Volume 3, Issue 4, April 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Encryption and Decryption Algorithm using 2-D Matrices

BALAJEE MARAM[1],
[1]*Asst. Prof., Dept. of Information Technology, GMRIT, RAJAM-532127, India.*

K LAKSHMANA RAO[2],
[2]*Asst. Prof., Dept. of Information Technology, GMRIT, RAJAM-532127, India.*

Y RAMESH KUMAR[3]
[3]*Asso. Prof., Dept. Of IT, Avanthi Inst. Of Technology, Vizianagaram, AP, INDIA.*

Abstract- Data Security is plays a vital role in Data Communication through Internet. Definitely there is a need to protect the data from unauthorized access. Data may exist in many forms like images, tables, Icons, Text, Video, Audio, Colours etc. Till now many methods or algorithms have been proposed in the world. Any way Cryptography plays an important role to encode and decode the Information. This paper also proposes a new method for encode and decode the data by using Shared-Secret-Key, Session-Key and Intermediate-Key and Matrix operations.

Keywords - Matrices, Matrix Operation, Encoder, Decoder, Message Matrix.

I. INTRODUCTION

Cryptography is a technique which allow human-being to encrypt the data in such a way that the decryption can be performed without the aid of sender. As the network technology has been greatly advanced, there is a need to send much information via the Internet. At the same time, the security issues are a crucial problem in the transmission process.

In this process, one shared-secret-key has been shared by the sender & receiver. When there is a need to send a message, one-time session-key will have been generated. Then all the characters will be shuffled based on mathematical techniques. Now all the characters will be arranged in different matrices. Again all the characters in all the matrices will be shuffled. Now the data will be encrypted using one-time session-key. Then the encrypted message and Intermediate-key will be transmitted to the Destination. When the cipher-text reaches the Destination, the session-key will be computed by using both one-time session-key and shared-secret-key. Then the message will be decrypted. The detailed explanation will come in next chapters.

II. EXISTING SYSTEMS

A. *HILL CIPHER method for Blocks*

Though Hill cipher's or linear block cipher is susceptible to cryptanalysis and unusable in practice, still serves an important pedagogical role in both cryptology and linear algebra. It is this role in linear algebra that raises several interesting questions [1]. In general, the key space of the Hill cipher is precisely GL(r, Zm) the group of r * r matrices that are invertible over Zm for a predetermined modulus m. We first present a formula for the order of this group. We then consider involuntary matrices, which eliminate the necessity of computing matrix inverses for Hill decryptions. Finally, we compare the total number of matrices with the number of invertible and involuntary matrices, identifying the effects of change in dimension and modulus on the order of the key space [1]. It is fundamentally equivalent and is consistent with modern texts in cryptography. A plaintext string over an alphabet of order m is rewritten as a vector over Zm using a natural correspondence. In either column major or row-major order, the vector is rewritten as a matrix P with d rows, where d is an arbitrarily chosen positive integer [1].

For a fixed n ϵ IN, the key space K is the set of all invertible n x n matrices in ZZ^{nxn}_{26} .P = C = ZZ^{n}_{26}. Messages m ϵ ZZ* that are longer than n are split into blocks of length n and are encrypted block-wise. All arithmetic operations are carried out modulo 26[1]. The Hill cipher is defined as follows:

For each K ϵ K, define the encryption function

EK : ZZ^{n}_{26} -> ZZ^{n}_{26} by[1]

EK (p) = K . p mod 26 ……(1)

Where "." denotes matrix multiplication modulo 26[1].

Letting K^{-1} denote the inverse matrix of K, the decryption function DK-1: ZZ^{n}_{26} -> ZZ^{n}_{26} is defined by

DK-1(c) = K^{-1} . c mod 26[1] ……...(2)

Since K-1 can easily be computed from K, the Hill cipher is a symmetric cryptosystem. It is also the most general linear block cipher. Affine linear block ciphers are easy to break by known-plain-text attacks. That is, for an attacker who knows some sample plain texts with the corresponding encryptions, it is not too hard to find the key used to encrypt these plain texts [1].

