Chapter 65
Computational Intelligence in Cryptology

Wasan Shaker Awad
Ahlia University, Bahrain

El-Sayed M. El-Alfy
King Fahd University of Petroleum and Minerals, Saudi Arabia

ABSTRACT

Computational intelligence (CI) has attracted the attention of many researchers for its effectiveness in solving different kinds of problems. It has been applied to solve problems in a wide area of applications. The aim of this chapter is to present an overview of existing literature about the applications of CI in cryptology. It demonstrates and studies the applicability of CI in cryptology. The problems examined in this chapter are the automated design of cipher systems, and the automated cryptanalysis of cipher systems. It has been shown that CI methods, such as genetic algorithms, genetic programming, Tabu search, and memetic computing are effective tools to solve most of cryptology problems.

INTRODUCTION

Cryptology problems, such as designing good cryptographic systems and analyzing them, attracted many researchers, and hence we can find in the literature different techniques and methods that have been proposed to solve these problems. In recent years, many algorithms that take advantage of approaches based on computational intelligence (CI) techniques have been proposed, and there is a growing interest toward CI techniques because of these recent successes. However, there still are a number of open problems in the field that should be addressed.

In this chapter, the most important achievements in solving information security related problems using CI are presented. The main objective is to investigate the application of various CI techniques in the fields of automated cryptanalysis and automated cryptographic function generation (cipher systems design), to demonstrate the applicability of CI in solving these problems, and to give interested researchers an overview of emerging methodologies and new directions in cryptosystems as the heart of information security.

DOI: 10.4018/978-1-5225-1759-7.ch065

According to our research, several works have been found that considered the applications of CI to cryptographic problems; these techniques include Genetic Algorithms (GA), Simulated Annealing (SA), Tabu search, Ant Colony Optimization (ACO), Artificial Neural Networks (ANN), and DNA. Moreover, a number of authors gave surveys of cryptographic applications, such as designing different types of cipher systems (RSA hardware, S-Boxes, and key-stream generators) in addition to attacking cipher systems, that can be developed by using CI methods (Clark, 1998; Volná, 2000; Isasi and Julio, 2004; Isasi, 2005; Xiao et al., 2006; Laskari, et al. 2007; Anam et al., 2010; Picek and Golub, 2011; Danziger and Henriques, 2011; Zhang and Fu, 2012; Cherian et al. 2013). It has been concluded that CI techniques show potential for use in the field of automated cryptology, some promise when used to optimize existing methods for attacking certain ciphers, and CI is very effective for problems which require searching a large solution space for solutions with good characteristics. In addition, CI techniques can help to create ciphers that are more robust. However, the problem formulation and representation, and the proper definition of the fitness function have a great effect on the performance of CI methods in cryptography. In this chapter, a more comprehensive survey is presented.

In the next section, the core concepts of cryptology are first reviewed briefly. Then, the third and fourth sections discuss the CI-based methods for designing and attacking different classes of cryptographic systems.

OVERVIEW OF CRYPTOLOGY

The growth in computer systems, and computer communication and networking has increased the dependence of organizations on the information stored, processed, and communicated using these systems. This, in turn, has led to a heightened awareness of the need to security. Security is the quality or state of being secure, to be free from danger and to be protected from adversaries. Information security is the process of protecting information from unauthorized access, use, disclosure, destruction, or modification. One of information security goals is confidentiality, which is probably the most common aspect of information security. It is about protection of confidential information. An organization needs to guard against malicious actions that endanger the confidentiality of its information. Attacks threatening confidentiality are snooping and traffic analysis. The confidentiality goal can be achieved by applying encryption mechanism (Stalling, 2006).

A lot of work has been done in cryptology. Cryptology is the study of the encryption techniques to protect data and the techniques to attack the encryption techniques. Thus, it is combination of two areas: cryptanalysis and cryptography, where cryptanalysis is the study of the techniques used for breaking cryptographic (cipher) systems, and cryptography is the science of protecting private information against unauthorized access by encrypting it.

Any cryptographic system (cryptosystem, or cipher system) has five elements: plaintext (clear text), ciphertext (encrypted text), encryption algorithm which is a procedure used to encipher (encrypt) the plaintext and transform it to ciphertext, decryption algorithm which is the inverse of the encryption algorithm, and the key which is a parameter used to prevent the plaintext from being easily revealed by an authorized person (Schneier, 1996; Stalling, 2006).

Nowadays, you can find different kinds of cipher systems (cryptosystems), used for encrypting the private information. A number of cipher systems have been proposed with different levels of security. Choosing among cryptographic alternatives a critical and sensitive decision. In these situations, there is