Information Hiding: A Secure Scheme Using Reverse Transposition Algorithm

J. Hari[1], A. SaiPrasad[2], Y. V. N. GeethikaSravya[3], J. Varalakshmi[4], K. Navya[5], B. Sandhya[6]
1. Assistant Professor, Vignan's Institute of Engineering For Women,

2. Assistant Professor,Vignan's Institute of Engineering For Women,
3,4,5,6 IV-IT, Vignan's Institute of Engineering For Women

Abstract

Network Security & Cryptography *is a concept to protect network and data transmission over wireless-network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security. Cryptography is the science of information security. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption).There are several algorithms for encryption and decryption purpose. There are 2 types of cryptography: Symmetric key cryptography and Asymmetric key cryptography. There are few symmetric cryptography algorithms such as DES, IDEA, RC2, RC4 etc.*

This paper describes cryptography, ***"Reverse Transposition Algorithm (RTA)****" in detail and then proposes a new symmetric key algorithm. Algorithms for both encryption and decryption are provided here. The advantages of this new algorithm over the others are also explained.*

1. Introduction

Security is often viewed as the need to protect one or more aspects of network's operation and permitted use (access, behaviour, performance, privacy, and confidentiality included). Security requirements may be global or local in their scope, depending upon the networks or internetworks purpose of design and deployment. Security attacks compromises the information security. The concept of securing messages through cryptography has a long history. Indeed, Julius Caesar is credited with creating one of the earliest cryptographic systems to send military messages to his generals.

Cryptography is the art and science of keeping data secure. Cryptographic services help ensure data privacy, maintain data integrity, authenticate communicating parties, and prevent repudiation (when a party refutes having sent a message). Basic encryption allows you to store information or to communicate with other parties while preventing non-involved parties from understanding the stored information or understanding the communication. Encryption transforms understandable text (plaintext) into an unintelligible piece of data (ciphertext). Decryption restores the

understandable text from the unintelligible data. Both functions involve a mathematical formula (the algorithm) and secret data (the key).

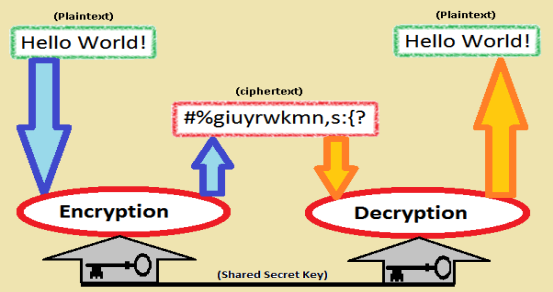


Fig: Cryptography Concept

2. TYPES OF CRYPTOGRAPHIC ALGORITHMS:

There are two types of cryptographic algorithms:

1. **Secret Key Cryptography**

With a **secret** or **symmetric** key algorithm, the key is a shared secret between two communicating parties. Encryption and decryption both use the same key. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are examples of symmetric key algorithms.

There are two types of symmetric key algorithms:

Block ciphers

In a block cipher, the actual encryption code works on a fixed-size block of data. Normally, the user's interface to the encrypt/decrypt operation will handle data longer than the block size by repeatedly calling the low-level encryption function. If the length of data is not on a block size boundary, it must be padded.

Stream ciphers

Stream ciphers do not work on a block basis, but convert 1 bit (or 1 byte) of data at a time.

The figure below shows the symmetric key cryptography process.

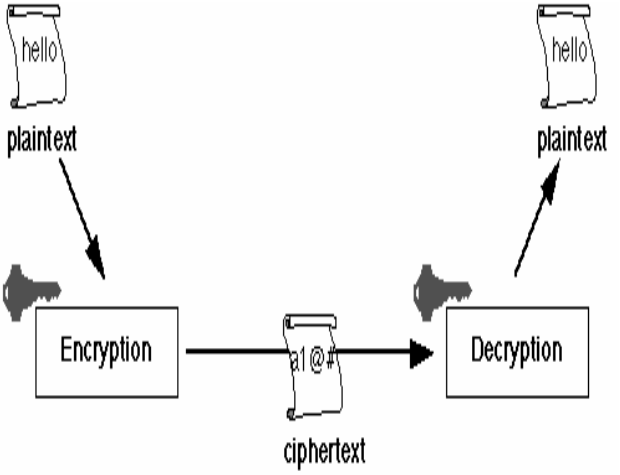


Fig: Secret Key Cryptography

2. Asymmetric Key Cryptography

With a **public key** (PKA) or **asymmetric key** algorithm, a pair of keys is used. One of the keys, the private key, is kept secret and not shared with anyone. The other key, the public key, is not secret and can be shared with anyone. When data is encrypted by one of the keys, it can only be decrypted and recovered by using the other key. The two keys are mathematically related, but it is virtually impossible to derive the private key from the public key. The RSA algorithm is an example of a public key algorithm.