B. *HILL CIPHER for Visual Cryptography*

Hill cipher, developed by the mathematician Lester Hill in 1929, lies in the manipulation of matrix. For encryption, algorithm takes m successive plain text letters and substitutes m cipher letters. In Hill cipher, each character is assigned a numerical value like α=0, β=1 …… ζ=25[3]. The substitution of cipher text letters leads to „m" linear equation. This can be expressed ασX=KΠ, ωηερε C and P are column vectors, representing the plain text and cipher text respectively, and K is the encryption key matrix. All these operations are performed with modulo 26. Decryption requires using the inverse of the matrix K. The inverse matrix K^{-1} of a matrix K is defined by the equation $KK^{-1}=k^{-1}K=I$, where I is the Identity matrix. But the inverse of the matrix does not always exist, and when it does, it satisfies the preceding equation. is K^{-1} applied to the cipher text, and then the plaintext is recovered. In general term, this is written as follows:

For encryption:

$C=E_K(P)=K_P$

For Decryption:

$P=D_K(C)=K^{-1}C=K^{-1}K_P=P$

C. The Double-Reflecting Data Perturbation Method

The Double-Reflecting Data Perturbation Method [4] denoted by DRDP reverberates the original data by x-axis and y-axis to achieve the perturbed data for some confidential attribute. In this method, the randomization function plays a very crucial rule, and if the function is not properly chosen it May degrade the clustering quality. The distortion operation performed to the confidential attribute is given by

$op_j = \rho_{Aj} + (\rho_{Aj - aj) = 2} \rho_{Aj - aj.}$

Where Aj ($1 \leq j \leq n$) is a confidential attribute and a j ($1 \leq j \leq n$) is an instance of Aj. ρ_{Aj} is defined by the following formula

$\rho_{Aj} = |(\max Aj + \min Aj)/2|$

Where max Aj and min Aj are respectively the maximum value and minimum value of attribute Aj. The 'student' relational database before and after applying DRDP is shown in the following Table:

S.No	RollNo	Name	Marks	Distored Marks
1	101	Raj	78	92
2	102	Ravi	89	81
3	103	Rohan	92	78
4	104	Rani	82	88
5	105	Rahul	80	90

III. PROPOSED SYSTEMS

A. Algorithm for Encryption

Steps:

1) There is a need to share one secret-key is called "Shared-Secret-Key". This is permanent key between the Sender and Receiver. Its length is 16-byte.
2) A one-time key has been generated is called "Session-Key". This is temporary key is valid for specific session only. Its length is 16-byte.
3) Now an Intermediate-Key will be generated based on both Shared-Secret-Key and Session-Key in the following way:

$$\begin{pmatrix} sk_{11} & sk_{12} & sk_{13} & sk_{14} \\ sk_{21} & sk_{22} & sk_{23} & sk_{24} \\ sk_{31} & sk_{32} & sk_{33} & sk_{34} \\ sk_{41} & sk_{42} & sk_{43} & sk_{44} \end{pmatrix} \text{ is XORed with}$$

$$\begin{pmatrix} s_{11} & s_{12} & s_{13} & s_{14} \\ s_{21} & s_{22} & s_{23} & s_{24} \\ s_{31} & s_{32} & s_{33} & s_{34} \\ s_{41} & s_{42} & s_{43} & s_{44} \\ i_{41} & i_{42} & i_{43} & i_{44} \end{pmatrix} = \begin{pmatrix} i_{11} & i_{12} & i_{13} & i_{14} \\ i_{21} & i_{22} & i_{23} & i_{24} \\ i_{31} & i_{32} & i_{33} & i_{34} \end{pmatrix}$$

Here $t_{11}=sk_{11}$ XOR s_{11} , $t_{12}=sk_{12}$ XOR s_{12} ….. so on.

. Its length is also 16-byte only. Here sk stands for Shared-Secret-Key, s stands for Session-Key and i stands for Intermediate-Key.

