Encryption/decryption tool with cryptanalysis

[1]Rizwan Ali, [2]Ashish Kumar, [3]Esh Narayan
[1] Master of Technology in IFTM University, Moradabad
[1,2,3]Computer Science & Engineering
[2]Dept. of Computer science and Engineering IFTM University, Moradabad
[3]Dept. of Computer Science and Engineering PRABHAT ENGINEERING COLLAGE KANPUR (UP)
[1]rizwanali.cs@gmail.com, ashishcse29@gmail.com, [3]narayanesh1984@gmail.com

Abstract- The dissertation titled" Encryption/Decryption Tool with Cryptanalysis" is based on the concept of cryptographic system. We have implemented a set of encryption/decryption methods which include Hill Cipher, Caesar Cipher and Transposition Cipher & RSA. These methods are used to convert a given text into secret code it to another user & vice-versa. Further another possibility of finding out a text when a secret code is found out without knowing about the key, the sender has used to encrypt it. Hence we provide a way for encryption, decryption and an attack on any file and thus get the way for a secured communication between users.

Key words: Feather selection, Encryption/Decryption mat lab, RSA, Network Analysis etc

1. INTRODUCTION

Cryptography is probably the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security. Cryptography is the study of secret writing that deals with the all aspects of data security, authentication, digital signature, electronic money and other application. It concerned with the development of algorithms which can be used to provide security to the data in multimedia transmission, verify the correctness of the message at the recipient and form the basis of many technological solution to computer and communication security problem. In the other we can say cryptography is science of mathematical concept that is used to encrypt and decrypt the information, so no one can read it except the intended recipient.

1.1 Security trends

A security attack can be viewed as access to a confidential data. An attack can be occurred with the intention of reading the data or modifying the data. This report made a general consensus that the Internet needs more and better security, and it identified key areas for security mechanisms. Among these were the need to control of network traffic, the need to secure end to end user traffic using authentication, secure the network infrastructure from unauthorized monitoring and encryption mechanisms [1]. With the emergence of information technology, the attacks on the Internet and Internet-attached systems have grown more sophisticated and drastically while the amount of expertise and awareness needed to undertake an attack has declined. Critical infrastructures gradually more rely on the Internet for operations. Individual users rely on the security of the Internet, email, the Web, and Web-based applications to a greater extent than ever. Thus, a wide range of technologies and tools are needed to counter the growing threat. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:

1.1.1 Passive Attack

A passive attack on a cryptosystem is one in which the cryptanalyst cannot interact with any of the parties involved, attempting to break the system solely based upon observed data (i.e. the cipher text). In this type of attack, the main aim of the opponents is to obtain the information. It means they never harm the recourses or modify the information, they just read the information. It is very hard to detect this type of attack because passive attacks cannot be sensed by the decrypted message. There are two types of passive attacks, release of message content and traffic analysis.

1.1.2 Active Attack

Active attacks are used to modify the encrypted information or the creation of false stream which can change the meaning of the decrypted message [4]. Four types of active attack are these: Masquerade, Replay, Modification of the messages, and Denial of service.

It uses two keys; public key and private key, sender encrypts the message by using the public key of receiver and receiver decrypt the message by using his private key. So there is no need of key transfer, which increases its security. In this technique both parties have their set of key, public key and private key. Public key is public to all in the network can be access by everyone while private key is private to its owner.

1.2 Problem description

The basic aim here is to provide a means for secured communication between sender & the receiver by scrambling the message that has to be transmitted using various cryptographic methods. Along with this, implementing different types of attacks on an encrypted text & finding out the actual text being transmitted for the end-user using conventional & public-key encryption techniques. We have to take into account the computational efficiency, memory requirements, flexibility, hardware & software suitability & simplicity.

The project caters to three major objectives:-

1. *Encrypting a given text file* ***:***

Here we convert a given file with human readable text into a secret code with the help of secret key that is known only to sender & receiver.

2. Decrypting a given encrypted file

Here we convert a given encrypted file into a human readable text file with the help of same secret key as used by sender to encrypt that file.

3. Attacking an encrypted file

Here we check the possibility of all key combinations as the actual key is not known. We apply each combination on the secret code to break it.

