International Journal of Mathematical Archive-6(11), 2015, 52-56
Available online through www.ijma.info ISSN 2229 – 5046

ENHIDE AND DEHIDE MESSAGES USING MATRIX

D. MURUGAN[1], T. N. KAVITHA*[2]

**[1]Research Scholar, [2]Assistant Professor of Mathematics,
SCSVMV University, Enathur, Kanchipuram, India.**

(Received On: 06-10-15; Revised & Accepted On: 24-11-15)

ABSTRACT

We try to find the new algorithm for cryptography using matrix. This is the successful method for make the message more secure. Here we are enhide the message using a arbitrary matrix and using some row column operation we make it the message more secure. We dehide the message using the matrix inverse of the same matrix.

INTRODUCTION

Cryptology is the science of creating messages into secreted form. Nowadays, cryptology has become an extremely important field in exchange of information (credit card numbers, passwords, etc.). Mathematics is often used to develop systems for creating codes. Here we try to find the cryptographic writing using some mathematical operations.
What is cryptography?

In our school day's we pass messages to our friends using some code words, otherwise we add some extra letters with the messages and pass it, the third person should unable to understand the message.

First, we are converting the message into alphabetic numerals and after that using some mathematical operations for enhide and dehide the message. The process of enhide means to hide the message, and dehide means the process of recover the hidden message.

We prepare an algorithm newly to hide the message; the following example explains the algorithm with its procedure

Example:

Step-1: Assign numbers to the letters of the alphabet. For encrypt our message we will use the following:
A 1 B 2 C 3 D 4 E 5 F 6 G 7 H 8 I 9 J 10 K 11 L 12 M 13 N 14 O 15
P 16 Q 17 R 18 S 19 T 20 U 21 V 22 W 23 X 24 Y 25 Z 26.

Step-2: Choose an encoding matrix; it is an arbitrary matrix (it must have an inverse.)

$$A=\begin{bmatrix}1 & 2 & 3\\ 2 & 1 & 1\\ 1 & 1 & 1\end{bmatrix}$$

Step-3: Write your message using the alphabetical numbers

D	I	A	M	O	N	D	C	U	T	S	D	I	A	M	O	N	D
4	9	1	13	15	14	4	3	21	20	19	4	9	1	13	15	14	4

Step-4: Change the message as 3x6 matrices

$$X=\begin{bmatrix}4 & 13 & 4 & 20 & 9 & 15\\ 9 & 15 & 3 & 19 & 1 & 14\\ 1 & 14 & 21 & 4 & 13 & 4\end{bmatrix}$$

Corresponding Author: T. N. Kavitha[2]*
[2]Assistant Professor of Mathematics, SCSVMV University, Enathur, Kanchipuram, India.

Already we choose an encoding matrix, multiply the matrix using matrix multiplication with the message matrix.

Step-5: Encoding matrix (A) and text message matrix (X), multiply the both

$$AX\begin{bmatrix}1 & 2 & 3\\ 2 & 1 & 1\\ 1 & 1 & 1\end{bmatrix}=\begin{bmatrix}4 & 13 & 4 & 20 & 9 & 15\\ 9 & 15 & 3 & 19 & 1 & 14\\ 1 & 14 & 21 & 4 & 13 & 4\end{bmatrix}$$

$$AX=\begin{bmatrix}25 & 85 & 73 & 70 & 50 & 55\\ 18 & 55 & 32 & 63 & 32 & 48\\ 14 & 42 & 28 & 43 & 23 & 33\end{bmatrix}$$

For more secure, we should subtract row two from row one and the resultant as our row one now.

Step-6: R1 - R2 = R1

$$AX=\begin{bmatrix}7 & 30 & 41 & 7 & 18 & 7\\ 18 & 55 & 32 & 63 & 32 & 48\\ 14 & 42 & 28 & 43 & 23 & 33\end{bmatrix}$$

From the third row a scalar 2(any arbitrary value) can be subtract to eliminate the row.

Step-7: R3 = R3 – 2

$$AX=\begin{bmatrix}7 & 30 & 41 & 7 & 18 & 7\\ 18 & 55 & 32 & 63 & 32 & 48\\ 12 & 40 & 26 & 41 & 21 & 31\end{bmatrix}$$

We choose another scalar 3, and subtract it from row two.

