Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Chetankumar Kamble, IJPRET, 2014; Volume 2 (9): 1066-1070 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A NEW APPROACH OF ENCRYPTION: MULTILEVEL ENCRYPTION TECHNIQUE

MR. CHETANKUMAR B. KAMBLE[1], DR. H. R. DESHMUKH[2], PROF. S. A. CHANDURE[3]

1. M. E. First Year, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
2. Prof and HOD, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
3. Asst. Prof, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Encryption is usually used to ensure information safety in today's data communication. The Multilevel Encryption technique comprises combination of one or more algorithm that produces only one cipher text. It is immune from cipher text search attack and or cipher text substitution attack, and allows cipher text to be decrypted. The objective of this technique is to achieve a secured file transfer on Internet. This paper proposes a theoretical aspect related with multi level encryption technique.

Keywords: Encryption, Decryption, Multi level encryption

PAPER-QR CODE

Corresponding Author: MR. CHETANKUMAR B. KAMBLE

Access Online On:

www.ijpret.com

How to Cite This Article:

Chetankumar Kamble, IJPRET, 2014; Volume 2 (9): 1066-1070

INTRODUCTION

Encryption is now commonly used in protecting information within many kinds of civilian systems. The most important application of encryption is in the banking and business data transaction, where the data security is the important issue. All of the users use the some encryption technique to hide the information from unauthorized person. But these techniques are might not so secure i.e. they are subjected to risk of being broken by the snoopers.

The Multilevel Encryption Technique serves as a solution on such problem. Multilevel encryption converts the data into such a strong cipher text which is almost impossible to break. By using this technique the data can be safely transmitted and received on the internet. In the multilevel encryption we can use any number of algorithms in series to make a multilevel algorithm.

Encryption:

Encryption is the process of converting information into an encrypted form, so that it is intelligible only to someone who knows how to 'decrypt' it to obtain the original message. It is commonly used in connection with electronic data whether stored on a computer or transmitted over an unsecured network such as the Internet. [2]

Decryption

It is exact reverse process of encryption; it is applied to the cipher text to extract the original data. In symmetric decryption the same key is used for decryption and in asymmetric decryption the receiver's private key is used for decryption.

Methods of Encryption:

There are two types of encryption i.e. symmetric and asymmetric encryption.

1.Symmetric:

Symmetric encryption also called as secret-key encryption means the same key is used to encrypt and decrypt data. On the other hand, symmetric encryption keys must be kept secure - you would need to make sure each person who needs the key gets it without any risk of compromise. [7]

Ex:

- Simple ciphers (e.g. a=1, b=2, etc.)
- DES (Data Encryption Standard) - uses 56-bit keys

- RC5(Rivest Cipher)

2.Asymmetric:

Symmetric encryption also called as public-key encryption means that you have one key for encryption i.e. a public key and another key for decryption i.e. a private key. [7]

Ex:

- RSA - Rivest, Shamir, and Adleman

Multilevel Encryption:

The Multilevel Encryption specifies many security algorithms as a chain and will be represented in a list. During encryption the data will be first encrypted using the first top level algorithm and the output of this algorithm, which is an encrypted content, is again encrypted using the second algorithm in the list and so on till the last algorithm in the list. This method of encryption makes the data very secured and hard to decode or decipher.

Literature Survey:

Methods, systems and computer program products are provided which encrypt a document by dividing the document into at least a first portion having a first security level and a second portion having a second security level. The document is then encrypted utilizing at least two encryption keys so as to encrypt the first portion of the document with a first of the at least two encryption keys and so as to encrypt the second portion of the document with a second of the at least two encryption keys [6] A Multi-level encryption scheme is provided for a wireless network. A first level of encryption is provided primarily for wireless communications taking place between a mobile terminal and an access point. In addition, a second, higher level of encryption is provided which is distributed beyond the wireless communications onto the system backbone itself [1].

Proposed Approach:

The current techniques which are available for encryption use only one particular algorithm which can be broken by snoopers, to overcome this problem it is proposed to introduce encryption technique which uses three algorithms which are connected in series i.e. multilevel encryption.

In Multilevel Encryption

- Use combination of both symmetric and asymmetric types of algorithms in series to make a multilevel of algorithm.

- The output of one algorithm will be Given to as an input to the next algorithm in series.
- This series of algorithm can be arranged in proper sequence depending upon the algorithm used.
- To achieve the maximum compatibility one has to arrange the series of algorithm depending on their types i.e. say in a series of three algorithms two of them are symmetric and other is asymmetric. So the series can be of first asymmetric and then two symmetric algorithms or first both symmetric and then asymmetric algorithm.
- In order to get original data, one has to decrypt in the reverse order of encryption i.e. start decryption with last algorithm.

In this multilevel encryption technique, three algorithms were identified for implementation.

- RSA (Rivest, Shamir, and Adleman)
- DES (Data Encryption Standard)
- RC5 (Rivest Cipher 5)

RSA

International Standards Organization list RSA as compatible cryptographic algorithm. This algorithm continues to be reliable and be used as long as factorization of large number proves to be difficult procedure [5]. Public keys can be freely distributed without worrying since it is only used to scramble the data. The sender doesn't need the recipient password to use his or her public key to encrypt data.

DES

The most widely used encryption scheme is based on the Data Encryption Standards (DES) adopted in 1977 by the National Bureau of Standards. Over the years there have been numerous attempts to find and exploit weakness in the algorithm, making DES the most studied encryption algorithm in existence. Despite numerous approaches, no one has so far succeeded in discovering fatal weakness in DES [4].

RC5

The RC5 encryption algorithm is a fast symmetric block cipher suitable for hardware or software implementation. RC5 has a variable word size, a variable number of rounds, and a variable length secret key. RC5 provide a variety of parameter setting so that user may select encryption algorithm whose speed and security are optimized for their application [3].

In Multilevel Encryption, it is proposed to introduce new technique by modifying above listed three algorithms. In this technique the first level algorithm is RSA, middle level is DES and the last is RC5.The user will specify the input to the first level algorithm i.e. RSA, this algorithm will encrypt the data and convert it into the cipher text. This cipher text is given to DES algorithm and then next to the RC5 algorithm. The user will need not to provide key i.e. password to algorithm for encryption and decryption.

CONCLUSION

The security to the data which is transmitted or shared on the internet between users plays a vital role. The Multilevel Encryption technique introduces a new way for encrypting the data which is very hard to decipher. The previously existing techniques or mechanisms for encryption and decryption have had fewer drawbacks and also advantages also. The proposed technique may be applied in varied application domain. Thus in future all important internet applications can be implemented using the Multilevel Encryption Technique.

REFERENCES:

1. Us Patent 6526506-Multilevel Encryption Access Point For Wireless Network By Daniel E Lewis.

2. Parliamentary Office Of Science And Technology Post Note October 2006 Number 270 Data Encryption.

3. "The Rc5 *Encryption* Algorithm" By Ronald L. Rivest. Mit Laboratory For Computer Science.

4. Network Security Essential *By William Stallings*

5. Rsa: Design And Practice By Marwa Nur Muhammad Http://*Mainline*.Brynmarw.Edu//Course/Cs330/Spring2008/Iimportantalgorithm/Mmuhammad (Rsa).Pdf

6. Us Patent 6598161 B1-Methods, Systems And Computer Programme Products For Multilevel Encryption By Karen Ruth Kluttz, Raleigh, Nc(Us); Sandeep Kishan Singhal, Raleigh, Nc(Us) Http://Itim.*Tamu*.Edu/Encryption/Types.Html