Network Security Enabled Text Encryption Using Matrices

K.Sri Harsha, J.Yasaswi, M.Viswanath Prateek

Abstract - Most companies offering facilities to access host computers by their employees even from outside the organization. Network security involves all those activities which protect the information on the host computers/servers. Security of information has become a popular subject during the last decades. Since matrices have unique powerful concept, and can be easily understood, it could be applied as an efficient way of encrypting and storing text. This paper introduces a way of using positions of text represented in matrices for cryptography. The encryption system uses a matrix to store the text entered by the sender in the form of their positions, using an algorithm to encrypt these values.

Keywords - Matrices, Encryption, Decryption.

1 INTRODUCTION

With the rapid development of network and multimedia technologies, the digital information has been applied to many areas in real-world applications. Communication has become a very important aspect in today's life. So, security plays an important role in transferring the data. One such way to secure information is cryptography. In cryptography we hide the information from unauthorized users by employing various techniques; encryption is one such technique where we transform the data into a form understandable only by the authorized users. We need to hide the data for privacy purpose and for ensuring data received at the authenticated user end is not modified .We have several encryption and decryption algorithms for encrypting the data at sender end and decrypting the same at receiver side ensuring secure data transfer.

An encryption algorithm is used to convert plaintext (P) into cipher text (C). This requires encryption (E) and decryption (D) functions, such that

$$E(P) = C, D(C) = P$$

Encryption algorithms are idempotent. Each encryption creates cipher text that can be decrypted into plaintext. Repeated encryptions may generate different cipher text, but the original plaintext can always be recovered by using the decryption algorithm the number of times the encryption algorithm has been used.

2. NETWORK SECURITY

Security is concerned with making sure that nosy people cannot read, or worse yet, secretly modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, non-repudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when people think about network security. Authentication deals with determining whom you are talking to before revealing sensitive. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Non-repudiation deals with signatures.

2.1 SECRECY

Contents of the transmitted message should be understood only by the sender and the intended receiver. Because eavesdroppers may intercept the message, this necessarily requires that the message be somehow encrypted (disguise data) so that an intercepted message cannot be decrypted (understood) by an interceptor. This aspect of secrecy is probably the most commonly perceived meaning of the term "secure communication." However, this is a restricted definition of secure communication and secrecy as well.

2.2 AUTHENTICATION

The authentication service is concerned with assuring that a communication is authentic in the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from source that it claims to be from. In the case of an ongoing interaction such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered within such a way that a third party can masquerade as one of the two legitimate parties for the purposes of the unauthorized transmission or reception.

2.3 INTEGRITY

Even if the sender and receiver are able to authenticate each other, they also want to insure that the content of their communication is not altered, either maliciously or by accident, in transmission. Extensions to the check summing techniques that we encountered in reliable transport and data link protocols. An integrity service can be applied with or without recovery. As these services are related to active attacks, the major concern is to detect them rather than preventing them. If the integrity is violated and detected, then the service must simply notify its violation and find out the ways of recovering from it.

2.4 NON-REPUDIATION

This provides protection against the denying by one of the entities involved in communication. Thus, once a message is sent, the receiver assures that the message was sent by an intended sender and upon reception; the sender assures that the message is received by the correct receiver.

3. PROPOSED CRYPTOSYSTEM

3.1 INPUT OF STRING

We consider any text S to be encrypted. Let the length of the text be n (including blank spaces). Each symbol (either an alphabet or blank space) in the text is assigned a numerical label ranging from 1 – k (excluding those numbers including 0 like 20, 30,…, 100, 101,…), k n. We allow 10 alone since after encryption an entry 100 will mean that 10 is the index value , the second 0 represents the meaning of the definition as defined in 2 below (will be used to differentiate the entry value of two alphabets). Consider a 26 x 26 matrix A. The rows and columns of this matrix represent the alphabets from A – Z.

We now construct a diagonal matrix A as follows.

1. Choose the first symbol in the first word. Suppose it represents alphabet i, then the label value of the first symbol is entered in position a_{ii}.