Public key algorithms are slower than symmetric key algorithms. Applications typically use public key algorithms to encrypt symmetric keys (for key distribution) and to encrypt hashes (in digital signature generation).Together, the key and the cryptographic algorithm transform the data. All of the supported algorithms are in the public domain. Therefore it is the key that controls access to the data. You must safeguard the keys to protect the data.

Since this paper deals more with Secret/Symmetric Key cryptography further details of the same are discussed below.

The figure below shows the asymmetric key cryptography process.

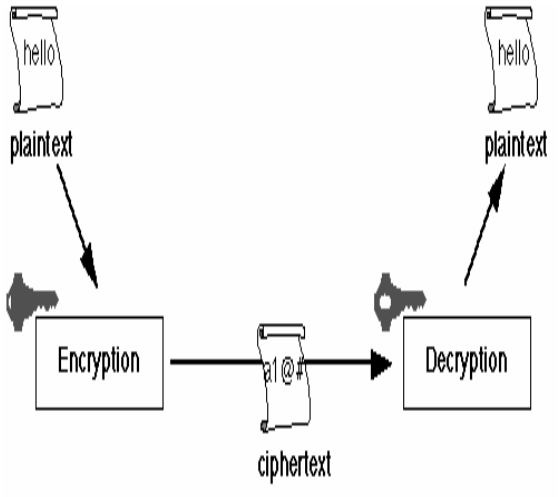


Fig: Asymmetric Key Cryptography

Basic goals of Cryptography:

Every cryptography has four basic goals- confidentiality, integrity, authentication and non-repudiation. Every algorithm ensures that these four goals are met while transmitting any digital message.

a. Confidentiality- this ensures that while transmitting date in a network or Internet, it will remain confidential. No one can read this message except your intended receiver. The two types of key systems in use for confidentiality- public key and secret key.

b. Integrity-this ensure that a message is not altered in the way of transmission. So, a receiver of the message becomes certain that his received message is identical to the original message- no alteration of message by a third party. This functionality is ensured by digitally signed the original message.

c. Authentication- this is a very important function of crypto system and it verifies the claimed identity of the users. For instance, Dan wants to communicate with one of your friend, Jim. Jim sends Dan a challenge message by saying that proves your claim by encrypting the message. Then, Dan encrypts the message with his secret key only known to him and Jim. The encrypted message is sent back to Jim and after his verification that the encrypted message matches with the original message, he become sure that he is communicating with Dan.

d. Non repudiation-this gives assurances to the receiver of a message that it actually came from the sender and no one is faking the identity of the sender. This function of cryptography is provided with Public Key System only.

4. EXISTING ALGORITHM

Encryption Algorithm

Step-1: Take any alphabet.
Step-2: Give the ASCII value of that alphabet.
Step-3: Convert ASCII value into binary format.
Step-4: Do complement of that binary conversation.
Step-5: Take 10 as a secret key for encryption. Multiply that key with complement of that binary conversion.
Step-6: Whatever the result comes from multiplication with secret key, the result will be converted into hexadecimal format. It gives cipher text.

Decryption Algorithm

Step-1: Whatever the cipher text comes as a hexadecimal format, the result will be converted into binary format.
Step-2: Take 10 as a secret key for decryption and the result will be divided by the secret key.
Step-3: Do complement of above result.
Step-4: Convert the complement result into decimal format.
Step 5: Take the ASCII value of that decimal format and Convert the given ASCII value into alphabet which is original plain text.

5. PROPOSED ALGORITHM

Encryption Algorithm

Step 1: Generate the ASCII value of the letter (plain text)
Step 2: Generate the corresponding binary value of it.
[Binary value should be 8 digits (no matter how much the length of it, we should represent it in 8 digits (28=256). e.g. for

decimal 32 binary number should be **00**100000 (underlined zeros are required)]

Step 3: Reverse the 8 digit's binary number

Step 4: Take a 4 digits divisor (>=1000) as the ***Key***

Step 5: Divide the reversed number with the divisor

Step 6: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively.

If any of these are less than 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the ciphertext i.e. encrypted text. Now store the remainder in first 3 digits & quotient in next 5 digits.

