IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A New Symmetric Key Encryption and Decryption Algorithm

Rajashri V.Hundekari
Assistant Professor ,
Department of Management and Computer Science,
Sangameshwar College, Solapur.

Abstract— Cryptography has gained importance in today's world. Cryptography is used by the means to prevent the unauthorized users from access of data. Cryptographic algorithms have been developed to prevent the attacks. A large variety of applications are being used in today's modern era such as online shopping , online payments etc .To protect these from serious attacks encoding and decoding mechanism has to be followed. A large variety of cryptographic algorithms are available today such as RSA, DES etc.The algorithm should consume less memory space and must be faster in terms of CPU execution. The algorithm must be complex for a cryptanalyst to break or read the text.

The new cryptographic algorithm proposed by us uses substitution and transposition method. The algorithm provides good performance and less implementation cost as it follows the base of private key encryption technique.

Keywords— Encryption algorithm, Decryption algorithm, RSA, DES, Substitution, Transposition.

I. Introduction

Encryption is the mechanism of converting the plain text into cipher text. Decryption is the mechanism of converting cipher text into plain text. For example if "abc" is plain text then after applying cipher key k=1, the cipher text which we get is"bcd". This is known as encryption. If we apply k=1 to cipher text then we get the plain text as "abc". This is known as decryption. Hence, Cryptography is a technique of secret writing.

Cryptography has been divided into several types as given:

1. Private Key Encryption or Symmetric Key Encryption

In this technique the same cipher is used to encrypt and decrypt the text .The sender and receiver share same key among them for the entire process.

For example : The sender wants to send plain text " hello" .He will apply cipher K=1 and will get cipher text "ifmmp" . The sender sends "ifmmp" to receiver. The receiver will decrypt it using K=1and he will obtain original plain text "hello".

This encryption method consists of:

Substitution method-

In this method the original character is replaced by new character. For example "abc" is original message. The substitution method will replace the characters after applying the cipher. The cipher text is "bcd"(K=1).

Transposition method-

In this method the positions of characters are interchanged. For example "abc" is original message. After applying the cipher (key=213) the cipher text is "bac".

2. Public Key Encryption or Asymmetric Key Encryption

In this technique the sender has a set of keys, private key and public key and the receiver has his set of keys, private key and public key .The private key is kept confidential by the user and public key is known to all. The sender encrypts the message using receiver's public key and sends it to receiver. The receiver decrypts the message using his own private key.

3. Hybrid Key Encryption

This technique is combination of private key encryption and public key encryption. The private key is faster and public key is secure. The sender sends the message using public key encryption method. The further communication is done using private key encryption technique. This method enjoys the benefits of both techniques.

II. Caesar cipher

The earliest & simplest use of substitution cipher was by Julius Caesar. This involves replacing each letter of alphabet with letter standing there place further down [1].

Plain text: a b c d e f g h i j k l m n o p q r s t .....z

Cipher text: d e f g h i j k l m n o p q r s t u v c

The drawback of Caesar cipher is that it allows repetition of alphabets and hence it is easier for cryptanalyst to break the text. To overcome this we have proposed this new algorithm.

Algorithm for Encryption

1. Read String,S.
2. Compute Length,L.
3. Apply Cipher Key=2 to S. If repetition of alphabet is found then compute distance from nearest neighbour (previous alphabet) and place it.
4.If L is odd, the last alphabet is kept unchanged and positions of every two alphabets from start are exchanged .
5. If L is even, positions of every two alphabets from start are exchanged.

Algorithm for Decryption

1. Read String,S.
2. Compute Length,L.
3. If L is odd, the last alphabet kept unchanged and positions of every two alphabets from start are exchanged .
4. If L is even, positions of every two alphabets from start are exchanged
5. Apply Cipher Key=2 to S. If repetition of alphabet is found then compute distance from nearest neighbour (previous) and decode.

Example for encryption: The message is "atharv" .The length of message is 6(even). By applying cipher(K=2) it will become "dwk2Duy" and position is interchanged "wd2Dkyu".

Example for decryption: The message is "wd2Dkyu".The length of message is 6(even).Position is interchanged and the text is "dwk2Duy".Apply the cipher and check for nearest neighbour if repetition found and message is decoded to "atharv".

II. Conclusions

The newly developed algorithm is faster and it is complicated to break for cryptanalyst as it uses combination of substitution and transposition method. It removes the repetition of characters from cipher text.

REFERENCES

[1] Sinkov, A. . Elementary cryptanalysis A mathematical approach.Washington, DC: the mathematical association of America, 1966.

[2] Delfs, Hans & Knebl, Helmut (2007). "Symmetric-key encryption". Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436.