A Comparative Survey on Cryptology-Based Methodologies

Allan Rwabutaza, ATR Center, Wright State University, USA

Ming Yang, Southern Polytechnic State University, USA

Nikolaos Bourbakis, ATR Center, Wright State University, USA

ABSTRACT

Security is an important issue related to the storage and communication of data and information. In data and information security, cryptography and steganography are two of the most common security techniques. On one hand, there is cryptography, which is the secret communication between two parties by message scrambling on the sender's side and message unscrambling on the receiver's side so that only the intended receiver gets the secret message. Cryptography and cryptanalysis constitute cryptology (or crypto) while steganography and steganalysis make up steganology (or stegano). This paper presents a comparative survey of various cryptology and steganology techniques by analyzing and comparing different methodologies using a set of predefined parameters. It also offers to the reader valuable knowledge on the state of the art techniques used on cryptanalysis.

Keywords: Cryptanalysis, Cryptology, Date Information Security, Security Techniques, Steganalysis

INTRODUCTION

Cryptography is the secret communication between two parties by message scrambling on the sender's side and message unscrambling on the receiver's side. An unintended interception of the message reveals a scrambled message, which is useless to the attacker. If an attacker undoes this process by unscrambling the intercepted unintelligible message to get the intelligible message, then we get *cryptanalysis*, which is the reverse engineering of cryptography (Jacobs, 2011; Gebbie, 2002; Nguyen & Stern, 2001; Cheddad, Condell, Curran, & McKevitt, 2010; Nemati & Yang, 2011). Cryptography and cryptanalysis both constitute cryptology. Since cryptanalysis works against cryptography, the second section of the paper will look at cryptography, the third will focus on cryptanalysis and the fourth will be on the works of contemporary cryptologists.

DOI: 10.4018/jisp.2012070101

Basic Cryptology Concepts

Cryptography is the process where an individual or party sends a message to another individual or party in a scrambled unintelligible manner such that only the intended party will get the scrambled message, which will be unscrambled to get the original message. The reverse engineering of cryptography is known as cryptanalysis. Cryptography and cryptanalysis together constitute cryptology.

A cryptography system is known as a *cryptosystem*, or a *cipher*. Any cryptosystem must have a sender, plaintext, an enciphering (encrypting) function, an enciphering (encrypting) key, an algorithm, ciphertext, a transmission medium, a decrypting (deciphering) function, a decrypting (deciphering) key and a receiver (Figure 1).

Plaintext is the original intelligible message a *sender* sends to the *receiver*. In order to scramble the plaintext to make it unintelligible to the potential attacker, an *algorithm,* along with a *key,* maps the plaintext to the unintelligible message known as *ciphertext*. This plaintext to ciphertext scrambling is known as *enciphering*. An algorithm is a mathematical function that maps one message to another message. A key is a variable that gives a unique output map when used with an algorithm. In enciphering, the function is referred to as *an enciphering function* and the key is referred to as *an enciphering key.* After encryption, the ciphertext is sent through a transmission medium to the receiver. When a receiver receives the ciphertext, he reverses the encryption to get the original plaintext. This reversing is referred to as *deciphering*. A *deciphering function* and a *deciphering key* are synonymous to their corresponding counterparts in encryption.

CRYPTOGRAPHY

Types of Cryptography

There are two types of cryptography: Symmetric (private or secret) key cryptography and Asymmetric (public or shared) key cryptography. In symmetric key cryptography, the same key is used to decrypt and encrypt the message. While

Figure 1. A cryptosystem