DEVELOPING DSA TECHNIQUE BASED APPLICATION USING SQUARE GRID TRANSPOSITION

Praveen Kumar Patel, Anurag Tiwari, Dr. Manuj Darbari

Abstract— Data encryption is the conversion of data into a form, called cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form. In literature, different techniques are used for encryption and decryption of text, image, audio and video. In this work text files have been used for encryption and decryption in a grid size of 32X32 by using DSA (Digital Signature Algorithm) encryption algorithm. In this paper work a modified approach for encryption of text is used with popular DSA encryption algorithm. In this work, the binary data of a file is divided into equal sized blocks called grids. The bit streams of each grid are taken and grid transposition technique is applied over it. A key of 160 bits is used by the DSA algorithm for the grid size 32X32. The key is wrapped up with public key DSA algorithm for secret key transposition so that intruder cannot identify it. For decryption, the reverse grid transposition and private key is applied in this work. The included session key is obtained by decrypting the wrapped key with receiver's private key. The efficiency of the work with DSA algorithm is also compared with the reported work with RSA. In this paper work, a modified approach for the encryption of the text is used called the DSA (Digital Signature Algorithm) encryption algorithm. The binary data of file is divided into equal sized blocks called as grids.

Index Terms— Cryptography, Encryption, Grid Transposition, Decryption, RSA, DSA.

— — — — — — — — — — ◆ — — — — — — — — — —

1 INTRODUCTION

Encryption as provided in is a process of converting messages, information, or data into a form unreadable by anyone except the intended recipient [3,4].

Encrypted data must be deciphered, or decrypted, before it can be read by the recipient.

The root of the word encryption…

crypt—comes from the Greek word kryptos, meaning hidden or secret [2,6,7]. In its earliest form, people have been attempting to conceal certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures, this paper work highlights in chronology the history of Cryptography throughout centuries. For different reason, humans have been interested in protecting their messages. Threats to computer and network security[1,2] increase with each passing day and come from a growing number of sources. No computer or network is immune from attack. A recent concern is the susceptibility of the power grid and other national infrastructure to a systematic, organized attack on the United States from other nations or terrorist organizations[12,13,16].

Encryption, or the ability to store and transmit information in a form that is unreadable to anyone other than intended persons, is a critical element of our defense to these attacks[10,11,16]. Indeed, man has spent thousands of years in the quest for strong encryption algorithms.

II. METHODOLOGY

Step 1:A square grid of required size constructed by taking binary data from source file.

Step 2: Now grid transposition applied by reading data diagonally and writing it down on row basis from left to right.

Step 3:A secret key that varies with each session as combination of 0's and 1's is generated based on the grid size, say 160 – bit for 32– sized, 384 – bit for 64 – sized etc.

Step 4:A new grid generated after transposition.

Step 5: The new grid is converted into ASCII sequence and written to another file called encrypted file.

Step 6: Steps 1 to 5 are repeated until the total file is formed into grids and encrypted.Padding with 0's is done in grid formation deficiency.

Step 7: Key generated for each file is encrypted with the public key of sender using DSA algorithm.

Step 8: The encrypted key is then divided into various blocks and appended to file.

The above steps can be shown as the operational structure of the technique which includes the source file and then the implementation of the technique.

The operational structure of the technique is shown below:

The figure below shows all the steps in sequence.

Initially, Plaintext is given as input in the form of .txt file and then the file is encrypted and decrypted using

- *Praveen Kumar Patel is currently pursuing masters degree program in Computer Science in Babu Banarasi Das University, India PH-9935766184 E-mail: Praveenpatelsiet@gmail.com*
- *Anurag Tiwari is currently pursuing masters degree program in Computer Science in Babu Banarasi Das University, India PH-9935766184 E-mail: E-mail: anuragrktiwari@gmail.com*
- *Dr. Manuj Darbari is currently working as Assit. Prof in department of Information technology Babu Banarasi Das University ,lucknow*

public key algorithm called DSA and ultimately the same .txt file is regenerated using the decryption algorithm.

