Chapter 13
Encryption Techniques for Modern World

Uma Ramachandra Pujeri
MIT – World Peace University, India

Sharmishta Suhas Desai
MIT – World Peace University, India

Amit Savyanavar
https://orcid.org/0000-0001-6092-7017
MIT – World Peace University, India

ABSTRACT

Encryption is the process of converting confidential private data into unreadable form and securing information in the file from unauthorized access using various encryption algorithms. We live in the information age where the exchange of private information has become the integral part of our day-to-day activities. Billions of e-mails and business data are sent throughout the world through internet daily. The success of the information age is to keep private secure data from unauthorized access and key to access the private and secure data for authorized users. Encryption in this information age plays a vital role in the protecting the confidential data from unauthorized access. In the last few decades, the computer network has created a revolution in the use of information. Authorized users access their data or send their private data from anywhere in the world; hence, it has become very important to secure the private data not only where it is stored, but also to maintain high level of confidentiality while transmission of this private data from one machine to another.

DOI: 10.4018/978-1-5225-8458-2.ch013

INTRODUCTION

In today's digital world, billions of emails and pieces of business data are sent across the world via the Internet, which has provided an infrastructure for digital marketing, e-commerce, and online banking that allows money to flow through cyberspace. For example, according to estimates each day half of the world's gross domestic product (GDP) travels through the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network. Because authorized users need to access or send private data from anywhere in the world at any time, it has become crucial to not only secure private data where it is stored, but also to maintain a high level of confidentiality while transmitting such data from one machine to another. In that sense, computer security protects the integrity of information systems. Critically, the success of such activities depends on the ability to protect information as it flows around the world, in a process that relies upon the power of cryptography. By definition, *encryption* is process of converting private, confidential data to unreadable form or concealing private, secure information in the file from unauthorized access by using various encryption algorithms. Today and for the foreseeable future, encryption plays and will play a vital role in protecting confidential data from unauthorized access.

Goals of Information and Data Security

The goals of securing online information and data are threefold: confidentiality, integrity, and availability. Whereas confidentiality is needed in the protection of private data from unauthorized access, integrity is needed in changes made by authorized entities via authorized mechanism. Last, availability is necessary for information created by organizations or users that should be available to authorized entities at anytime and anywhere.

Although computer security ensures the protection of confidential data, computer and network security present major challenges. For one, designing security algorithms is complex as algorithms must consider all possible attacks on security features. To that end, security mechanisms in computer and network systems require constant monitoring. Accordingly, security is an integral to designing algorithms and maintaining them after their implementation. Moreover, managing private data in mobile networks presents the challenge of ensuring the confidentiality of data. Among threats to such confidentiality are internal threats, including when members of organizations inject malware or viruses into local organizational area networks in order to access the confidential data of their organizations.

To ensure the security of private data, cryptography is often used to conceal the contents of messages containing such data by enciphering them. The general aim of this chapter is thus to clarify various encryption and mathematical algorithms that can be applied to prevent unauthorized users (e.g., hackers) from accessing the private data of network users. Once such algorithms are clarified, we present the design of an advanced encryption algorithm using certain mathematical algorithms to facilitate such prevention efforts. In this chapter, we discuss how data encryption plays a vital role in day-to-day life, as well as different mathematical techniques needed to generate ciphertext. Then, we address the design of the Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Afterwards, we explain elliptic curve cryptography (ECC), then we will define and test our hypothesis. Last, we conclude the chapter by addressing the past and future of encryption.