Chapter X

Cryptography: Deciphering Its Progress

Leslie Leong
Central Connecticut State University, USA

Andrzej T. Jarmoszko
Central Connecticut State University, USA

Abstract

The emphasis and increased awareness of information security require an understanding and knowledge of the technology that supports it. As the risks and complexity of security keep growing along with the development of the Internet and e-commerce, securing information has become of utmost importance. With the worries about cyber-terrorism, hackers, and white-collar crimes, the demand for a stronger security mechanism in cryptography becomes apparent. Although wireless cryptography is still in its infancy, there are encryption technologies that may support the limitations of a mobile device.
Introduction

Protecting information has always been a great concern. Securing information can be accomplished through cryptography and an encoding process that is analogous to encryption. Both terms will be used interchangeably throughout this chapter. Cryptography is not a product of the modern technological age. In fact this technique has been known and applied for centuries to intelligently and mathematically scramble messages. Historical evidence reveals cryptography that dates back to ancient periods. In 1900 B.C. an Egyptian scribe used non-standard hieroglyphs in an inscription (Ellison, 2001). Julius Caesar’s troops used it to communicate with each other from unsafe distances apart (Ackerman, 1999). The Caesar-shift substitution cipher is one of the easiest encryption techniques (Davis & Bennamati, 2003). Cryptography did not begin to advance into the powerful ciphering tool that it is today until the 20th Century. In the 1920s, cryptography and cryptanalysis became popular with governments (Ellison, 2001). During World War II, German forces used an encrypting machine called Enigma. It was constructed using mathematical and technological advances that were available at the time (it was cracked by three Polish mathematicians and provided valuable information to the Allied forces). Until the mid-1990s ciphering text was primarily a focus of national security, but with the emergence of electronic commerce, the private sector expanded its implementations. Typical Internet transactions require parties to exchange valuable personal and financial information via communications channels. To ensure protection of the exchanges, many companies turned to cryptography. This chapter will focus on the structure of private-key and public-key encryption methods. It will look at specific examples of security validations, the legal aspects regarding export controls, and finally explore the emerging technologies in wireless cryptography.

Cryptography

“Cryptography, from the Greek kryptos (‘hidden’) and graphein (‘to write’), is defined as the creation of systems to render a message unintelligible to unauthorized readers. Cryptanalysis, in contrast, is the practice of breaking codes, usually when the key is not known. Cryptology is the study of the two disciplines.” (Petras, 2001, p. 689)
11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/chapter/cryptography-deciphering-its-progress/23351?camid=4v1


www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

Security Issues for Cloud Computing

www.igi-global.com/chapter/security-issues-cloud-computing/62720?camid=4v1a

Flawed Security of Social Network of Things

www.igi-global.com/chapter/flawed-security-of-social-network-of-things/201605?camid=4v1a
[www.igi-global.com/article/hazmat-transport-safety-and-alternative-transport-modes/177837?camid=4v1a](www.igi-global.com/article/hazmat-transport-safety-and-alternative-transport-modes/177837?camid=4v1a)

Personal Information Ethics
[www.igi-global.com/chapter/personal-information-ethics/13519?camid=4v1a](www.igi-global.com/chapter/personal-information-ethics/13519?camid=4v1a)