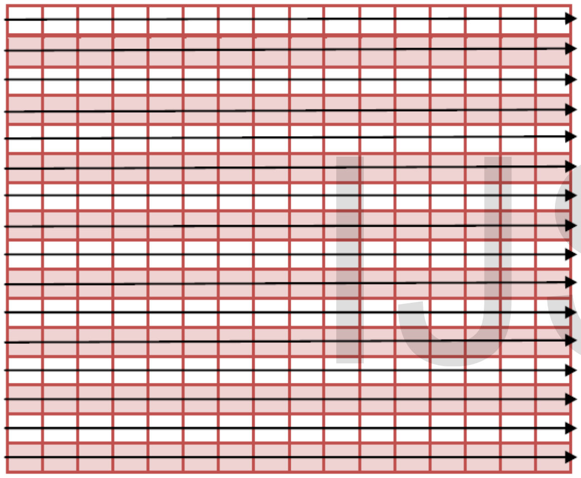
MODULES

1)Grid Reading
2)Grid Writing
3)Encryption
4)Decryption

1. GRID READING

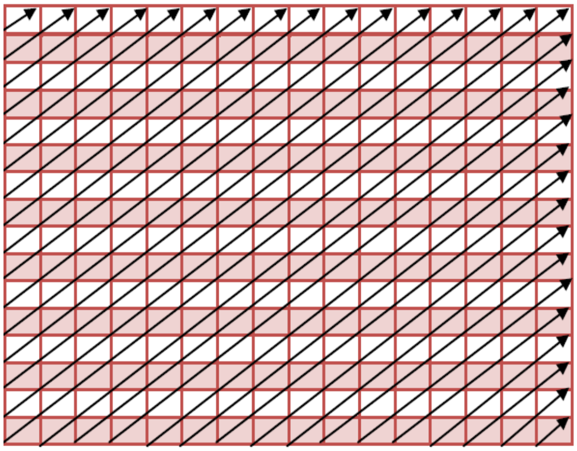
Grid Reading is nothing but it is the generation of combination of ASCII values of the plaintext in a grid size of 32X32.

It means that we take the plaintext and get the 8- bit ASCII values of each character in the plaintext and fill the grid of size 32



2 GRID WRITING

The data read as above format is written into a new equal sized grid starting from the left to right row by row. Grid Writing is performed only after grid reading have done.This is as follows:



3. ENCRYPTION

Data encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people[8,9,17].

Encryption is done by using public key algorithm called DSA with the use of private key of the sender and the plaintext to be encrypted.

During Encryption process the key of required size is generated.

DSA Key Generation

1.choose a prime p,between 512 and 1024 bits in length.The number bits in p must be a multiple of 64.

2.Choose a 160 bit prime q in such a way that q divides (p-1).

3.create e_1 to be the q^{th} root of 1 modulo p (e_1^p =1 mod p).choose a element e_0 and calculate $e_1=e_0^{(p-1)/q}$ mod p.

4. choose d as private key and calculate $e_2=e_1^d$ mod p.

5.public key is (e_1,e_2,p,q); private key is (d).

M:Message r;Random Secret h(M):Message Digest

S_1,S_2: Signature d: private key V:Verification

(e_1,e_2,p,q): Public key

DSA Signature Creation

1.Choose a random number r (1<=r<=q).

2.Calculate signature S_1 =(e_1^r mod p)mod q.

3. Create a digest of message h(M).

4. calculate signature S_2 =(h(M)+d S_1)r^{-1}mod q.

5.Send M, S_1 and S_2

DSA Signature Verification

1.Check to see if 0< S_1<q.

2.Check to see if 0<S_2<q.

3.CalculateV=[(e_1h(M)S_2^{-1} $e_2S_1S_2^{1}$)modp]modq.

4.If S_1 is congruent to V ,the message is accepted ;otherwise it is rejected.

4 DECRYPTION

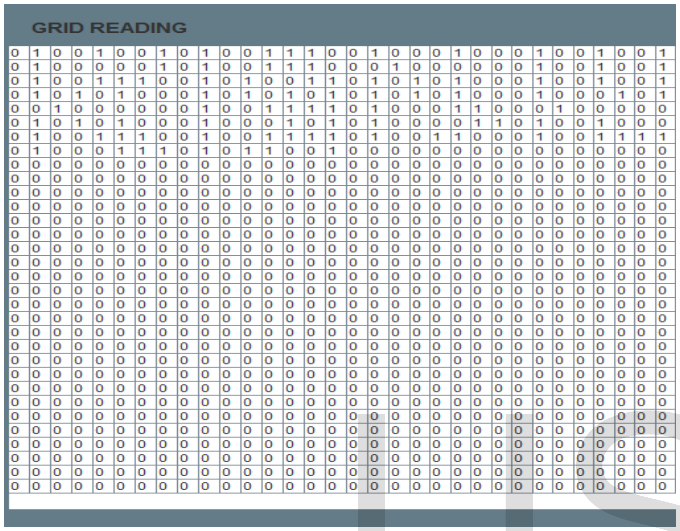
Decryption is done by using the public key of the sender and the encrypted file.

Decryption is the reverse process of encryption.provides authentication, confidentiality[5,17].

RESULTS

The result for the module "GRID READING" is shown below.
We have a text file say "**INDIAN INSTITUTE OF TECHNOLOGY**."
We will take ASCII value representation in 8 bit of each character of the above .txt file.

