Chapter VIII
Cryptography

Kevin Curran
University of Ulster, UK

Niall Smyth
University of Ulster, UK

Bryan Mc Grory
University of Ulster, UK

ABSTRACT

One of the main methods of security is cryptography encrypting data so that only a person with the right key can decrypt it and make sense of the data. There are many forms of encryption, some more effective than others. Cryptography works by taking the original information and converting it with ciphertext, which encrypts the information to an unreadable form. To decrypt the information we simply do the opposite and decipher the unreadable information back into plain text. This enciphering and deciphering of information is done using an algorithm called a cipher. A cipher is basically like a secret code, but the main difference between using a secret code and a cipher is that a secret code will only work at a level of meaning. This chapter discusses a little of the history of cryptography, some popular encryption methods, and also some of the issues regarding encryption, such as government restrictions.

INTRODUCTION

The art of cryptography reaches back as far as 1900 BC, when an Egyptian scribe used a derivation of hieroglyphics to communicate. Throughout history, there have been many people responsible for the growth of cryptography. Many of these people were quite famous and one of these was Julius Caesar. He used a substitution of characters and just moved them about. Another historical figure who used and changed cryptography was Thomas Jefferson. He developed a wheel cipher that was made in 1790. This cipher was then to be used to create the Strip cipher, which was used by the U.S. Navy during the second World

War. During World War II, several mechanical devices were invented for performing encryption, this included rotor machines, most notably the Enigma cipher. The ciphers implemented by these machines brought about a significant increase in the complexity of cryptanalysis. Encryption methods have historically been divided into two categories: substitution ciphers and transposition ciphers. Substitution ciphers preserve the order of the plain-text symbols but disguise them. Transposition ciphers, in contrast, reorder the letters but do not disguise them. Plain text is the common term for the original text of a message before it has been encrypted (Cobb, 2004). In this chapter, we discuss a little of the history of cryptography, some popular encryption methods, and also some of the issues regarding encryption, such as government restrictions.

BACKGROUND

Possibly the earliest encryption method was developed by a Greek historian of the 2nd century BC named Polybius, and it is a type of substitution cipher (Burgess, Pattison, & Goksel, 2000). This method worked with the idea of a translation table containing the letters of the Greek alphabet. This was used for sending messages with torch telegraphy. The sender of the message would have 10 torches, five for each hand. He would send the message letter by letter, holding the number of torches representing the row of the letter in his left hand, and the number of torches representing the column of the letter in his right hand. For example, in the case of the letter "s," the sender would hold three torches in his left hand and four in his right hand. Polybius wrote that "this method was invented by Cleoxenus and Democritus but it was enhanced by me" (Dénes, 2002, p. 7). This method, while simple, was an effective way of encrypting telegraphic messages. The table could easily be changed without changing the method, so as long as both the sender and receiver were using the same table and no one else had the table they could send messages that anyone could see being sent, but which would only be understood by the intended recipient. This is a form of private key encryption—where both the sender and the recipient share the key to the encrypted messages. In this case, the key is the letter table.

Another type of substitution cipher is the Caesar cipher, attributed to Julius Caesar (Tannenbaum, 1996). In this method, the alphabet is shifted by a certain number of letters; this number being represented by *k*. For example, where *k* is 3, the letter A would be replaced with D, B would be replaced with E, Z would be replaced with C, and so forth. This is also a form of private key encryption, where the value of *k* must be known to decrypt the message. Obviously this simple form of encryption is not difficult to crack, with only 26 possible values of *k*; it is only a matter of shifting the encrypted message with values of *k* until you get a comprehensible decrypted message. There are also more complex methods of cracking this encryption, such as using letter frequency statistics to work out some likely letters from the message. For example, E is the most common letter in the English language, so the most common letter in the encrypted message is likely to be E. Replacing the most common letters in the encrypted message with the most common letters of the language may help to make sense of some words. Once a word is partially decrypted, it may be easy to guess what the word is, which will then allow more letters to be substituted with their decrypted versions. For example, if E and T had been used to replace the most common letters and one of the partially decrypted words is "tXe," then the X is likely to be H forming the word "the," so replacing all occurrences of X in the message with H may provide some more words that can be guessed easily (Garrett & Lieman, 2005).

A common transposition cipher, the columnar transposition, works with a private key. The private key is a word or phrase not containing any repeated letters, for example, "HISTORY." This key is used to number columns, with column 1 being under the letter closest to the start of the alphabet and so forth. The plain text is written in rows under the key, and the encrypted text is read in columns, starting with column 1. An example is shown in Figure 1.