Data Encryption using Ciphers

Information Security: CPTR-2800

Adam Giunta

Becker College

Abstract

Data Encryption using Ciphers

Data encryption is a hugely diverse branch of computer science that is the backbone for all computer security. When computers first started becoming mainstream for big businesses and wealthy people, it was clear that some sort of method for protecting data would be needed. Computer data is arranged in bytes, which is an 8-character long sequence of binary digits. Because of data’s inherent mathematical nature, applying different kinds of ciphers would prove to be a simple feat. Using a program written by myself, we will explore a couple of different basic ciphers used early during adoption of data encryption.

**Background**

While still a young research topic, many historians agree that some sort of early cryptography was being used a few thousand years ago. One piece of evidence suggests that an early form of cryptography was used in ancient Egypt around 1900 BC. The method was used by the Egyptian nobleman, Khnumhotep II. The inscriptions on the walls of the main chamber of his tomb used some unique and unusual glyphs that are said to have some sort of secret meaning. While historians are unsure of the true purpose of the hieroglyphics, they stand to be one of the earliest pieces of evidence for the use of cryptography.

**The Cesar Shift Cipher**

The Cesar Shift Cipher, or simply the Cesar Cipher, is an early text encryption technique that substitutes each letter in a message as another letter a set distance along the alphabet. Each letter in the alphabet would be assigned a numeric value corresponding to its position in the alphabet, and each letter in the message would be changed so that it is equal to the letter of the alphabet after adding an amount to the original letter’s position equal to the shift amount. If a letter is close to the end of the alphabet and the shift sets a position not in the alphabet, the order is wrapped so that these letters become ones from the beginning.

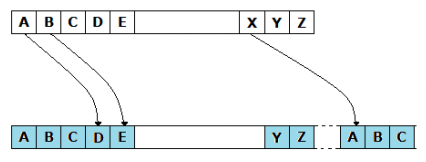
 Typically, the Cesar Cipher has a shift distance of three or four letters. This cipher was used in ancient Rome during the rule of Julius Cesar around 100 BC; hence the name.

Figure : A Cesar Cipher with a shift value of 3 in action

**C# and Unicode**

Fast-forward to 1984 and the advent of the Unicode Consortium. The Unicode Consortium was established to create a standard, universal collection of 16-bit codes for every symbol to be displayed on a computer screen. Similar to how the Cesar Cipher assigns every letter a number, Unicode is a unique 16-bit binary code that is assigned to every usable symbol in a computer’s operating system.

<https://www.unicode.org/history/summary.html>

<https://access.redhat.com/blogs/766093/posts/1976023>