2. Consider the second symbol in the first word. Suppose it represents alphabet j, then

$$a_{ij} = \begin{cases} \text{label value of alphabet j of first word} & \text{if } i \neq j \\ \text{<0>label value of alphabet j of first word} & \text{if } i = j \end{cases}$$

   that is a zero between two integer values in any entry for a_{ii}, i = 1, 2,…,26 represents the label value of two alphabets, that is 0 is used to differentiate the entry value of two alphabets. For example 10230123 means that the label of three different alphabets are 1, 23, 123 respectively.

3. We continue this procedure for each symbol in the first word.

We now will encounter a blank space. The label for the blank space will not be used anywhere in the matrix. Missing labels in the matrix represent blank spaces.

4. We continue this procedure for all the remaining words

We now choose any key matrix B, determine the matrix product AB and transmit it to the receiver as a two dimensional array.

Encryption of text

1. We take the text S that is to be encrypted from the user.
2. Determine A as described.
3. Input any random values in matrix excluding the diagonal values which are obtained.
4. Let C = AB where B is the key matrix.
5. Send C to the receiver as a two dimensional array.

Decryption of text

1. $A = C B^{-1}$
2. The random values can be ignored and diagonal values are to be considered.
3. Generate the text from matrix A.

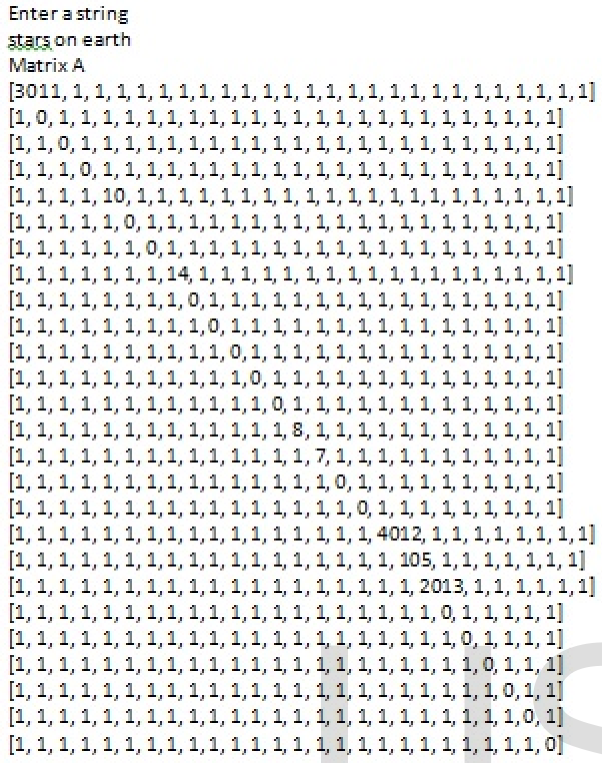
We have also done a program for the proposed algorithm. This algorithm encrypts the message and if the encrypted message is obtained, then the program decrypts the message and provides the output of the original message.

4. EXAMPLE

Suppose we like to encrypt the message “stars on earth”. By assigning numerical values to this message we obtain the sequence as 123456789111213. When this message is encrypted we obtain the following output matrix 1.

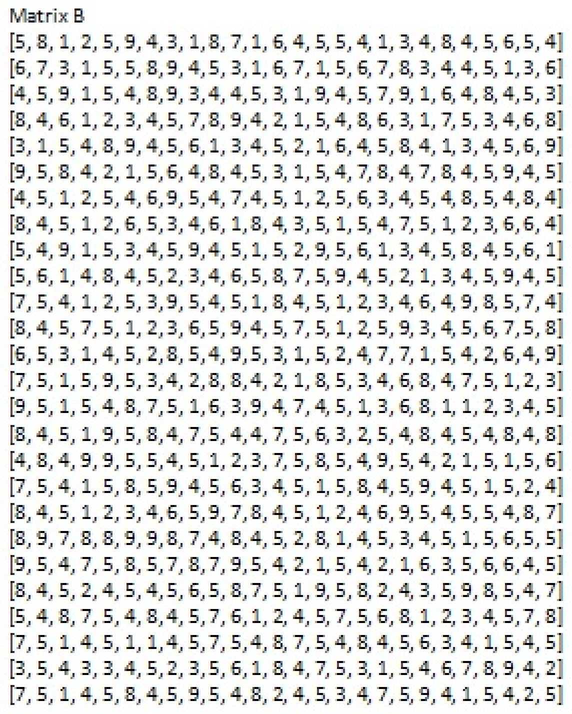
It can be noted that 6 and 9 represents a blank space and it is nowhere seen along the diagonal in the matrix. Also A is repeated three times, in the three different words. So the first row first column entry 306011 represents the different occurrence of A. It can be noted that 3, 6, 11 are separated by 0 in between them, so that the index value of the alphabets is encrypted proper.