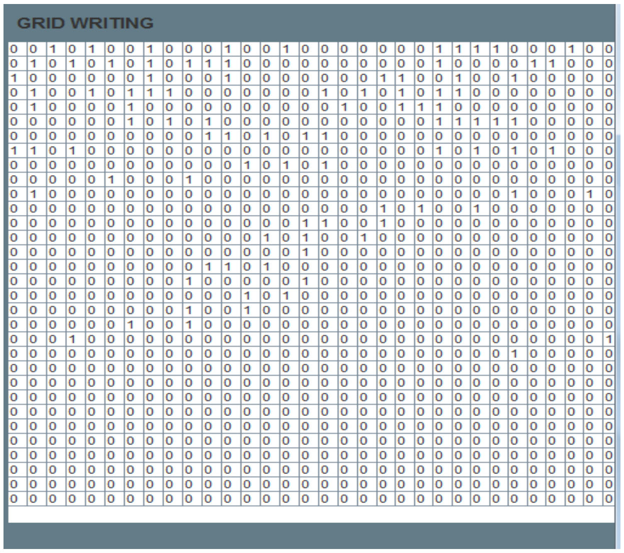
Now the grid reading for the above text is shown below which will be in the form of 0's & 1's.



GRID READING

0	1	0	0	1	0	0	1	0	1	0	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	0	0	1	0	0	1
0	1	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0	0	1
0	1	0	0	1	1	1	0	0	1	0	1	0	0	1	1	0	1	0	1	0	1	0	0	0	1	0	0	1	0	0	1
0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1
0	0	1	0	0	0	0	0	0	1	0	0	1	1	1	1	0	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0
0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1	0	1	0	0	0	0	1	1	0	1	0	0	1	0	0	0
0	1	0	0	1	1	1	0	0	1	0	0	1	1	1	1	0	1	0	0	1	1	0	0	0	1	0	0	1	1	1	1
0	1	0	0	0	1	1	1	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The result for the module "GRID WRITING" is shown below.
The value read diagonally in the above grid and written left to right of equal size grid row by row which is shown below.

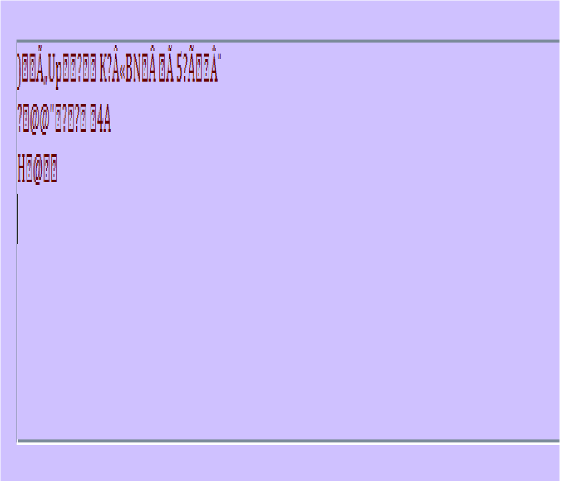


GRID WRITING

0	0	1	0	1	0	0	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	1	1	1	0	0	0	1	0	0
0	1	0	1	0	1	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0
1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	0	0	1	0	0	0	0	0
0	1	0	0	1	0	1	1	1	0	0	0	0	0	0	0	1	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

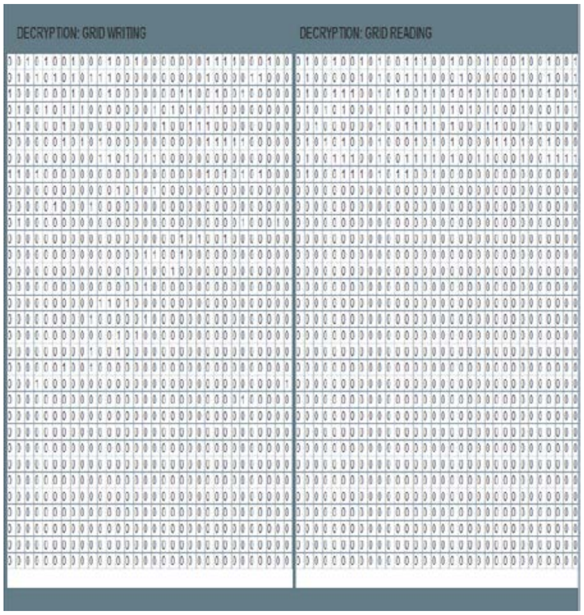
After the implementation of grid writing, encryption is to be done by using DSA algorithm.

