International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 3 (2013), pp. 125-130

http://www. irphouse.com /ijict.htm

An Approach to Improve the Data Security using Encryption and Decryption Technique

Anju[1], Babita[2], Reena[3] and Ayushi Aggarwal[4]

[1, 2, 3]CSE, Hindu College of Engineering, Haryana, India.
[4](CSE/IT Deptt.), Hindu College of Engineering, Haryana, India.

Abstract

Cryptography is an art and science. It is a playing major role in information and security division. The main aim of the cryptography is protecting the data from unauthorized users or hackers. "Cryptography is subject contains two parts one is encryption and another one decryption. Encryption is a process converting the plain text to cipher text using some keys. Decryption is a process of converting the cipher text to plain text using the keys". Cryptographic algorithms play a vital role in providing the data security.In the today's world, security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Encryption of data is an important topic for research, as secure and efficient algorithms are needed that allow optimized encryption and decryption of data. There are several algorithms in cryptography to encode and decode the data based on the key.The paper can give brief description about symmetric key algorithm and proposed new algorithm in symmetric key cryptography. The proposed algorithm contains two levels of Exclusive OR (XOR) operation. This algorithm is useful in transmission of messages and data between one user and another.

Keywords: Encryption, Decryption, Security, Symmetric and Secret key Cryptography.

1. Introduction

Cryptography is the study of Secret (crypto) -Writing (graphy).It is the science or art ofencompassing the principles and methods of transforming an intelligible message

intoone that is intelligible and then transforming the message back to its original form [4][8]. As thefield of cryptography has advanced; cryptography today is assumed as the study oftechniques and applications of securing the integrity and authenticity of transfer ofinformation under difficult circumstances.Today's cryptography is more than encryption and decryption. Authentication is asfundamentally a part of our lives as privacy.[3]The Author use authentication throughout oureveryday lives when The Author sign our name to some document and for instance and , as The Author move to world where our decisions and agreements are communicated electronically, The Author need to have electronic techniques for providing authentication. Cryptography providesmechanisms for such procedures.A digital signature binds a document to the possessor of a particular key, while a digitaltimestamp binds a document to its creation of a particular time. These cryptographicmechanisms can be used to control access to shared disk drive, a high securityinstallation, or a pay-per-view TV channel. The field of cryptography encompassesother uses as well. With just a few basic cryptographic tools[13], it is possible to buildelaborate schemes and protocols that allow us to pay using electronic money, to prove The Author know certain information without revealing the information itself, and to share quantityin such a way that a subset of the shares can reconstruct the set[12][15]. While moderncryptography is growing increasingly diverse, cryptography is fundamentally based onproblems that are difficult to solve. A problem may be difficult because its solutionrequires some secret knowledge such as decrypting an encrypted message or signingsome digital document.

2. Proposed Algorithm

It includes two parts:

1. Encryption Algorithm
2. Decryption Algorithm

Encryption Algorithm

Step1: Input the key randomly.
Step2: Convert the key to 16-bit binary format.
Step3: Construct the list for the prime no. then convert each number to the 16-bit binary format.
Step4: XOR the binary values of key and prime number.
Step5: Pick the characters one by one from the whole Data(Plain Text).
Step6: Convert the characters one by one to 16-bit binary format.
Step7: XOR the step4 resultant and Step5 resultant.
Step8: Result produced in step7 is divided in two parts including each of 8-bit value.
Step9: Put the decimal values for each 8-bit value and convert each value to Text format.
Step10: finally, cipher text is generated.

Decryption Algorithm

Step1: Convert the decimal values of cipher text into binary format selecting one by one.
Step2: Convert the cipher text to 16-bit binary format.
Step3: Construct the list for the prime no. then convert each number to the 16-bit binary format.
Step4: XOR the binary values of Cipher Text and prime number.
Step5: Enter the Key randomly.
Step6: Convert it to the 16-bit binary format.
Step7: XOR the step4 resultant and Step5 resultant.
Step8: Result produced in step6 is converted into decimal value.
Step9: Convert the decimal values to Text format.
Step10: finally, Plain text is achieved.