ISSN 2229-5518



```
Enter a string
stars on earth
Matrix A
[3011, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 10, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 14, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 8, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 7, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 4012, 1, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 105, 1, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2013, 1, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1]
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0]
```

This can be multiplied by any matrix of our choice. We shall choose the following matrix B seen in matrix 2, to generate the product matrix AB as shown in matrix 3.



```
Matrix B
[5, 8, 1, 2, 5, 9, 4, 3, 1, 8, 7, 1, 6, 4, 5, 5, 4, 1, 3, 4, 8, 4, 5, 6, 5, 4]
[6, 7, 3, 1, 5, 5, 8, 9, 4, 5, 3, 1, 6, 7, 1, 5, 6, 7, 8, 3, 4, 4, 5, 1, 3, 6]
[4, 5, 9, 1, 5, 4, 8, 9, 3, 4, 4, 5, 3, 1, 9, 4, 5, 7, 9, 1, 6, 4, 8, 4, 5, 3]
[8, 4, 6, 1, 2, 3, 4, 5, 7, 8, 9, 4, 2, 1, 5, 4, 8, 6, 3, 1, 7, 5, 3, 4, 6, 8]
[3, 1, 5, 4, 8, 9, 4, 5, 6, 1, 3, 4, 5, 2, 1, 6, 4, 5, 8, 4, 1, 3, 4, 5, 6, 9]
[9, 5, 8, 4, 2, 1, 5, 6, 4, 8, 4, 5, 3, 1, 5, 4, 7, 8, 4, 7, 8, 4, 5, 9, 4, 5]
[4, 5, 1, 2, 5, 4, 6, 9, 5, 4, 7, 4, 5, 1, 2, 5, 6, 3, 4, 5, 4, 8, 5, 4, 8, 4]
[8, 4, 5, 1, 2, 6, 5, 3, 4, 6, 1, 8, 4, 3, 5, 1, 5, 4, 7, 5, 1, 2, 3, 6, 6, 4]
[5, 4, 9, 1, 5, 3, 4, 5, 9, 4, 5, 1, 5, 2, 9, 5, 6, 1, 3, 4, 5, 8, 4, 5, 6, 1]
[5, 6, 1, 4, 8, 4, 5, 2, 3, 4, 6, 5, 8, 7, 5, 9, 4, 5, 2, 1, 3, 4, 5, 9, 4, 5]
[7, 5, 4, 1, 2, 5, 3, 9, 5, 4, 5, 1, 8, 4, 5, 1, 2, 3, 4, 6, 4, 9, 8, 5, 7, 4]
[8, 4, 5, 7, 5, 1, 2, 3, 6, 5, 9, 4, 5, 7, 5, 1, 2, 5, 9, 3, 4, 5, 6, 7, 5, 8]
[6, 5, 3, 1, 4, 5, 2, 8, 5, 4, 9, 5, 3, 1, 5, 2, 4, 7, 7, 1, 5, 4, 2, 6, 4, 9]
[7, 5, 1, 5, 9, 5, 3, 4, 2, 8, 8, 4, 2, 1, 8, 5, 3, 4, 6, 8, 4, 7, 5, 1, 2, 3]
[9, 5, 1, 5, 4, 8, 7, 5, 1, 6, 3, 9, 4, 7, 4, 5, 1, 3, 6, 8, 1, 1, 2, 3, 4, 5]
[8, 4, 5, 1, 9, 5, 8, 4, 7, 5, 4, 4, 7, 5, 6, 3, 2, 5, 4, 8, 4, 5, 4, 8, 4, 8]
[4, 8, 4, 9, 9, 5, 5, 4, 5, 1, 2, 3, 7, 5, 8, 5, 4, 9, 5, 4, 2, 1, 5, 1, 5, 6]
[7, 5, 4, 1, 5, 8, 5, 9, 4, 5, 6, 3, 4, 5, 1, 5, 8, 4, 5, 9, 4, 5, 1, 5, 2, 4]
[8, 4, 5, 1, 2, 3, 4, 6, 5, 9, 7, 8, 4, 5, 1, 2, 4, 6, 9, 5, 4, 5, 5, 4, 8, 7]
[8, 9, 7, 8, 8, 9, 9, 8, 7, 4, 8, 4, 5, 2, 8, 1, 4, 5, 3, 4, 5, 1, 5, 6, 5, 5]
[9, 5, 4, 7, 5, 8, 5, 7, 8, 7, 9, 5, 4, 2, 1, 5, 4, 2, 1, 6, 3, 5, 6, 6, 4, 5]
[8, 4, 5, 2, 4, 5, 4, 5, 6, 5, 8, 7, 5, 1, 9, 5, 8, 2, 4, 3, 5, 9, 8, 5, 4, 7]
[5, 4, 8, 7, 5, 4, 8, 4, 5, 7, 6, 1, 2, 4, 5, 7, 5, 6, 8, 1, 2, 3, 4, 5, 7, 8]
[7, 5, 1, 4, 5, 1, 1, 4, 5, 7, 5, 4, 8, 7, 5, 4, 8, 4, 5, 6, 3, 4, 1, 5, 4, 5]
[3, 5, 4, 3, 3, 4, 5, 2, 3, 5, 6, 1, 8, 4, 7, 5, 3, 1, 5, 4, 6, 7, 8, 9, 4, 2]
[7, 5, 1, 4, 5, 8, 4, 5, 9, 5, 4, 8, 2, 4, 5, 3, 4, 7, 5, 9, 4, 1, 5, 4, 2, 5]
```