Step-8: R2 = R2 – 3

$$AX=\begin{bmatrix}7 & 30 & 41 & 7 & 18 & 7\\ 15 & 52 & 29 & 60 & 29 & 45\\ 12 & 40 & 26 & 41 & 21 & 31\end{bmatrix}$$

We wants to make into more protected message, so again add a scalar 2 with column one.

Step-9: C1 = C1 + 2

$$AX=\begin{bmatrix}9 & 30 & 41 & 7 & 18 & 7\\ 17 & 52 & 29 & 60 & 29 & 45\\ 14 & 40 & 26 & 41 & 21 & 31\end{bmatrix}$$

any scalar can be used to add with any row or any column. It is accordind to our wish. Here in this example we choose columns and add any arbitrary scalars with the column, we can select any rows and add any scalar operations multiplication or addition.

Step-10: C2 = C2 + 3

$$AX=\begin{bmatrix}9 & 33 & 41 & 7 & 18 & 7\\ 17 & 55 & 29 & 60 & 29 & 45\\ 14 & 43 & 26 & 41 & 21 & 31\end{bmatrix}$$

Step-11: C3 = C3 + 5

$$AX=\begin{bmatrix}9 & 33 & 46 & 7 & 18 & 7\\ 17 & 55 & 34 & 60 & 29 & 45\\ 14 & 43 & 31 & 41 & 21 & 31\end{bmatrix}$$

Step-12: C4 = C4 – 5

$$AX = \begin{bmatrix} 9 & 33 & 46 & 2 & 18 & 7 \\ 17 & 55 & 34 & 55 & 29 & 45 \\ 14 & 43 & 31 & 36 & 21 & 31 \end{bmatrix}$$

Step-13: C5 = C5 + 6

$$AX = \begin{bmatrix} 9 & 33 & 46 & 2 & 24 & 7 \\ 17 & 55 & 34 & 55 & 35 & 45 \\ 14 & 43 & 31 & 36 & 27 & 31 \end{bmatrix}$$

Step-14: C6 = C6 – 4

$$AX = \begin{bmatrix} 9 & 33 & 46 & 2 & 24 & 3 \\ 17 & 55 & 34 & 55 & 35 & 41 \\ 14 & 43 & 31 & 36 & 27 & 27 \end{bmatrix}$$

Step 15: Message is now safe to send! We use the multiplication modulo 26, to hide our message, this total process from step 1 to step 14 we call it as enhide

9	17	14	33	55	43	46	34	31	2	55	36	24	35	27	3	41	27
I	Q	N	G	C	Q	T	H	E	B	C	J	X	I	A	C	O	A

The enhide message is ready now

I	Q	N	G	C	Q	T	H	E	B	C	J	X	I	A	C	O	A

Now send the enhide message.

The receiver can received the message in the form

I	Q	N	G	C	Q	T	H	E	B	C	J	X	I	A	C	O	A

Now the receiver have to dehide the enhide message. First the receiver have to change the message into alphabetical numerals as follows

I	Q	N	G	C	Q	T	H	E	B	C	J	X	I	A	C	O	A
9	17	14	7	3	17	20	8	5	2	3	10	24	9	1	3	15	1

Now write the corresponding 3 x 6 matrices:

$$X = \begin{bmatrix} 9 & 7 & 20 & 2 & 24 & 3 \\ 17 & 3 & 8 & 3 & 9 & 15 \\ 14 & 17 & 5 & 10 & 1 & 1 \end{bmatrix}$$

Next our process everything are reverse work of the enhide process that we call it as dehide

Step-1: C6 = C6+4

$$X = \begin{bmatrix} 9 & 7 & 20 & 2 & 24 & 7 \\ 17 & 3 & 8 & 3 & 9 & 19 \\ 14 & 17 & 5 & 10 & 1 & 5 \end{bmatrix}$$

Step-2: C5 = C5-6

$$X = \begin{bmatrix} 9 & 7 & 20 & 2 & 18 & 7 \\ 17 & 3 & 8 & 3 & 3 & 19 \\ 14 & 17 & 5 & 10 & -5 & 5 \end{bmatrix}$$

Step-3: C4 = C4+5

$$X = \begin{bmatrix} 9 & 7 & 20 & 2 & 18 & 7 \\ 17 & 3 & 8 & 8 & 3 & 19 \\ 14 & 17 & 5 & 15 & -5 & 5 \end{bmatrix}$$

