IGI PUBLISHING **ITB14885**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Web Services Security and E-Business**
edited by **G. Radhaman & G. S. V. Radha Krishna Rao**

Chapter XV

Generic Algorithm for Preparing Unbreakable Cipher: A Short Study

R. A. Balachandar, Anna University, India

M. Balakumar, Anna University, India

S. Anil Kumar, Anna University, India

Abstract

This chapter addresses the need of cryptographic algorithm to prepare unbreakable cipher. Though the performance of symmetric key algorithms is far better than asymmetric key algorithms, it still suffers with key distribution problems. It is highly evident that there is always a demand for an algorithm to transfer the secret key in a secure manner between the participants. This chapter argues that by providing the randomness to the secret key, it would be increasingly difficult to hack the secret key. This chapter proposes an algorithm effectively utilizes the random nature of stock prices in conjunction with plain text to generate random cipher. This algorithm can be used to exchange the secret key in a secure manner between the participants.

Introduction

The goal of the chapter is to assure a secure communication between the sender and the receiver. Nowadays, most of the transactions are held across the Internet, so providing security to such transactions is extremely important. Network security is the capability to send a message electronically from the client to the server in a secure manner, so that only the intended receiver receives the secret message. Even though many protocols were developed to ensure a secure communication between the participants, they all have their own pitfalls. All these protocols effectively utilize the various existing cryptographic algorithms. With this chapter, we are providing a new cryptographic algorithm that can be used to develop a secure protocol. This chapter also addresses the problem of providing randomness to the cipher text. Cipher text generated by the symmetric key cryptosystem is unique with the secret key and can be decrypted once the secret key is hacked by the intruder. If the secret key were changing randomly with some factors, then it would be extremely difficult to hack.

This chapter utilizes the stock prices of a stock exchange to provide randomness to the cipher. The stock price does not follow any pattern and is generated by forces driving the overall market place, various sectors (aerospace, retail, etc.) and the individual stock prices. Here, we proposed a detailed procedure to prepare random key by fusing the secret key with current stock price. With this random key, it is possible to obtain a random cipher that is highly unbreakable. This procedure can be used to exchange the secret key in a secure manner between the participants. The procedure discussed here utilizes the random stock prices in conjunction with the plain text to generate random cipher. The next section provides a brief description on the objectives of cryptography.

Objectives of Cryptography

Cryptography is the study of mathematical techniques related to the aspects of information security such as confidentiality, data integrity, authentication, and nonrepudiation (Schneier, 1996). Any secure system requires fulfilling all the four aspects.

Cryptographic algorithms are used to transform plaintext or a secret message into encrypted data in which the secret message is hidden (Stallings, 2000). The act of hiding the information is called encryption. The process of transforming the encrypted data back to the plaintext is known as decryption.

Cryptographic algorithms can be classified into two types:

1. symmetric key cryptosystem and
2. asymmetric key cryptosystem