issue of security. Here comes the concept of Cryptography, the most recent technique used for security. Many works and research have been done to keep the data integrity and security intact. One of the popular and effective techniques is Hill Cipher algorithm for encryption and decryption in which provided alphabetical letters are encrypted.**

In our research paper we have appended numeric characters and arithmetic operators for encryption and decryption. We have used Modulo forty as there are forty total characters. We have titled our research Paper as "Enhancement of Arithmetic operators in Hill Cipher algorithm of Encipher & Decipher".

Keywords— **Cryptography, Arithmetic operators, Encipher, Decipher, Security, Internet, Hill Cipher Algorithm.**

I. Introduction

1.1 Encryption and decryption

Data that can be read and understood without any special measures is called Plaintext or clear text. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. We use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data.

Encryption is a process of translating a message, called the Plaintext, into an encoded message, called the Ciphertext. This is usually accomplished using a secret Encryption Key and a cryptographic Cipher.

Two basic types of Encryption are commonly used:

- Symmetric Encryption, where a single secret key is used for both encryption and decryption.
- Asymmetric Encryption, where a pair of keys is used -- one for Encryption and the other for Decryption.

The process of reverting cipher text to its original plaintext is called decryption.

1.2 What is cryptography?

Cryptography's the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across. Insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

An Introduction to Cryptography: While cryptography is the science of securing data, crypto analysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

1.3 Conventional cryptography

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government. Fig 1.1 is an illustration of the conventional encryption process.

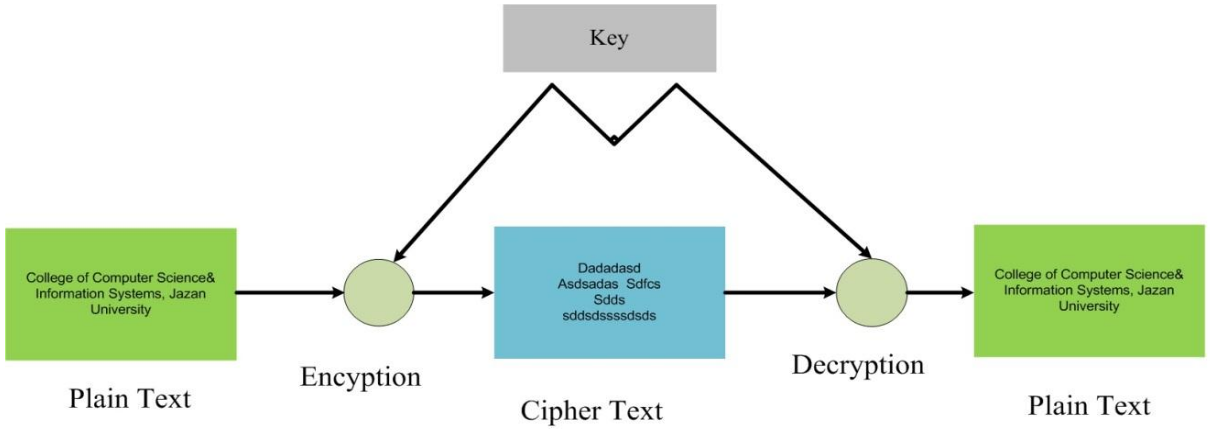
Key
College of Computer Science& Information Systems, Jazan University
Plain Text
Encyption
Dadadasd Asdsadas Sdfcs Sdds sddsdssssdsds
Cipher Text
Decryption
College of Computer Science& Information Systems, Jazan University
Plain Text

Fig 1.1 Conventional Encryption

1.4 Caesar’s Cipher

An extremely simple example of conventional cryptography is a substitution cipher. A substitution cipher substitutes one piece of information for another. This is most frequently done by offsetting letters of the alphabet. Two examples are Captain Midnight’s Secret Decoder Ring, which you may have owned when you were a kid, and Julius Caesar’s cipher. In both cases, the algorithm is to offset the alphabet and the key is the number of characters to offset it. For example, if we encode the word “SECRET” using Caesar’s key value of 3, we offset the alphabet so that the 3rd letter down (D) begins the alphabet. So starting with ABCDEFGHIJKLMNOPQRSTUVWXYZ and sliding everything up by 3, you get DEFGHIJKLMNOPQRSTUVWXYZABC where D=A, E=B, F=C, and so on. Plain text cipher text plaintext decryption encryption.

II. Previous Work

Hill Cipher

Hill ciphers is an application of linear algebra to cryptology. It was developed by the mathematician Lester Hill. The Hill cipher algorithm takes m successive plaintext letters and substitute’s m cipher text letters for them. The substitution is determined by m linear equations in which each character is assigned a numerical value) 25 ,...., 1 , 0 (= = = z b a . Let m be a positive integer, the idea is to take m linear combinations of the m alphabetic characters in one plaintext element and produce m alphabetic characters in one cipher text element. Then, an m × m matrix A is used as a key of the system such that A is invertible modulo 26 [5]. For the plaintext block (x= x_1, x2…xm) (the numerical equivalents of m letters) and a key matrix A, the corresponding cipher text block (y= y1, y2, …ym) can computed as

Encryption --

$(y_1, y_2, \dots y_m) = (x_1, x_2, \dots . x_m)\ A \bmod(26)$

Where

$$A = \begin{bmatrix} a_{11}, a_{12}, & \dots & a_{1m} \\ a_{21}, a_{22}, & \dots & a_{2m} \\ , & , & \dots, \\ \dots a_{m1}, a_{m2}, & \dots & a_{mm} \end{bmatrix}$$

The cipher text is obtained from the plaintext by means of a linear transformation. Decryption:

$(y_1, y_2, \dots y_m) = (x_1, x_2, \dots . x_m)\ A^{-1} \bmod(26)$

Where A^{-1} is the inverse of matrix of A.