2. LITERATURE SURVEY

When applied for wireless sensor networks. While in Asymmetric Encryption, two keys are used. The SCADA communication takes place over radio, modem, or devoted serial lines. The internet SCADA facility has brought several advantages in terms of control, data generation and presentation. With these advantages, come the security issues about web SCADA. Masadeh, Turab (2010) this paper encryption algorithm are compared on the basis of wireless network. Encryption techniques play a main role in wireless network security systems. However, these schemes consume a significant amount of computing resources such as CPU time, and packet size [3]. .This can be extended to many rounds. we generalize RSA encryption method in order to be implemented in the general linear group on the ring of integer mod n. The encryption method has no restriction in encryption and decryption order and is claimed to be efficient, scalable and dynamic. To remedy the wireless network security issue, a novel work has been deployed to secure the transmitted data over wireless network and examine a method for analyzing trade-off between efficiency and security. A comparison has been conducted for those encryption techniques at different settings for each method such as different sizes of data blocks, different platforms and different encryption/decryption speed. They offered proof of concept by applying a definite privacy homomorphism for sensor network. Sorry to say as shown by Rivest, et al., any privacy homomorphism is unconfident even against cipher text that only attacks if they support comparison operations [8]. In this paper we show that a particular order preserving encryption technique achieve the above mentioned energy benefits and give when used to support comparison operations over encrypted texts for wireless sensor networks. The technique is shown to have reasonable memory and computation. In this paper, comparison between Encryption techniques as used in Communication between SCADA Components is discussed. The reason reverse to the efficiency (separate nodes perform different tasks), fault-tolerance (if some nodes are occupied then others can perform the task) and security (the trust essential to perform the task is shared between nodes) that order differently [9]. This paper aims to describe and review the different research that has completed toward text encryption and description in the block cipher.

3. SPECIFICATION OF ENCRYPTION TECHNIQUES

In this chapter we elaborate all the four consider encryption techniques Caesar Cipher, Hill cipher, Transposition and RSA in section 3.1. Cryptanalysis is also described of respective algorithms. In section 3.2, data flow diagram of encryption and decryption techniques are described.

3.1 Encryption Techniques

3.1.1 Caesar Cipher

The previously known use of a substitution cipher, and the simplest, was by Julius Caesar [7]. The Caesar cipher replaces each letter of the alphabet with the letter standing three places further down the alphabet. For example:

Plain text: we are indian

Cipher text: zh duh lqgldq

The alphabet is wrapped around, so that the letter following Z is A. which can be defined as follows:

Plain: a b c d e f g h i j k l m n o p q r s t u v w x y z

cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Now we assign a numerical equivalent to each letter:

A	B	C	D	E	f	G	H	I	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	P	q	r	S	T	U	v	w	X	y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

The algorithm for the Caesar cipher can be defines in term of cipher text (C), plain text (P) and decrypted text (D) with the help of modular arithmetic.

$C = (P + 3) \bmod 26$

A shift may be of any number, so that the general Caesar algorithm is

$C = (p + k) \bmod 26$

Where, k takes on a value in the range 1 to 25 and the decryption algorithm is simply

$D = (C + k) \bmod 26$

*3.1.1.1 Cryptanalysis of Caesar Cipher***:** Caesar cipher is very easy to break because of its encryption nature.

Brute Force Attack: Brute force can be simply applied to the encrypted text if the technique used for encryption is known. So in case of Caesar Cipher Brute force attack is applied by taking all the possible set of keys [2]. There are only 25 possible keys to attack the code. Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:

1. The encryption and decryption techniques are known.
2. There are only 25 possible keys to try.
3. The language of the plaintext is identified and easily decipherable.

In most of the networking situations, we can consider that the techniques are known. But the large size of key employed in an algorithm makes brute-force cryptanalysis impractical. The third characteristic is also considerable. If the language of the plaintext is not known, then plaintext output may not be decipherable.

3.1.2 Hill Cipher

Hill cipher is a multi letter cipher, developed by the renowned mathematician Lester Hill in 1929. The encryption technique takes m successive plaintext letters and substitutes for them m cipher text letters. The substitution is determined by m linear equations in which each alphabet is assigned a numerical value (a = 0, b = 1 ... z = 25). For m = 3, the system can be expressed follows

$$C = KP \bmod 26$$

Where C and P are column vectors of length 3, representing the plaintext and cipher text, and K is a 3 x 3 matrix, representing the encryption key. Operations are performed mod 26.

