Chapter 11
Applicability of Cellular Automata in Cryptanalysis

Harsh Bhasin
Jawahar Lal Nehru University, India

Naved Alam
Jamia Hamdard, India

ABSTRACT

Cryptanalysis refers to finding the plaintext from the given cipher text. The problem reduces to finding the correct key from a set of possible keys, which is basically a search problem. Many researchers have put in a lot of effort to accomplish this task. Most of the efforts used conventional techniques. However, soft computing techniques like Genetic Algorithms are generally good in optimized search, though the applicability of such techniques to cryptanalysis is still a contentious point. This work carries out an extensive literature review of the cryptanalysis techniques, finds the gaps there in, in order to put the proposed technique in the perspective. The work also finds the applicability of Cellular Automata in cryptanalysis. A new technique has been proposed and verified for texts of around 1000 words. Each text is encrypted 10 times and then decrypted using the proposed technique. The work has also been compared with that employing Genetic Algorithm. The experiments carried out prove the veracity of the technique and paves way of Cellular automata in cryptanalysis. The paper also discusses the future scope of the work.

1. INTRODUCTION

One of the most important factors responsible for the development of human race is the ability to communicate. The development and the design of communication system has become one of the most contentious issues. The security of communication is, therefore, one of the most essential attributes in any communication system. The development in the field of cryptography has helped achieve the dream of a secured communication. However, the system becomes vulnerable in one of the following cases. The intruder might want to 'listen' to the communication, which is referred to as eavesdropping. The

DOI: 10.4018/978-1-7998-1763-5.ch011

intruder might want to change data or worse might use it for some other purpose. A sound cryptography technique prohibits any of these. One of the easiest methods of cryptography is to apply XOR function on the data (plaintext) and key. The resultant is referred to as cipher-text. The key when XOR-ed with the plaintext again produces plaintext (Bruce, 1995; & Rothe, 2002). The soundness of a system, though, is not easy to ascertain. The breakability of the key can be one of the major factors in determining the goodness of a system.

One of the ways of doing so is to find how good a system is to diversified attacks. Given the cipher-text, the process of finding the plaintext is referred to as Cryptanalysis. Cryptanalysis has been one of the most researched topics in the field of Network Security. Various researchers have devised different methodologies to accomplish the task. Owing to the importance of the topic, it is therefore necessary to carry out an extensive literature review of the techniques and find the gaps therein. The review is also important to justify the applicability of soft computing techniques, especially Cellular Automata (CA), to handle the problem. The work intends to achieve the above goals.

The goals of this paper are as follows.

- To carry out a literature review of cryptanalysis using soft computing
- To find the gaps in the existing techniques
- To propose a technique using CA
- To verify and validate the technique

The paper has been organized as follows. The second section explains the literature review, the third section explains the concepts of CA, the fourth section explains the proposed work, the fifth section gives the results and the last section concludes. The work paves way of CA in cryptanalysis.

2. LITERATURE REVIEW

Cryptography is one of the most researched topics in Computer Science. The topic is not only important in securing essential data from eavesdropping and theft but has also been used to win wars. The power of cryptography was demonstrated in World War II. Cryptanalysis is the crafting of key, given a set of data and corresponding encrypted code. The researchers developed many models for cryptanalysis during the Second World War. These models proved instrumental in proving a strategic edge to Britain. The development in the field continued there-after, when the world was divided into two groups, both wanting to gain as much information as possible from the other. The turn of events would remind the fraternity of the importance of the cryptography. The breaking of PURPLE by William Friedman, breaking of ENIGMA by Alan Turing, problems faced in accessing the contents of Bin Laden's drive was the constant reminders of the importance of this topic.

The conventional techniques of Cryptanalysis include frequency counts, in order to ascertain the most frequently used syllabi. The use of letters and words in English gives a cue of what to expect from a given text. Another technique of cryptanalysis uses the study and analysis of patterns. Some of the researchers have used side chain attacks for accomplishing the above task but the method works only in constrained environment.