III. Proposed Method (Enhancement of Arithmetic operators in Hill Cipher)

This algorithm can be used to encrypt and decrypt the message which is the combination of Alphabetical, Numbers and Arithmetic operators. In this algorithm we are using modulo 40. Asymmetric cryptographic technique is being used in this algorithm.

Public key: Cipher Message, N, 40
Private Key: I matrix

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1
14	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**
2	3	4	5	6	7	8	9	+	-	*	/		
28	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**		

Table 3.1 Alphabet, Numbers and Arithmetic Operator Corresponding Value

3.1 Enciphering Procedure

a) Assign numbering 0, 1 …39 corresponding alphabetic, number and arithmetic operators (A, B,……Z, 0, 1,2….., +,-,*,/) .
b) Given text message, store in a string variable. This is called m. Store the text To encrypt a text message at first the given text and numbers are stored in a string variable, say m.
c) Choose I matrix of i*i and natural number N.
d) Convert message into blocks according the matrix I Make plain text or message as blocks according to the I matrix.
e) Multiply text message (corresponding number) with I matrix , after the result matrix is multiplied by N.
f) Find remainder apply modulo 40 on resultant matrix step e. this is the decrypted text..

3.2 Deciphering Procedure

a) Find the I^{-1} and N^{-1} by using private key I and N.
b) Convert encrypted message in the form blocks like $I^{-1.}$
c) Multiply encrypted message (corresponding value) with N^{-1}
d) Find the remainder by using modulo 40 of result message of step c. this result is decrypt message.

Requirement of Basic Matrix theory

To follow above procedure, we should be familiar with basic matrix theory and modular arithmetic. We will be expected to:

- Know common terms and definitions such as “vector” and “transpose.”
- Multiplication of matrices.
- Find the determinant of a matrix.
- Find the residue modulo 40 of entries in a vector.
- Perform elementary row operations in a matrix.

IV. Implementation

Enhancement of arithmetic operators in hill cipher algorithm is shown here by using an example. Suppose we have to send message “SEND 2*SALARY” from one end to another end systems through internet. Encipher will be performed sender end with help of public key 40, e and private key k. Decipher will be performed sender end with help of public key 40, e^{-1} and private key I^{-1}.

A. Enciphering a Message

a) Assigning the data value corresponding to the message

SNO	1	2	3	4	5	6	7	8	9	10	11	12
Message	S	E	N	D	2	*	S	A	L	A	R	Y
Data Value	18	4	13	3	28	38	18	0	11	0	17	24

Table 4.1 for Data value corresponding Plain Text

b) Group the plaintext blocks of 3. If we do not able to make last block repeat last letter.

Block	Plain Text Block of 3 Letters			Data Value Block		
1	S	E	N	18	4	13
2	D	2	*	3	28	38
3	S	A	L	18	0	11
4	A	R	Y	0	17	24

Table 4.2 for Data value Block

c) We chose a matrix ixi which is invertible, where i= 3

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix}$$

Det(I)= 11

$$\text{Adj } I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix}$$

Now I^{-1} = (Determinants' Reciprocals modulo 40)*Adj A * Modulo 40.

$$K^{-1} = 11* \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix} \text{ Modulo 40, } \quad K^{-1} = \begin{bmatrix} 11 & 0 & 0 \\ 0 & 11 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

d) Enciphering the plaintext

s =(18,4,13), invertible matrix I

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix}$$

cipher =(I* S)mod 40

$$\text{Cipher of (S EN)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix} * \begin{bmatrix} 18 \\ 4 \\ 13 \end{bmatrix} \text{ Mod } 40 = \begin{bmatrix} 18 \\ 4 \\ 23 \end{bmatrix}$$

$$\text{Cipher of (D 2 *)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix} * \begin{bmatrix} 3 \\ 28 \\ 38 \end{bmatrix} \text{ Mod } 40 = \begin{bmatrix} 3 \\ 28 \\ 18 \end{bmatrix}$$

$$\text{Cipher of (S A L)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix} * \begin{bmatrix} 18 \\ 28 \\ 38 \end{bmatrix} \text{ Mod } 40 = \begin{bmatrix} 18 \\ 28 \\ 18 \end{bmatrix}$$

and

$$\text{Cipher of (A RY)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix} * \begin{bmatrix} 0 \\ 17 \\ 24 \end{bmatrix} \text{ Mod } 40 = \begin{bmatrix} 0 \\ 17 \\ 24 \end{bmatrix}$$