3.1.3 Transposition

This technique is known as transposition cipher. The simplest such cipher is the rail fence technique is one of the simplest technique which uses transposition, in which the plain text is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encrypt the message "meet me after the toga party" with a rail fence of depth 2, we perform the following:

m e m a t r h t g p r y e t e f e t e o a a t

The encrypted text is “MEMATRHTGPRYETEFETEOAAT”

This sort of thing would be trivial to crypt analyzer. Another more complex technique is to write the message in a rectangle, row by row, and read the message off, column by column, and permute the order of the columns. The order of the columns then becomes the key to the scheme. For example,

Key: 4 3 1 2 5 6 7

Plain text: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z

Cipher text: TTNAAPTMTSUOAODWCOIXKNLYPETZ

A pure transposition cipher is simply acknowledged because it has the same letter frequencies as the original plain text. For the type of columnar transposition just shown, cryptanalysis is fairly straight forward and includes laying out the cipher text in a matrix and playing around with column positions. Diagram and trigram

frequency tables can be helpful. The transposition cipher can be made considerably more robust by performing more than one level of transposition. The result is a more complex transformation that is not easily reconstructed. Thus, if the foregoing message is re-encrypted using the same scheme,

Key: 4 3 1 2 5 6 7

Input: t t n a a p t
m t s u o a o
d w c o i x k
n l y p e t z

Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

3.1.4 RSA

This is a block cipher which makes use of an expression with exponentials. This technique uses public key (e, n) and private key (d, n) for encryption and decryption. It takes a plaintext block M and encrypt it in a cipher text C by using the following expression [RSA].

$C = M^e \bmod n$

Decryption of the encrypted block C is done using the formula below

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Where n is a number greater than both M, C and should be known both sender and receiver of the message. The following requirements must be met to satisfy the public key encryption.

1. It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$.
2. It is relatively easy to calculate mod M^e mod n and C^d for all values of $M < n$.
3. It is infeasible to determine d given e and n.

The first condition holds if e and d are multiplicative inverses modulo ∅(n), where ∅(n) is the Euler totient function. For the two distinct prime numbers p and q:

$n = p*q$

$\emptyset(n) = (p-1)(q-1)$

So the relationship between e and d can be expressed as

***ed* mod ∅*(n)* ≡ 1**

e and d are multiplicative inverses mod ∅(n). Note that, according to the rules of modular arithmetic, the above equation is true if and only if, d and e are relatively prime to ∅(n). Means gcd (∅(n),d) = 1 and gcd(∅(n),e) = 1 must be satisfied.

3.1.4.1 Cryptanalysis

There are four ways to attack RSA encryption technique.

i. Brute Force Attack

In this attack, all the possible combination of private key is used to decrypt the code. So, large size of key can avoid Brute force attack. RSA can use large size key but that reduces speed of computation.

ii. Mathematical attack

It involves factoring the product of two prime numbers [10]. Most discussions of the cryptanalysis of RSA have focused on the task of factoring n into its two prime factors. We can identify three approaches to attacking RSA mathematically:

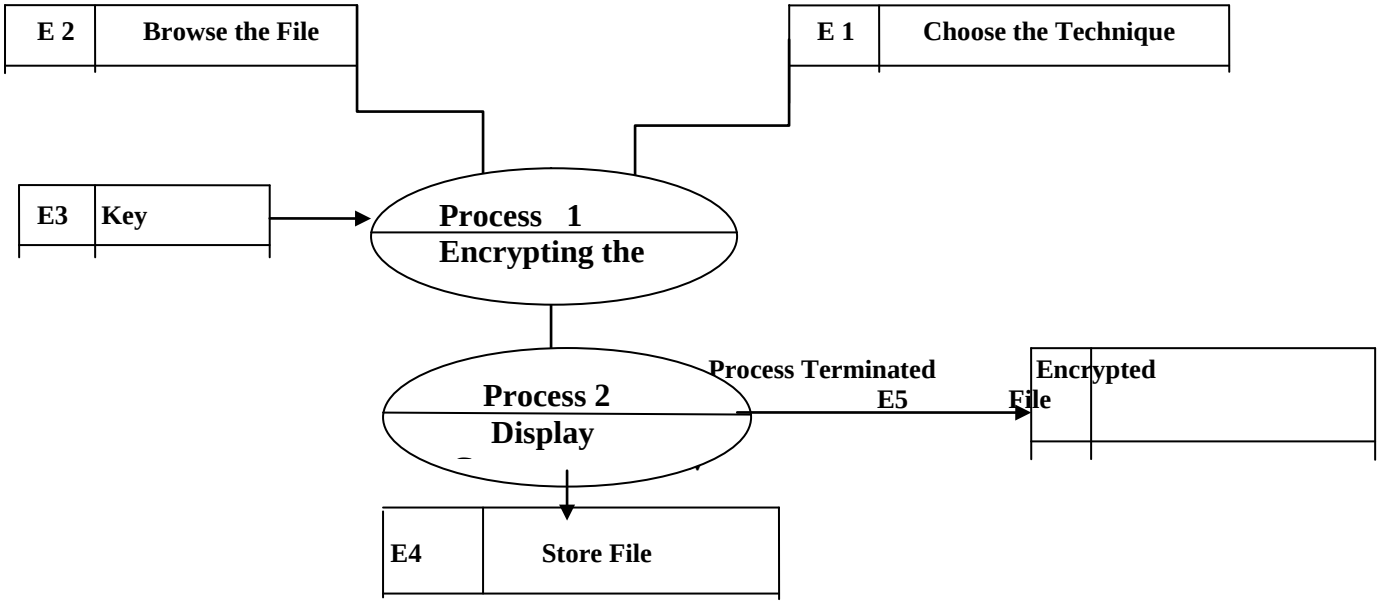
- Factor n into its two prime factors. This enables calculation of Ø (n) = (p-1) x (q-1), which in turn enables determination of $d \equiv e^1 \pmod{Ø(n)}$.
- Calculating Ø (n) directly, without first determining p and q. This one also enables the determination of $d \equiv e^1 \pmod{Ø(n)}$.
- Determine d directly, without first determining Ø (n).

RSA tackles with this attack by using large prime numbers which in turn provide a large value of n and factoring of a large n is a hard problem.

3.2 Data flow diagram

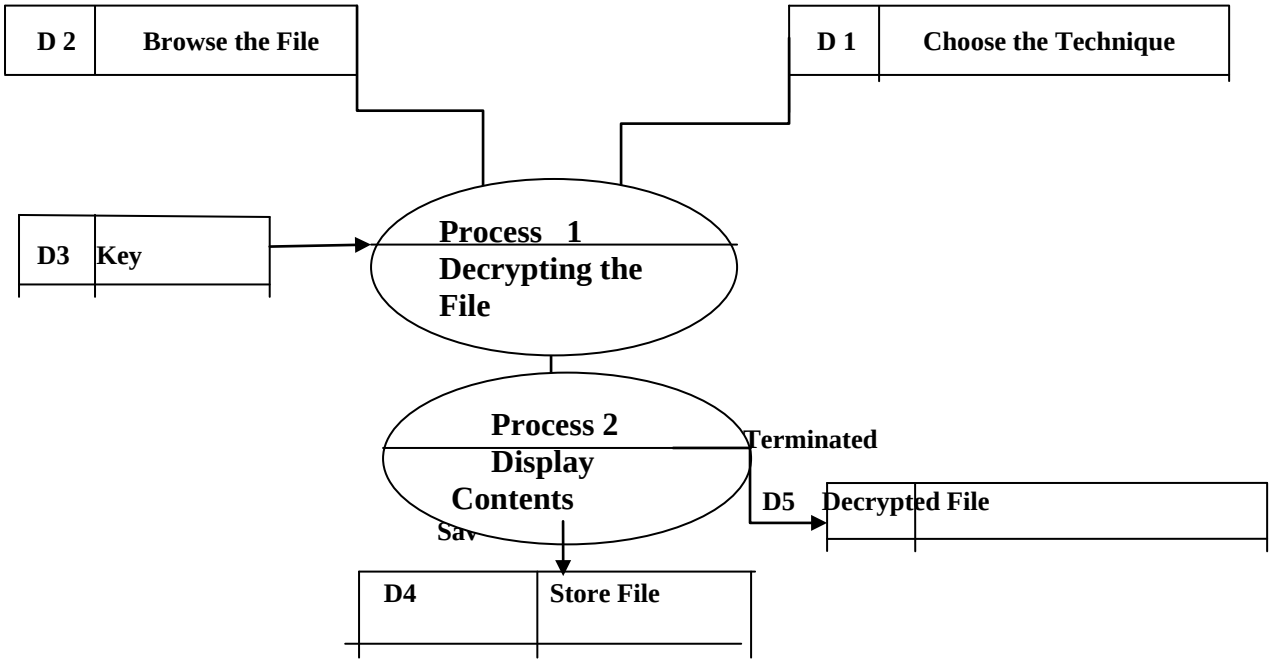
"The purpose of Data Flow Diagram is to provide a semantic bridge between the users and the system developers"