3. Analysis of Algorithms

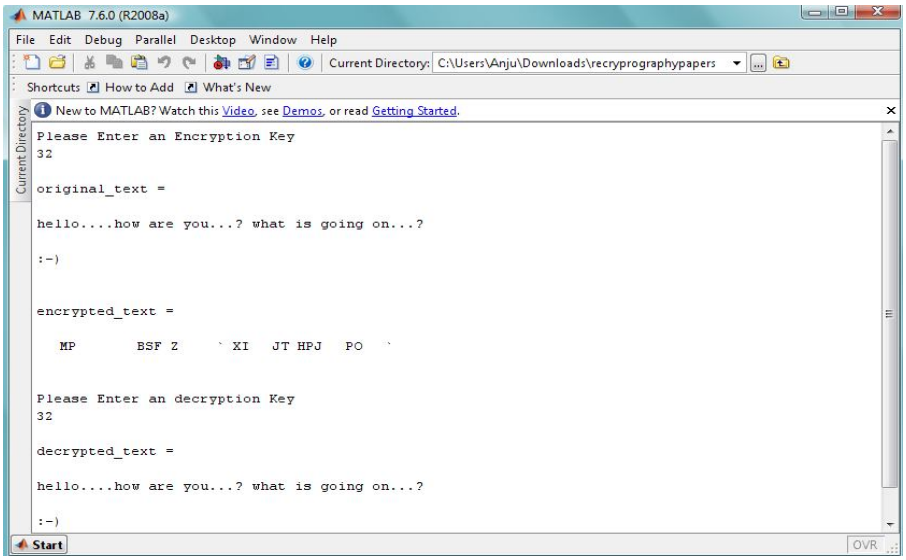

Fig. 1: Running implementation of the algorithm in MATLAB.

4. Programming Environment

MATLAB(**mat**rix **lab**oratory) 7.6.0.324(R2008a) is a numerical computing environment and fourth generation programming language developed by Mathworks, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms[3], creation of user interfaces, and interfacing with programs written in other languages, including C, C++, JAVA, Fortran. In 2004, MATLAB had around

one million users across industry and academia.MATLAB users come from various backgrounds of engineering, science, and economics. MATLAB is widely used in academic and research institutions as well as industrial enterprises. The MATLAB application is built around the MATLAB language, and most use of MATLAB involves typing MATLAB code into the Command Window (as an interactive mathematical shell), or executing text files containing MATLAB code and functions.

5. Conclusion

Cryptography protects users by providing functionality for the encryption of data and authentication of other users. This technology lets the receiver of an electronic message verify the sender, ensures that a message can be read only by the intended person, and assures the recipient that a message has not be altered in transit.This paper describes the cryptographic concepts of symmetric key encryption [1].

Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret [1][2]. The irony is that today, secrecy is not the key to the goodness of a cryptographic algorithm.Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well known and well-documented because they are also well-tested and well-studied. In fact, time is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one. The strength of cryptography lies in the choice (and management) of the keys; longer keys will resist attack better than shorter keys.

References

[1] PritiV. Bhagat, KaustubhS.Satpute, Vikas R. Palekar, ”*Reverse Encryption Algorithm: ATechnique for Encryption and Decryption*”, IJLTET, VOL. 2 ISSUE 1, JAN. 2013

[2] Cryptography and Network Security –By William Stallings, fifth edition.

[3] Dhanraj, C. Nandini, and Mohd. Tajuddin “*An Enhanced Approach for Secret Key Algorithm based on Data Encryption Standard*” International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 4, August 2011

[4] www.wikipedia.org.

[5] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with JayshreeUllal, senior VP of Cisco.

[6] YanWang, Ming Hu, Timing Evaluation of known cryptographic Algorithm, International Conference on Computational Intelligence and security, 2009.

[7] William stallings, Cryptography and NetworkSecurity:Principles & Practice II, second edition.

[8] SuyashVerma, RajnishChoubey, Roopalisoni “*An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security*” International Journal of Emerging Technology and Advanced Engineering Volume 2, Issue 7, July 2012.

[9] AndrewS.Tanenbaum, ”Computer Networks” forth edition, 2004.

[10] Sarker, M.Z.H., Parvez, and M.S., “*A Cost Effective Symmetric Key Cryptographic Algorithm for Small Amount of Data*” IEEE International Conference, 2005, pp. 1-6

[11] J. Freeman, R. Neely, and L. Megalo “*Developing Secure Systems: Issues and Solutions*”. IEEE Journal of Computer and Communication, Vol. 89, PP. 36-45. 1998.

[12] X. Lai and J. Massey, “*A proposal for a new block encryption stan-dard, ”* inAdvances in Cryptology—EUROCRYPT, I. B. Damgård, Ed. Berlin, Germany: Springer-Verlag, 1990, vol. 473, Lecture Notes in Computer Science, pp. 389–404.

[13] SolangeGhernaouti-Hélie, David Simms, IgliTashi, ”*Protecting information in a connected world:A Question of security and of confidence in security*”, International Conference on Network based Information System, 2011.