Plain Text	S	E	N	D	2	*	S	A	L	A	R	Y
Cipher Value	18	4	23	3	28	18	18	0	18	0	17	24
Cipher Text	S	E	X	D	2	S	S	A	S	A	R	Y

Table 4.3 for Enciphering

e) We select a natural number N= 9 , multiply by this number to cipher value of the text

Plain Text	S	E	N	D	2	*	S	A	L	A	R	Y
Cipher Value (CV)	18	4	23	3	28	18	18	0	1	0	17	24
N*CV	162	36	207	27	252	162	162	0	9	0	153	216
Mod 40	2	36	7	27	12	2	2	0	9	0	33	16

Table 4.4 for Cipher text

Now Cipher Text= C+H1MCCAJA7Q
Here Public key 40 and ‘I’ and natural number N are private key.

4.2 Deciphering

a) N^{-1} is the reciprocal inverse of 9. Then, $N^{-1} = 9$

Encrypted Data Value	2	36	7	27	12	2	2	0	9	0	33	16
N^{-1}*EDV	18	324	63	243	108	18	18	0	81	0	297	144
Mod40	18	4	23	3	28	18	18	0	1	0	17	24

Table 4.5 for multiplication reciprocal inverse of N

Now for decipher we have to use I^{-1} , for first block

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix} * \begin{bmatrix} 18 \\ 4 \\ 23 \end{bmatrix} \text{Mod } 40 = \begin{bmatrix} 18 \\ 4 \\ 13 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix} * \begin{bmatrix} 3 \\ 28 \\ 38 \end{bmatrix} \text{Mod } 40 = \begin{bmatrix} 3 \\ 28 \\ 38 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix} * \begin{bmatrix} 18 \\ 0 \\ 11 \end{bmatrix} \text{Mod } 40 = \begin{bmatrix} 18 \\ 0 \\ 1 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 11 \end{bmatrix} * \begin{bmatrix} 0 \\ 17 \\ 24 \end{bmatrix} \text{Mod } 40 = \begin{bmatrix} 0 \\ 17 \\ 24 \end{bmatrix}$$

Enciphering	Plain Text	S	E	N	D	2	*	S	A	L	A	R	Y
	Cipher Value	18	4	23	3	28	18	18	0	18	0	17	24
	N*CV	162	36	207	27	252	162	162	0	9	0	153	216
	Mod 40	2	36	7	27	12	2	2	0	9	0	33	16
Deciphering	N^{-1}*EDV	18	324	63	243	108	18	18	0	81	0	297	144
	Mod40	18	4	23	3	28	18	18	0	1	0	17	24
	Decrypted Text	S	E	N	D	2	*	S	A	L	A	R	Y

Table 4.6 for Enciphering and Deciphering Table

V. Result and Future Scope

The Working procedures of enhancement of arithmetic operator's encryption of decryption is correct in implementation. In this I have also used the asymmetric technique (public and private key) for enciphering and deciphering.
This technique can be used to encipher and decipher those plain texts which contain arithmetic operators.

VI. Conclusion

Cryptography is the one the technique to provide security of data, during transferring data over internet. Hill cipher Technique is better technique, in which encryption and decryption are performed through matrices methods. In our procedure, we have appended the arithmetic operators in hill cipher technique. We have also applied the asymmetric technique to provide the more security level in enchantment of arithmetic operators Hill cipher; this technique procedure has less complexity as compare RSA technique.

REFERENCES

[1] H. Imai, G. Hanaoka, J. Shikata, A. Otsuka, A.C. Nascimento, Cryptography with information theoretic security", Information Theory Workshop, 2002, Proceedings of the IEEE, 20-25 Oct 2002.

[2] Bibhudendra Acharya, Girija Sankar Rath, and Sarat Kumar Patra, Nove Modified Hill Cipher Algorithm, Proceedings of ICETAETS 2008.

[3] Parkash Kuppu swamy, Dr. C. Chandrasekar, Enrichment of security through cryptographic public key algorithmic based on block cipher, Indian Journal of Computer Science and Engineering (IJCSE), ISSN : 0976-5166 ,Jul 2011

[4] John C. Bowman, Math 422 Coding Theory & Cryptography,University of Alberta, Edmonton, Canada.

[5] David A. Santos, Linear Algebra Notes, January 2, 2010 Revision, dsantos@ccp.edu.

[6] Pranam Paul, Saurabh Dutta, "An Enhancement of Information SecurityUsing Substitution of Bits Through Prime Detection in Blocks", Proceedings of National Conference on Recent Trends in Information Systems (ReTIS-06)

[7] Katos, V. A Randomness Test for Block Ciphers. Applied Mathematics, (2005) Elsevier Publications

[8] D. Wright, "Nineteenth Century: Statistics," [online document], 1999 Nov 19, [cited 2007 Oct 4], http://www.math.okstate.edu/~wrightd/crypt/crypt-intro/node9.html

[9] X. Yuan, "Lecture 6: Classic Ciphers," [online document], Available http://vanets.vuse.vanderbilt.edu/~xue/cs291fall06/lecture6.pdf

[10] www.nai.com