3.2.1 DFD for Encryption



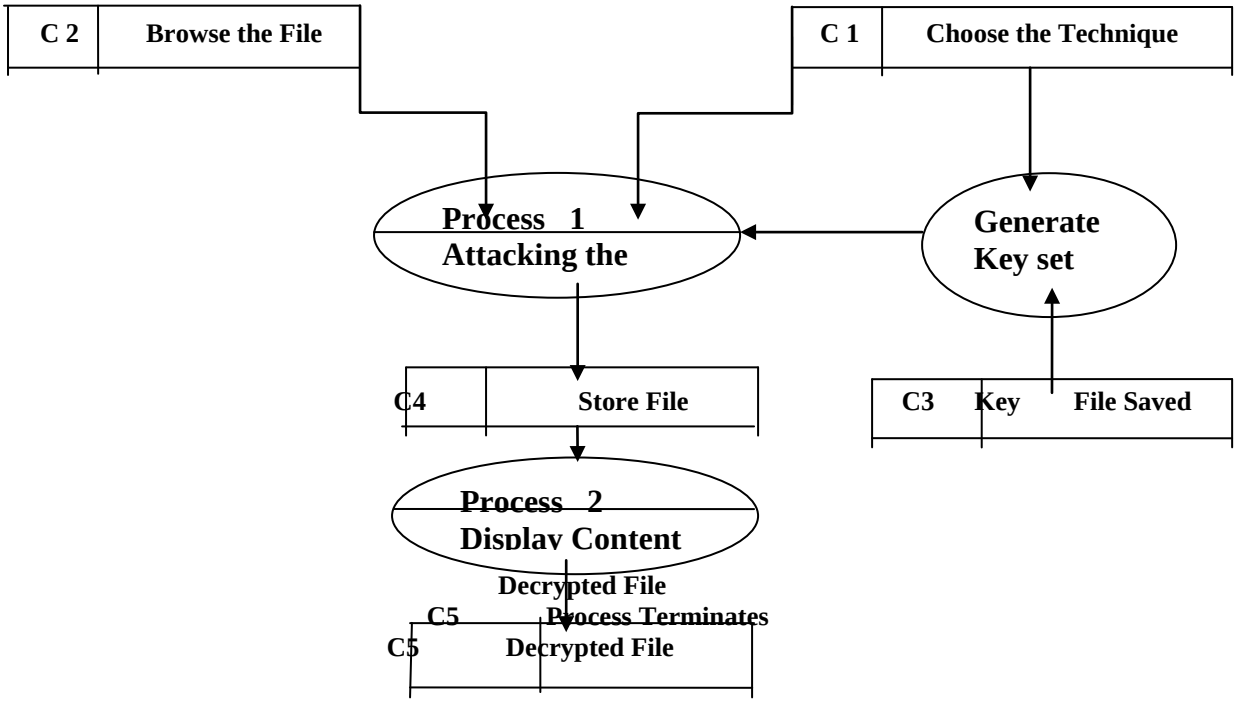
(Fig 2.1)

3.2.2 DFD for Decryption



(Fig 2.2)