Step-4: C3 = C3-5

$$X = \begin{bmatrix} 9 & 7 & 15 & 7 & 18 & 7 \\ 17 & 3 & 3 & 8 & 3 & 19 \\ 14 & 17 & 0 & 15 & -5 & 5 \end{bmatrix}$$

Step-5: C2 = C2-3

$$X = \begin{bmatrix} 9 & 4 & 15 & 7 & 18 & 7 \\ 17 & 0 & 3 & 8 & 3 & 19 \\ 14 & 14 & 0 & 15 & -5 & 5 \end{bmatrix}$$

Step-6: C1 = C1-2

$$X = \begin{bmatrix} 7 & 4 & 15 & 7 & 18 & 7 \\ 15 & 0 & 3 & 8 & 3 & 19 \\ 12 & 14 & 0 & 15 & -5 & 5 \end{bmatrix}$$

Step-7: R2 = R2+3

$$X = \begin{bmatrix} 7 & 4 & 15 & 7 & 18 & 7 \\ 18 & 3 & 6 & 11 & 6 & 22 \\ 12 & 14 & 0 & 15 & -5 & 5 \end{bmatrix}$$

Step-8: R3 = R3+2

$$X = \begin{bmatrix} 7 & 4 & 15 & 7 & 18 & 7 \\ 18 & 3 & 6 & 11 & 6 & 22 \\ 14 & 16 & 2 & 17 & -3 & 7 \end{bmatrix}$$

Step-9: R1 = R1+R2

$$X = \begin{bmatrix} 25 & 7 & 21 & 18 & 24 & 29 \\ 18 & 3 & 6 & 11 & 6 & 22 \\ 14 & 16 & 2 & 17 & -3 & 7 \end{bmatrix}$$

We Choose the square matrix A with inverse matrix that inverse matrix is used to dehide the message again. This inverse matrix we call it as encoding matrix.

$$\overline{A} = \begin{bmatrix} 0 & 1 & -1 \\ -1 & -2 & 5 \\ 1 & 1 & -3 \end{bmatrix}$$

Step 10: Multiply the encoding matrix with the message matrix we received the following matrix:

$$\overline{A}X = \begin{bmatrix} 4 & -13 & 4 & -6 & 9 & 15 \\ 9 & 67 & -23 & 45 & -53 & -38 \\ 1 & -38 & 21 & -22 & 39 & 30 \end{bmatrix}$$

Step-11: encoding matrix using mode 26

$$\overline{A}X = \begin{bmatrix} 4 & 13 & 4 & 20 & 9 & 15 \\ 9 & 15 & 3 & 19 & 1 & 14 \\ 1 & 14 & 21 & 4 & 13 & 4 \end{bmatrix}$$

Step-11: Change the numbers back into letters.

4	9	1	13	15	14	4	3	21	20	19	4	9	1	13	15	14	4
D	I	A	M	O	N	D	C	U	T	S	D	I	A	M	O	N	D

The message received by the receiver.

4. CONCLUSION

This method is the safest method for sending secret messages. No one can be tried to tract the message, since the password known by the sender and receiver and a mathematical knowledge is most the encode and decode the message that is the only demerit of this method. This demerit is also a merit and strength of this method.

REFERENCE

1. J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., Factorizations of $b^n \pm 1$, b=2, 3, 5, 6, 7, 10, 11, 12, up to High Powers, Amer. Math. Society, 1983.
2. D.D. Spencer, Computers in Number Theory, Computer Science Press, 1982.
3. L.E. Dickson, History of the Theory of Numbers, three volumes, Chelsea, 1952.
4. R.K. Guy, Unsolved Problems in Number Theory, springer – Verlag, 1982.
5. G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, 5th ed., Oxford University Press, 1979.
6. W.J. Leveque, Fundamentals of Number Theory, Addison – Wesley, 1977.
7. H. Rademacher, Lectures on Elementary Number Theory, Krieger, 1977.
8. K.H. Rosen, Elementary Number Theory and Its Applications, 3rd ed., Addison –wesley, 1993.
9. M.R. Schroeder, Number Theory in Science and communication, 2nd ed., springer-erlag, 1986.
10. D. Shanks, Solved and Unsolved Problems in Number Theory, 3rd ed., Chelsea Publ.Co., 1985.

Source of support: Nil, Conflict of interest: None Declared