The encrypted file for .txt file is shown below:

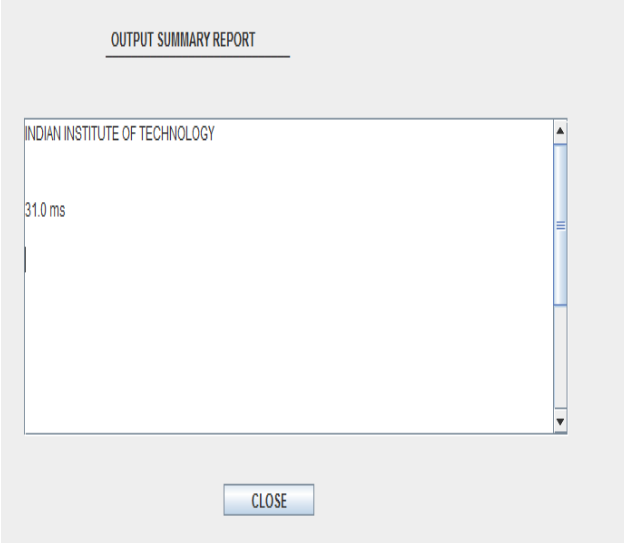


```
)▯▯Ã„Up▯▯?▯▯ K?Â«BN▯Â ▯Ã 5?Ã▯▯Â"
?▯@@"▯?▯?▯ ▯4A
H▯@▯▯
```

When the file is encrypted then the signed file and public key is used to decrypt the message using the same algorithm called DSA.



After decryption, we get the plaintext once again. The figure below shows the output of decrypted message in the form of grid and ultimately we get the same plaintext.



OUTPUT SUMMARY REPORT

INDIAN INSTITUTE OF TECHNOLOGY

31.0 ms

VI. CONCLUSION

This paper work has been implemented for text file with variable grid size of lenth 32 . It is being executed efficiently for 32 but when executed on grid length greater than does not work efficiently because there is a delay with grid size greater than 32. The encryption and decryption time taken by the algorithm is reduced to a great extent. In each session, the private and public keys are automatically generated for the file which has been encrypted and hence increased the security of the system.

In this work, only the text file has been used for encryption and decryption but it will be used to encrypt and decrypt the audio files, video files and images. This dissertation work used DSA algorithm for encryption and decryption of text files but in future the project will use any other public key algorithm for encryption and decryption of the audio, video and image files.

REFRENCE;

[1] Khaled A., Waiel F., Mohamed A., and Alaa A.,“Attack and Construction of Simulator for Some of Cipher Systems Using Neuro-Identifier,”*International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 365-372, 2010.

[2] B. Schneier, *Applied Cryptography: Protocols Algorithms, and Source Code in C*, Wiley & Sons, Inc.1996.

[6] A. Fuster, *“Técnicas criptográficas de protección d datos,”* Ed. Ra-Ma, 2001.

[7] Diffie, W., and Hellman, M. *“New directions in cryptography”* IEEE Trans.

[3] A.J. Menezes, P.C. Van Oorschot y S.A. Vanstone 1997.*“Handbook of Applied Cryptography”*, CRC Press. pp 15- 28 and. 283-291.

[4] J.A. Buchmann, *—Introduction to Cryptography. Marietta, GA: Springer-Verlag”*, 2000, pp. 139-153.

[5] D.R. Stinson, *“Cryptography: Theory and Practice Tercera edición”*, CRC Press. 2005.

[8] W. Stallings, *“Cryptography and Network Security: Principles and Practice”*,2da. Edición, Prentice-Hall, New Jersey, 1999.

[9] Stinson, D.R. : *—Cryptography Theory and Practice‖*,CRC Press, London, 1995

[10] *—Cryptography and Network security‖*, 2nd Edition by Atul Kahate. Tata Mc- Graw-Hill Publications, New Delhi.

[11] *“Security Requirements for Cryptographic Modules*, FIPS PUB 140-1, 1994 January 11

[12] Special Publication 800-12: *“An Introduction to Computer Security”*- The NIST Handbook

[13] Josef P. and Jennifer S., *—Cryptography, an Introduction to Computer security*,‖ Upper Saddle River NJ, Prentice Hall, 1989.

[14] Bruce S., *Applied Cryptography 2ed*, John Wiley and Sons, 1996.

[15] Schaefer F., “A Simplified Data Encryption Standard Algorithm‖, *Computer Journal of Cryptology*, vol. 20, no. 1, pp. 77-84, 1996.

[16] Rivest, R., Shamir A., Adleman L., “*A method for obtaining digital signatures and public key cryptosystems,Communication of the ACM* ”21 (1978), pp. 120-126.

[17] W.Stallings, (2005) "Cryptography and Network Security 4th Ed," Prentice Hall ,pp. 58-309.