ABSTRACT

When Julius Caeser sent messages to his generals, he did not trust his messengers. Therefore, he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only some one who knows the "shift by 3" rule could decipher his messages. Therefore, it has begun.

Throughout history, people have felt a need to keep some information secret to others. Cryptography is the art of constructing cipher systems and it has been used for many thousand years to hide information during storage and transmission. Those who are not intended to get the information are of course interested in knowing the secret information anyway and will then engage in cryptanalysis to try to break the cipher. For that, There is a constant struggle between the makers and the breakers of cipher systems since once a new cipher has been constructed it will be under attack and if it is broken, a new cipher needs to be constructed. The use of ciphers was until 30 (or so) years ago more or less restricted to the military and governments. After that, cryptography has been presented and made accessible to the public, which has led to a growing interest in this fascinating subject. Nowadays cipher systems are used in many places in the modern society, e.g. ATM machines, digital television, Internet shopping etc. This has increased the need to research into cryptology, which is the scientific study of cryptography and cryptanalysis.

The basic idea of a cipher is to provide two operations, encryption and decryption. The first transforms a plaintext into something unintelligible called a ciphertext and the other inverts this transformation and returns the plaintext. Both operations are functions that depend on an additional input called the key. Cipher systems can be classified into groups based on how they are constructed. In some systems, the same key is used for both encryption and decryption. These are said to be symmetric ciphers whereas asymmetric ciphers have different keys for the two operations. In symmetric cryptography, there are two main concepts: stream and block ciphers. Whilst a stream cipher encrypts one character at a time with a time varying transformation, a block cipher encrypts a group of

characters using a fixed but more complex function. The main objective of this thesis is to evaluate the two different cipher techniques (stream and block ciphers) to provide a measure of the cryptographic strength of each technique as well as to provide parameters for their comparison.

In general, the evaluation criteria for different types of cryptosystems are not completely defined. Under this work, general evaluation criteria for secret-key cryptography are introduced. For the block cipher, the statistical random tests are the most important criteria by which the block cipher can be evaluated. Statistical random tests are also part of the evaluation criteria employed to evaluate the stream cipher.

Keywords: Stream Cipher, Block Cipher, Evaluation Criteria, Random Tests