Step 7: Do 1's complement of that binary number obtained above.

Step 8: Whatever the result comes, the result will be converted into ASCII code. It gives cipher text. [Since it will works character by character that is why spaces, commas, each & every character will be treated as one single character & we have to apply the above algorithm for every character.]

Decryption Algorithm

Step 1: Whatever the cipher text comes, the result will be converted into ASCII Code.

Step 2: Generate the corresponding binary value of it.

Step 3: Do 1's complement of above result.

Step 4: Reverse the obtained result.

Step 5: Multiply last 5 digits of the ciphertext by the ***Key.***

Step 6: Add first 3 digits of the ciphertext with the result produced in the previous step.

Step 7: If the result produced in the previous step i.e. step 5 is not an 8-bit number we need to make it an 8- bit number.

Step 8: Reverse the number to get the original text i.e. the plain text

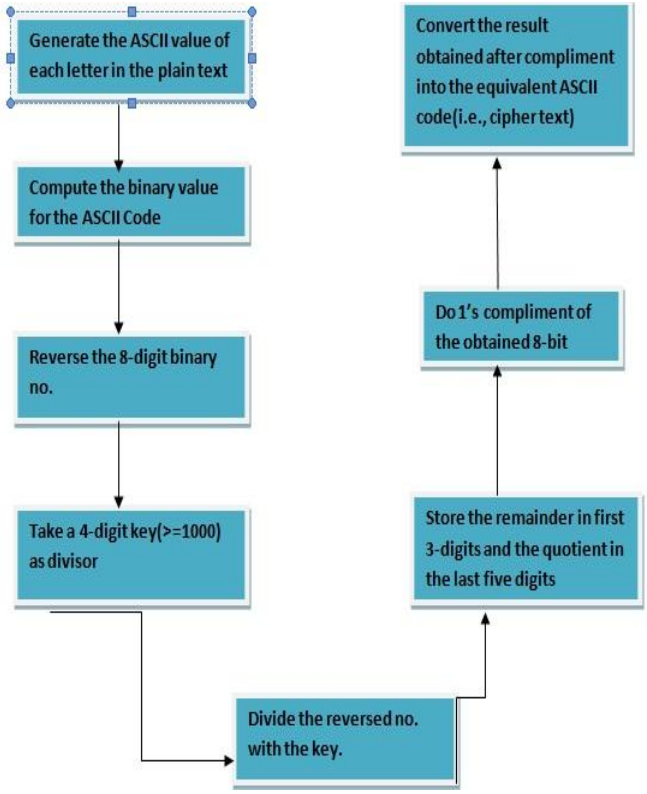


Fig: Encryption Process

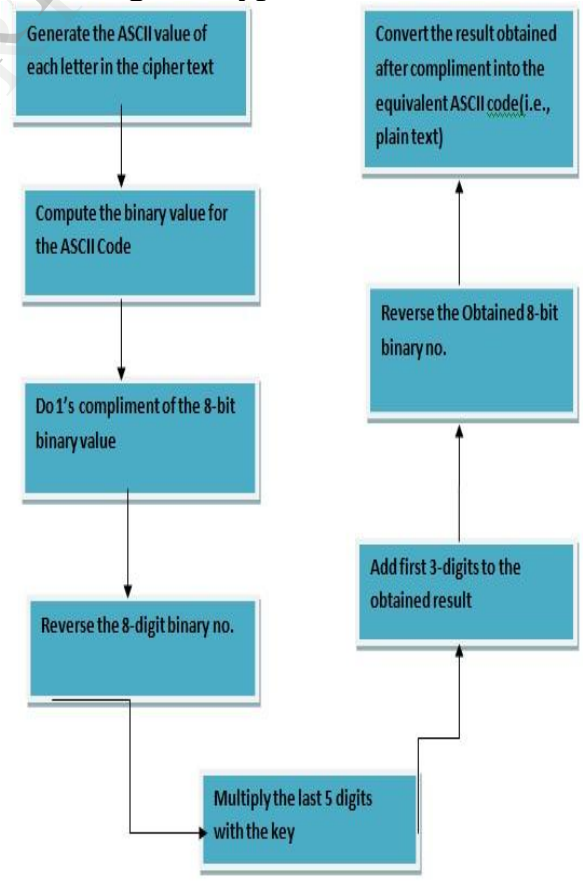
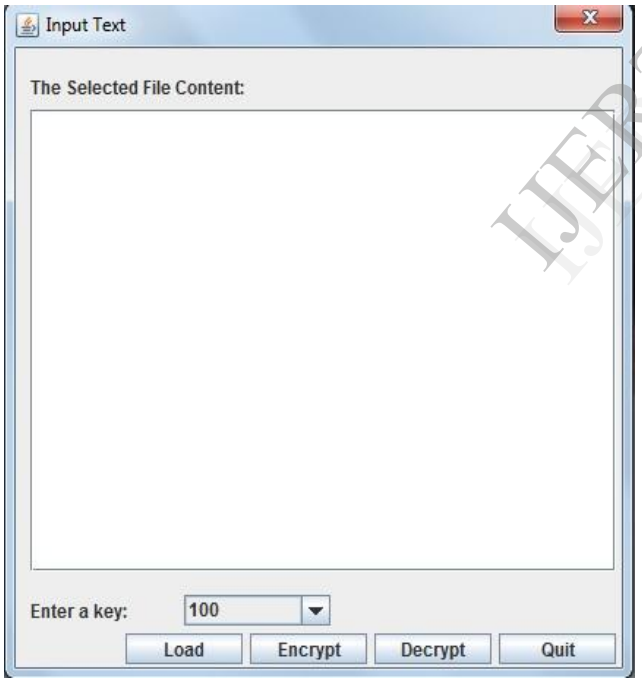