The two dimensional array AB will be send to the receiver.

C=AB
[15218, 24211, 3120, 6107, 15181, 27222, 12168, 9173, 3139, 24219, 21218, 3119, 18185, 12133, 15180, 15157, 12161, 3130, 9167, 12160, 24187, 12158, 15172, 18193, 15174, 12176]
[162, 124, 107, 86, 126, 127, 120, 134, 125, 134, 145, 108, 119, 86, 129, 102, 115, 113, 129, 117, 103, 114, 117, 132, 121, 130]
[164, 126, 101, 86, 126, 128, 120, 134, 126, 135, 144, 104, 122, 92, 121, 103, 116, 113, 128, 119, 101, 114, 114, 129, 119, 133]
[160, 127, 104, 86, 129, 129, 124, 138, 122, 131, 139, 105, 123, 92, 125, 103, 113, 114, 134, 119, 100, 113, 119, 129, 118, 128]
[195, 140, 155, 123, 203, 213, 164, 188, 183, 148, 175, 145, 170, 111, 139, 161, 157, 165, 209, 156, 116, 145, 158, 178, 178, 217]
[159, 126, 102, 83, 129, 131, 123, 137, 125, 131, 144, 104, 122, 92, 125, 103, 114, 112, 133, 113, 99, 114, 117, 124, 120, 131]
[164, 126, 109, 85, 126, 128, 122, 134, 124, 135, 141, 105, 120, 92, 128, 102, 115, 117, 133, 115, 103, 110, 117, 129, 116, 132]
[272, 183, 175, 100, 157, 210, 193, 182, 181, 217, 161, 213, 177, 132, 195, 120, 186, 172, 228, 185, 120, 144, 161, 211, 202, 188]
[163, 127, 101, 86, 126, 129, 124, 138, 120, 135, 143, 108, 120, 91, 121, 102, 115, 119, 134, 116, 102, 110, 118, 128, 118, 135]
[163, 125, 109, 83, 123, 128, 123, 141, 126, 135, 142, 104, 117, 86, 125, 98, 117, 115, 135, 119, 104, 114, 117, 124, 120, 131]
[161, 126, 106, 86, 129, 127, 125, 134, 124, 135, 143, 108, 117, 89, 125, 106, 119, 117, 133, 114, 103, 109, 114, 128, 117, 132]
[160, 127, 105, 80, 126, 131, 126, 140, 123, 134, 139, 105, 120, 86, 125, 106, 119, 115, 128, 117, 103, 113, 116, 126, 119, 128]
[162, 126, 107, 86, 127, 127, 126, 135, 124, 135, 139, 104, 122, 92, 125, 105, 117, 113, 130, 119, 102, 114, 120, 127, 120, 127]
[217, 166, 117, 122, 194, 167, 149, 171, 143, 195, 204, 137, 139, 100, 186, 142, 142, 148, 179, 176, 135, 167, 157, 140, 138, 157]
[222, 161, 116, 117, 155, 180, 170, 173, 135, 175, 166, 163, 149, 135, 154, 137, 127, 138, 173, 168, 113, 124, 134, 151, 148, 166]
[160, 127, 105, 86, 122, 127, 120, 139, 122, 134, 144, 105, 118, 88, 124, 104, 119, 115, 133, 112, 103, 113, 118, 125, 120, 128]

```
[164, 123, 106, 78, 122, 127, 123, 139, 124, 138, 146, 106, 118, 88, 122,
102, 117, 111, 132, 116, 105, 117, 117, 132, 119, 130]
[28245, 20186, 16154, 4098, 20186, 32220, 20183, 36242, 16173, 20194,
24214, 12142, 16169, 20148, 4141, 20162, 32209, 16164, 20192, 36219,
16151, 20173, 4133, 20188, 8146, 16180]
