SHORT COMMUNICATION REPORT

AN ALGORITHM FOR ENCRYPTING MESSAGES USING MATRIX INVERSION

*ADEWUMI, S. E. & GARBA, E. J. D

Department of Mathematics
University of Jos
Nigeria
*(Corresponding author)
adewumis@gmail.com
adewumisa@unijos.edu.ng

INTRODUCTION

Encryption is the process of transforming a plaintext to ciphertext with the sole aim of blocking intruders from having access to information being sent. Different encryption algorithms are gaining currency with cryptanalyst not relenting in devising new methods for breaking developed schemes. It is possible to transform a system of equation that is in the form of Ax=b into a form of $A^{-1}x=b$, a disguised form of Ax=b and still transmit them as if they are of the form Ax=b.

In our previous work (Adewumi & Garba 2003a, 2003b), we demonstrated how a plaintext is encrypted into equations in which an *n*-word plaintext is converted to an *n* x *n* (square) matrix that will lead to non-singular matrix. Singular matrix do not have inverse and therefore cannot be used to encrypmessages that need to be decrypted by solving the systems of equation to recover xi (the plaintext) by the receiver.

This work is aimed at reducing the incidence of people having access to information not belonging to them.

DEFINITIONS

(1) Given an n x n matrix A, if we can find a matrix B such that $AB=BA=I_n$, then B is a inverse of A.

(2) An n x n matrix A is said to be nonsingular if an n x n matrix A^{-1} exist with $AA^{-1} = A^{-1}A=I$. The matrix A^{-1} is called the inverse of A. That is $|A|\neq 0$. (O'Neil 1979)

THEOREMS

(1) For any nonsingular n x n matrix A:
  a. A^{-1} is unique
  b. A^{-1} is nonsingular and $(A^{-1})^{-1}=A$
  c. If B is also nonsingular n x n matrix, then $(AB)^{-1}=B^{-1}A^{-1}$ (Burden & Faires 1997)

(2) if A is nonsingular, then so is A^{-1}, and $(A^{-1})^{-!}=A$

  a. A^{-1} is unique
  b. A^{-1} is nonsingular and $(A^{-1})^{-1}=A$
  c. If B is also nonsingular n x n matrix, then $(AB)^{-1}=B^{-1}A^{-1}$ (Burden & Faires 1997)

MTRIX INVERSION ALGORITHM FOR ENCRYPTING MESSAGES

The system Ax=b can be transformed as follows:

a. Transform the message (plaintext) being sent into the form Ax=b using the method in (Adewumi & Garba 2003a, 2003b)

b. Obtain the matrix [A] from the equation Ax=b
c. Find A^{-1}
d. Send the encrypted message as

$A^{-1}x=b$. This will further disguise the message being transmitted.

DECRYPTION ALGORITHM

a. Obtain the matrix A^{-1} from $A^{-1}x=b$
b. Find $[A] = [A^{-1}]^{-1}$, recall from theorem (2) that $(A^{-1})^{-1}=A$
c. Transform the equation into Ax=b
d. Use the decryption algorithm described in (Adewumi & Garba 2003a, 2003b) for systems of linear equations to decrypt this message.

ALGORITHM FOR FINDING A^{-1}

a. Write an n x 2n matrix consisting of I_n placed on the left of A. The new matrix is denoted by $[I_n:A]$. The first n columns are called the left side, the second n columns, the right side. Example of $[I_n:A]$ is stated below:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & | & A_{11} & A_{12} & \cdots & A_{1n} \\ 0 & 1 & \cdots & 0 & | & A_{21} & A_{22} & \cdots & A_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \cdots & 1 & | & A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix}$$

b. Reduce A to A_R. Each elementary row operation performed on the right side is also performed on the left side. This results in an n x 2n $[C:A_n]$.

c. If $A_n \neq I_n$, then A is singular, and no inverse exists. If $A_R=I_n$, $A^{-1}=C$. (O'Neil 1979).