4) All the characters in each sentence will be shuffled according to Double-reflecting Data-Perturbation method. Here Delimiter is '. (dot)'.
5) All characters will arranged in 4X4 matrices (except last characters i.e. Total Number of Characters % 16).
6) All matrices will be transposed.
7) All 4 characters in each row in every matrix will be shuffled according to Double-reflecting-data-perturbation method.
8) Now the characters in 1st row, 2nd row, 3rd row and 4th row in 1st matrix will be arranged as a paragraph. Then from 2nd matrix and so on.
9) The first 16 characters are XORed with one-time Session-Key.
10) Next 16 characters are XORed by Intermediate-Key, and so on.
11) Now the Intermediate-Key is appended to cipher-text and transmitted to the destination

B. *Algorithm for Decryption*

Steps:

1) After receiving the cipher-text, the receiver simply extract last 16 characters, is nothing but Intermediate key.
2) The receiver calculates the Session-Key using Intermediate-Key and Shared-Secret-Key in the following way: $s_{11}=sk_{11}$ XOR $i_{11,}$ $s_{12}=sk_{12}$ XOR $i_{12,}$ …….. So on.
3) The first 16 characters are XORed with one-time Session-Key.
4) Next 16 characters are XORed by Intermediate-Key, and so on.
5) All characters will arranged in 4X4 matrices (except last characters i.e. Total Number of Characters % 16).
6) All 4 characters in each row in every matrix will be reshuffled according to Double-reflecting-data-perturbation method.
7) All matrices will be transposed.
8) Now all the characters in each row in each matrix including left-over characters are arranged as a paragraph.
9) All the characters in each row (dot is delimiter for each row) will be reshuffled according to Double-reflecting-Data-Perturbation method.
10) Then the original text will have been generated.
11)

IV. ILLUSTRATION

A. ENCRYPTION

1) Shared-Secret-Key:3Venee is G00d..
2) One-time Session-Key:Nature Kals me..
3) Intermediate-Key:}7"L4]
4) Input Text: My name is BALAJEE MARAM. I am working as an Assistant Professor in GMRIT. It is well known engineering college in Coastal Andhra.
5) Total No. of Characters: 130
6) Decimal format of the Input Text: 77 121 32 110 97 109 101 32 105 115 32 66 65 76 65 74 69 69 32 77 65 82 65 77 46 32 73 32 97 109 32 119 111 114 107 105 110 103 32 97 115 32 97 110 32 65 115 115 105 115 116 97 110 116 32 80 114 111 102 101 115 115 111 114 32 105 110 32 71 77 82 73 84 46 32 73 116 32 105 115 32 119 101 108 108 32 107 110 111 119 110 32 101 110 103 105 110 101 101 114 105 110 103 32 99 111 108 108 101 103 101 32 105 110 32 67 111 97 115 116 97 108 32 65 110 100 104 114 97 46
7) Now all the characters (Except.) in each sentence have been shuffled according to Double reflecting data perturbation method.
8) After shuffling the characters in the first sentence is like the following:

L y+8,4Y0&yWXMXOTTyLXGXL. In this way, all the characters in each sentence will be shuffled according to Double reflecting data perturbation method.

9) All characters will arranged in 4X4 matrices (except last characters i.e. Total Number of Characters % 16).
10) All matrices will be transposed.
11) All 4 characters in each row in every matrix will be shuffled according to Double-reflecting-data-perturbation method.
12) Now the characters in 1st row, 2nd row, 3rd row and 4th row in 1st matrix will be arranged as a paragraph. Then from 2nd matrix and so on.
13) Now the first 16 characters are "<PX0MAG 4y4Uy+MU"
14) The first 16 characters are XORed with one-time Session-Key. So the first 16 characters are converted like the following: "r1,E?$gkU G u Ec{".
15) Next 16 characters are XORed by Intermediate-Key, and so on.
16) Now the Intermediate-Key is appended to cipher-text and transmitted to the destination.

B. DECRYPTION

1) After receiving the cipher-text, the receiver extracts the last 16-bytes (Intermediate-Key)
2) Now the receiver can calculate the Session-Key by using Shared-Secret-Key and Intermediate-Key.
3) The first 16 characters are XORed with one-time Session-Key. So the first 16 characters are converted like the following: "r1,E?$gkU G u Ec{".
4) Next 16 characters are XORed by Intermediate-Key, and so on.
5) All characters will arranged in 4X4 matrices (except last characters i.e. Total Number of Characters % 16).
6) All 4 characters in each row in every matrix will be shuffled according to Double-reflecting-data-perturbation method.
7) All matrices will be transposed.
8) Now all the characters in each row in each matrix including left-over characters are arranged as a paragraph.
9) All the characters in each row (dot is delimiter for each row) will be reshuffled according to Double-reflecting-Data-Perturbation method.