3.2.3 DFD for Cryptanalysis

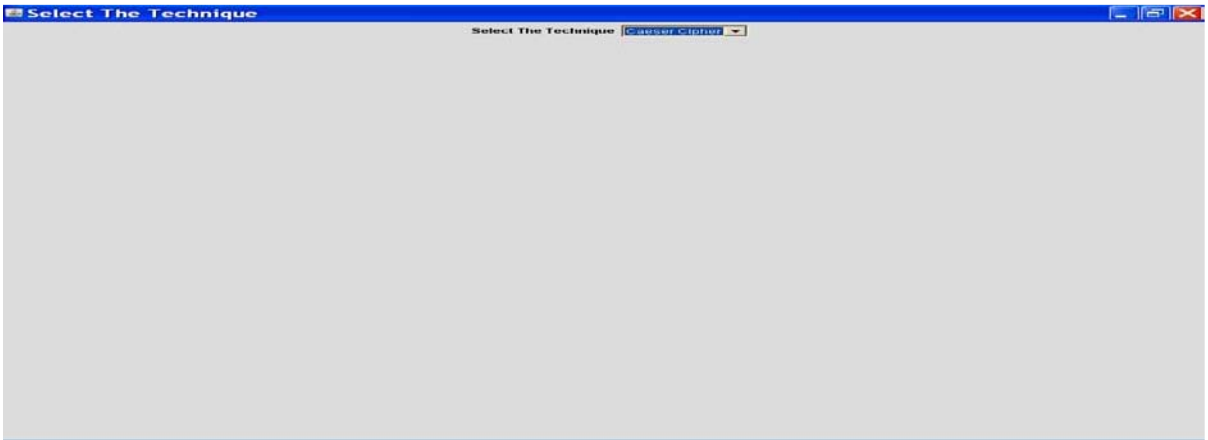


3.3 Screen Shots

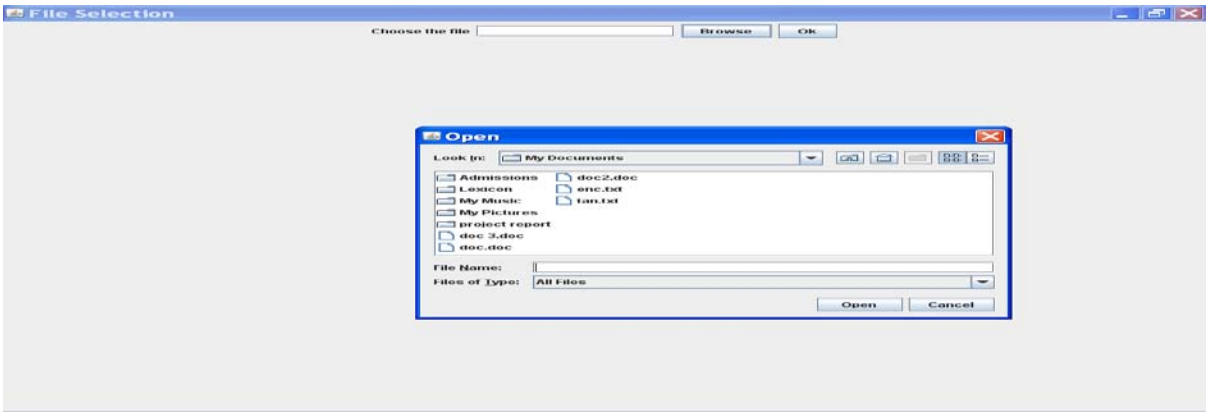
"The Screen Shots better describes the product and helps the users to evaluate it

3.3.1 User interface for main menu

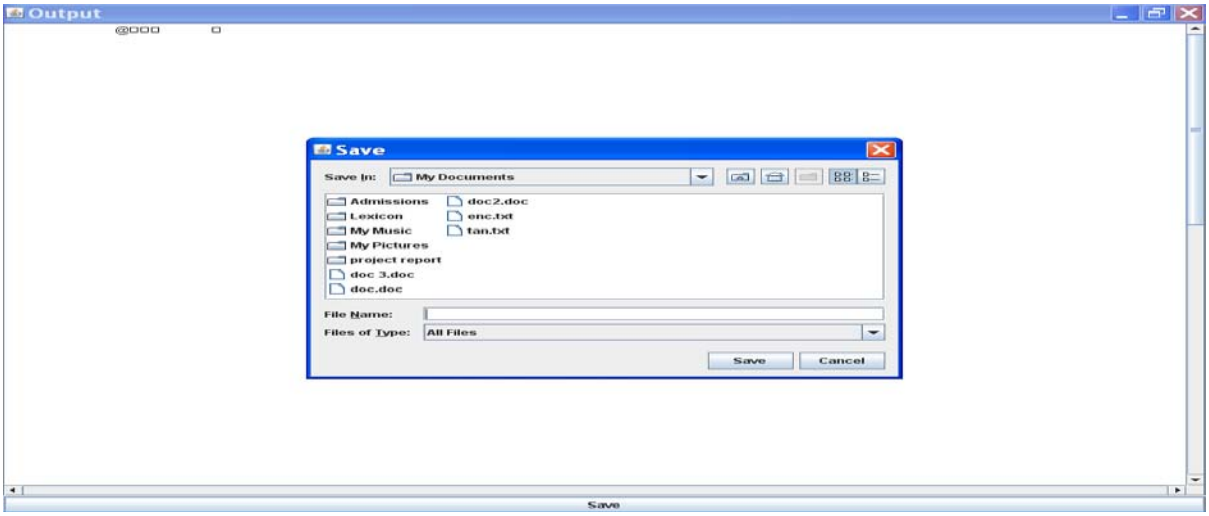
3.3.2 User interface for Selection of Techniques