[1000, 547, 630, 191, 339, 444, 544, 767, 649, 1075, 876, 941, 541, 613,
234, 315, 537, 744, 1073, 640, 523, 638, 642, 549, 956, 864]
[16264, 18239, 14194, 16183, 16227, 18240, 18236, 16239, 14213, 8187,
16244, 8157, 10185, 4117, 16226, 2119, 8169, 10180, 6173, 8168, 10167,
2130, 10182, 12205, 10184, 10196]
[159, 126, 106, 80, 126, 124, 123, 136, 121, 132, 139, 104, 121, 91, 129,
102, 117, 118, 136, 114, 104, 113, 116, 127, 120, 131]
[160, 127, 105, 85, 127, 127, 124, 138, 123, 134, 140, 102, 120, 92, 121,
102, 113, 118, 133, 117, 102, 109, 114, 128, 120, 129]
[163, 127, 102, 80, 126, 128, 120, 139, 124, 132, 142, 108, 123, 89, 125,
100, 116, 114, 129, 119, 105, 115, 118, 128, 117, 128]
[161, 126, 109, 83, 126, 131, 127, 139, 124, 132, 143, 105, 117, 86, 125,
103, 113, 116, 132, 114, 104, 114, 121, 128, 120, 131]
[165, 126, 106, 84, 128, 128, 123, 141, 126, 134, 142, 108, 117, 89, 123,
102, 118, 119, 132, 116, 101, 111, 114, 124, 120, 134]
[161, 126, 109, 83, 126, 124, 124, 138, 120, 134, 144, 101, 123, 89, 125,
104, 117, 113, 132, 111, 103, 117, 117, 129, 122, 135]
```

5. CONCLUSION

The use of this proposed algorithm has been studied thoroughly and examined. This paper presents protection of data using text encryption method based on simple matrix operations like multiplication and inverse. Experiment results have shown that the proposed encryption system is reasonably feasible and effective and it can be extensively used for the purpose of secure data storage and transmission.

Matrices are well known tool for storage of huge data. The proposed scheme is powerful, since it can be used to encrypt a message of any length using always a matrix of size 26 x 26, that is for any text of any size, the size of the input and output matrix remains the same. We have used basic matrix properties and matrix multiplication for communicating any message. So manipulations involved in sending any message is simple, but it is strong since until one knows the key matrix, determining A is not possible. Even if one obtains A, still it is not possible to know the message unless the way in which the matrix was constructed is known.

So the proposed encryption scheme is a simple but powerful and efficient one.

6. REFERENCES

[1] http://en.wikipedia.org/wiki/Cryptography
[2] https://docs.python.org/2/
[3]Modern cryptography : Theory and practice Mao, Pearson Education.
[4]Network Security : Private communication in a public world, 2/e. Kaufman,
Perlman &Speciner.PHI.