V. ADVANTAGES IN PROPOSED SYSTEM

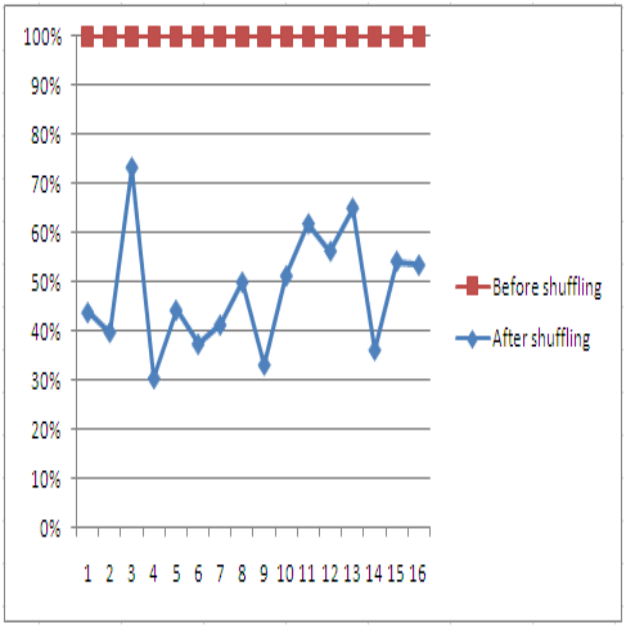
1) For even sentences, the Session-Key is applicable and for odd sentences, the Intermediate-Key is applicable. So two consecutive sentences will be encrypted differently.
2) No need to send both the keys i.e. Session-Key and Intermediate-Key.

VI. SECURITY LEVEL

In 1st phase of proposed method, all the characters in the sentence are converted into ASCII. Now those characters are shuffled according to their ASCII value based on Double Reflecting Data Perturbation Method. The privacy of data is measured by the variance between the actual and the perturbed values which is given by the following formula

$$A = \frac{\text{VAR}\,(A - A')}{\text{VAR}\,(A)}$$

It has been analyzed that the privacy or the security level of the confidential data is improved a lot by the proposed method for Encryption and Decryption. The Security level of the Double Reflecting Data Perturbation Method for 1st sentence "My name is BALAJEE MARAM" is shown the following chart.



After observing this Chart, easily we can identify no similarities between Character (before shuffling) and Character (after shuffling). So it is a good significance in Cryptography.

VII. CONCLUSION

As of now, many algorithms and technologies have been proposed by many researchers in the world. But till today, it is very difficult to provide security to the information which is being passed through Internet. So this proposed paper tries

to give one more new algorithm for Information Security. It is a Symmetric Encryption only. In near future, this will be extended to Public-Cloud.

ACKNOWLEDGEMENT

I am very thankful to all the authors and owners of websites which I mentioned in REFERENCES and BIBLIOGRAPHY section. Here I want to contribute and share my knowledge with rest of the world. Financially I am not expecting anything. So any Researcher want to use this content, please include that content which included in this paper. Thank you for Chief-Editor and Reviewers.

If any Researcher wants to include this paper, please use the following citation:

Balajee Maram, Lakshmana Rao K, Ramesh Kumar Y, 2013, "Encryption and Decryption Algorithm using 2-D Matrices", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol 3- Issue 4, April-2013.

REFERENCES

[1] John C. Bowman, Math 422 Coding Theory & Cryptography, University of Alberta, Edmonton, Canada
[2] http://aix1.uottawa.ca/~jkhoury/cryptography.htm
[3] Stallings. W, "Cryptography and Network Security", 4th edition, Prentice Hall, 2005
[4] A. Viji Amutha Mary, Dr. T. Jebarajan, A Novel Data Perturbation Technique with higher Security, IJCET, Vol:3, Issue:2, pp:126-132,2012
[5] http://aix1.uottawa.ca/~jkhoury/cryptography.htm)
[6] Maram Balajee, Challa Narasimham, "Double-reflecting Data Perturbation Method for Information Security", ISSN: 0974-6471 December 2012, Vol. 5, No. (2):Pgs. 283-288