3.3.3 User interface for File Selection



3.3.4 User Interface for output



4. TESTING AND COMPARATIVE ANALYSIS

Testing is done to make sure the generated output of the proposed idea, is according to the requirements. So we test our implemented concept by using different parameter of comparison because in this work the quality of proposed concept can be checked by comparing different encryption techniques. This analysis is based on three parameters time, Line of code (LOC) and number of attempt (NOP) to decrypt the encrypted text.

i. *Time*
Time is one of the fundamental parameter to check the efficiency of any algorithm. It refers, time taken to compute a particular output.

ii. *Line of Code*
Line of code is used to measure space complexity of a method implemented in a programming language.

iii. *No. of attempt*
This is one of the most important parameter for the comparative analysis of the defined encryption techniques. It counts the effort require to decrypt a particular encrypted code of an encryption algorithm. So in the cryptanalysis a series of attempt are used to decrypt the code. More number of attempts shows the robustness of the technique.

	Caesar Cipher	**Hill Cipher**	**Transposition**	**RSA**	
LOC	**95**	**119**	**134**	**330**	
NOA	**3**	**4**	**4**	**6**	

5. CONCLUSION AND FUTURE WORK

Successful completion of the encryption and decryption of the given text files for all the algorithms. Along with this we have the completion of cryptanalysis for the three algorithms of Caesar, Transposition & RSA encryption techniques. Hill cipher is in the processing stage for the cryptanalysis part. It counts the effort require to decrypt a particular encrypted code of an encryption algorithm. So in the cryptanalysis a series of attempt are used to decrypt the code. The proposed comparison is performed on the text file. It can be applied on the audio and video stream for more comparative analysis. As well as we can consider more number of different algorithms.

ACKNOWLEDGEMENT

I would like to thank God for not letting me down at the time of crisis and showing me the silver lining in the dark clouds and I wish to express my science profound gratitude to Mr. Ashish Kumar assistant Professor in IFTM Moradabad, whose supervision & guidance in this investigation has been carried out, without whose guidance and constant supervision. It is not possible for me to complete this research paper successfully.

REFERENCES

[1] In May 2009 “Audio encryption using higher dimensional chaotic map” R. Gnanajeyaraman, K. Prasadh 2, Dr.Ramar3, Research scholar, Vinayaka Missions University, Salem, Tamilnadu, India.
[2] In 2003 “Frequency –selective partial encryption of compressed audio” Servetti, A.; Testa, C.; De Martin, J.C
[3] *www.mathworks.in/products/matlab/.*
[4] Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings.
[5] Nadeem , "A performance comparison of data encryption algorithms", IEEE information and communication technologies, pp.84-89, 2006.Bn
[6] Rivest, R.; Shamir, A.; and Adleman, L. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." Communications of the ACM, February 1978.
[7] A comparison of data encryption algorithms with the proposed algorithm: Wireless security Masadeh, S.R. Aljawarneh,S.; Turab, N.; Abuerrub, A.M. Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference.
[8] Comparison of Encryption Schemes as Used in Communication between SCADA Components Ubiquitous Computing and Multimedia Applications (UCMA), 2011 International Conference on Robles, R.-J. Dept. of Multimedia Eng., Hannam Univ., Daejeon, South Korea Balitanas, M.; Caytiles, R.; Gelogo, Y.; Tai-hoon Kim
[9] Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System Acharya, B. ; Jena, D. ; Patra, S.K. ; Panda, G. Advanced Computer Control, 2009. ICACC '09. International Conference on IEEE Conference Publications
[10] “A Novel Key-Based Transposition Scheme for Text Encryption” Malik, S. Frontiers of Information Technology (FIT), 2011 Publication Year: 2011 , IEEE Conference Publications
[11] “An Efficient RSA Public Key Encryption Scheme” Aboud, S.J.; Al-Fayoumi, M.A. Al-Fayoumi, M. ; Jabbar, H. Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on Digital Object Identifier:10.1109/ITNG.2008.199 IEEE Conference Publications.