Fig: Decryption Process

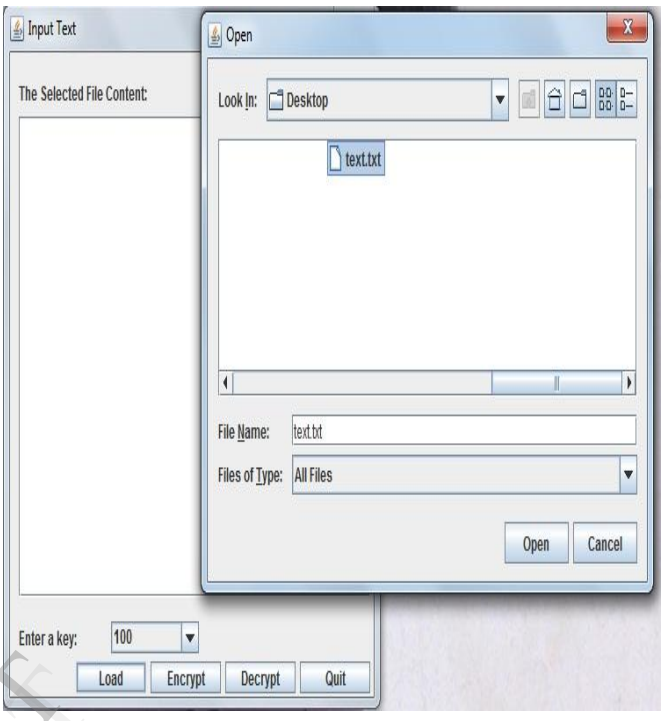
6. SCREEN SHOTS

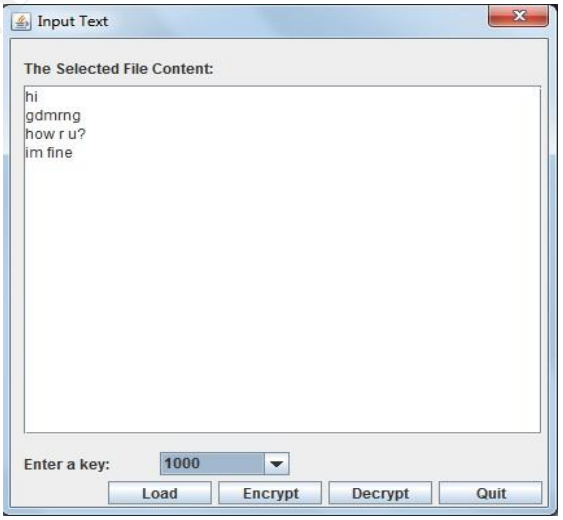
Login Form:

Text Input Screen:

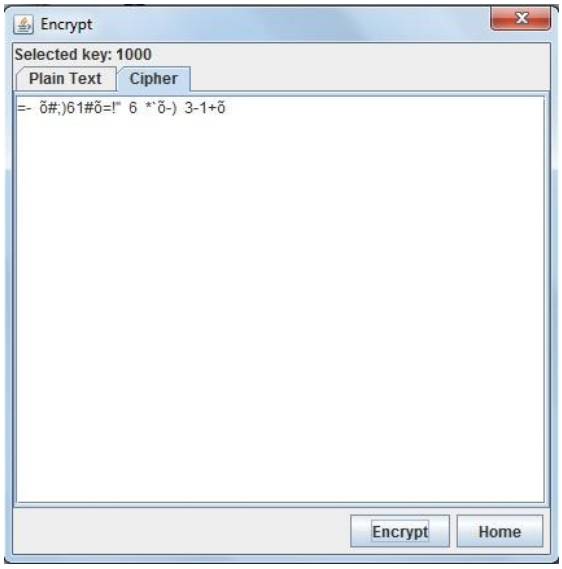


Loading a File:

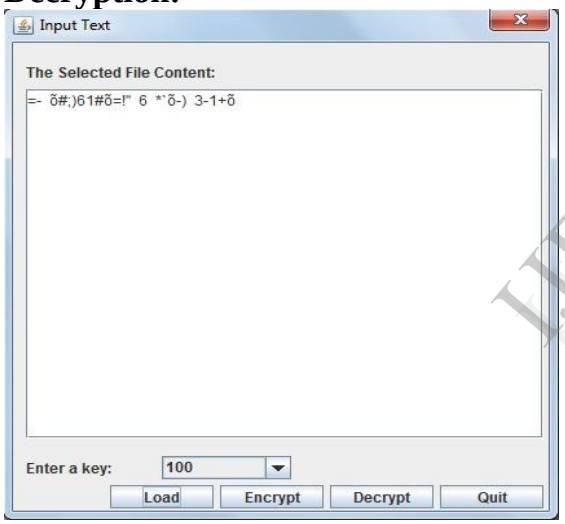




Encryption:



Decryption:



7. CONCLUSION

Cryptography is used to achieve few goals like Confidentiality, Data integrity, Authentication etc. of the data which has sent to the receiver from the sender. Now, in order to achieve these goals various cryptographic algorithms are developed by various people. It has been found that the algorithms which are available at this moment are more or less difficult or complex in nature, and of-course it is quite obvious. Because those algorithms are used to maintain high level of security against any kind of forgeries. For a very minimal amount of data those algorithms wouldn't be cost effective since those are not designed for small amount of data.

The aim of this work was to design and implement a new algorithm to address this issue so that we don't have to apply those algorithms (which are not cost-effective) to encrypt a small amount of data.

Keeping this goal in mind the proposed algorithm has been designed in a quite simple manner but of-course not sacrificing the security issues. A single is used for both encryption and decryption i.e. it is fallen under secret key cryptographic algorithm.

8. Advantages of Algorithm:

1. The algorithm is very simple in nature.
2. There are two reverse operations which makes it more secure.
3. CRC checking in receiver end is easier.
4. For small amount of data this algorithm works smoothly.

9. FUTURE SCOPE

We will continue to investigate the potentials of this algorithm and improve this proposed system to enhance the detection efficiency. The symmetric key cryptographic algorithm can be adjusted to avoid the attacks by hackers. We can trace the hackers by detecting the IP address from which the key is being accessed and changed. This method not only provides

more security but also ensures privacy for both sender and the receiver and can be helpful in finding out the hackers.

But as public key cryptography is more secured then secret key cryptography our next task would be to develop and design a public key cryptographic algorithm in a simple manner as it is done in this paper.

9. REFERENCES

1. Atul kahate,"Computer and Network security", Tata Mc Graw Hill, 2nd edition 2008.

2. Ayushi, "A Symmetric Key Cryptographic aalgorithm", International Journal of Computer Applications, 2010.

3. Zakir H Sarker, Md. Shafiul Parvez, "A Cost Effective Symmetric Key cryptographic Algorithm for Small Amount of Data", IEEE, 1995.

4. Sheetal Saigal, Saloni and Akshat Sharma, "A Secret Key Cryptographic Algorithm", Journal of computing, Volume 3, issue 8, August 2011.

5."Introduction to Public-Key Cryptography", an article available at developer.netscape.com/docs/manuals/security/pkin/contents.html

6. Gary C. Kessler, "An overview of cryptography", 1998, an article available at www.garykessler.net/library/crypto.htm

7. B. Forouzan, "Cryptography and Network ecurity" 4th edition, Mc Graw Hill, Inc 2007.

8.http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=%2Frzajc%2Frzajcconcepts.htm

9.http://discovery.bits-pilani.ac.in/rahul/netsec/netsec-sim-2006-01-dr-rahul-banerjee-bits-pilani-secure.pdf