This algorithm works by beginning on the left side with I_n, and performing elementary row operations used to reduce A, we produce in C a matrix that performs the complete sequence of reducing operations when multiplied on the left of A. That is, whether or not $A_R=I_n$, the matrix C in the final form $[C: A_R]$ has the property that $CA = A_R$. When $A_R=I_n$, then C must be A^{-1}

EXAMPLE TO DEMONSTRATE THE USE OF MATRIX INVERSION TO ENCRYPT MESSAGES

This example demonstrates the use of matrix inversion to encrypt and decrypt messages.

ATTACK NOW can be encrypted as a 2 x 2 systems of equations thus:

A T T A C K
$(x_1+0)+(x_2+18)+(x_2+18)+(x_1+0)+(x_1+2)+(x_2+9)$

N O W
$(x_1+13)+(x_2+13)+(x_1+22)$

The derivation of the above variables x_1, x_2, x_3 and constants have been described and demonstrated in (Adewumi & Garba 2003).

If we use the delta coding to hide the various distances of each letter, and taking $x_1=1$, $x_2=2$, $x_3=3$; the word **ATTACK NOW** is transformed into the form Ax=b as:

$$\begin{aligned} 3x_1 + 3x_2 &= 9 \\ 2x_1 + \ x_2 &= 4 \end{aligned} \qquad \text{... (1)}$$

The matrix A = $\begin{pmatrix} 3 & 3 \\ 2 & 1 \end{pmatrix}$ ... (2)

We now find the A^{-1} by manipulating the augmented matrix

$$\begin{pmatrix} 1 & 0 & | 3 & 3 \\ 0 & 1 & | 2 & 1 \end{pmatrix}.$$

If we carry out row operations on this matrix, we obtain the

$$\begin{pmatrix} -1/3 & 1 \\ 2/3 & -1 \end{pmatrix}$$

Equation (1) is sent as

$$A^{-1} = \quad \begin{aligned} -1/3\, x_1 + x_2 &= 9 \\ 2/3\, x_1 + -x_2 &= 4 \end{aligned}$$

This is the same as sending $A^{-1}x = b$, but this to an intruder, will look like $Ax = b$.

To decrypt, we use the algorithm for finding the inverse of *A* after obtaining

$$A = (A^{-1})^{-1}.$$

Once the values of x_1 and x_2 have been obtained, we use delta coding algorithm described in (Adewumi & Garba 2003a, 2003b) to recover the position of the various letters used in the plaintext.

CONCLUSION

We have demonstrated in this paper that matrix inverse is a good scheme for solving most cryptographic problems that are prevalent in our society. This scheme can be used for example, in our institutions in encrypting question papers to prevent examination leakages even when they change hands between the examiners and those with the responsibility of administering them to students. It can also be implemented in banking to secure funds transfer; the military to secure military secrets, diplomatic mission to secure classified messages. It can found usage in any message transfer that must be secured against intruder's attack.

REFERENCES

Adewumi, S. E. & Garba E. J. D. 2003a. A cryptosystems algorithm using systems of non linear Equations. *Iranian Journal of Information Science and Technology* 1(1):43-55.

Adewumi, S. E. & Garba E. J. D. 2003b. Appraising your e-Business site using a search engine. *Proceeding of Nigerian Computer Society National conference.* 14:80-87.

Adewumi, S. E. & Garba E. J. D. 2003c. Securing Transborder Messages: An Encryption Standard for developing countries. *Proceeding of the Fourth Annual Global Information Technology Management World Conference.* June 8-10, 2003. Calgary, Alberta, Canada:84-87

Adewumi, S. E & Garba, E. J. D. 2002. Data Security: A Cryptostems Algorithm Using Systems of Non-Linear Equations. *Proceeding of Computer Association of Nigeria*, Volume 13:200-221

Burden, R. L. & Faires, J. D. 1997. *Numerical Analysis* PWS Publishing Company, Boston.

O'Neil P. V. 1979. *Introduction to Linear Algebra (Theory and applications)* Wadsworth Publishing Company, Inc. Beltmont, California.