Enigma Slide Rule Cipher

The enigma slide rule cipher utilizes classic Vigenere polyalphabetic substitution logic in an easy to use yet very secure manner. The liner design also incorporates the use of numbers, special characters, and punctuation. These are rarely seen in ciphers, but they are useful features that can make encoding messages much faster and clearer.

Ciphers have been needed for thousands of years to send secret messages. Numerous schemes have been developed to make these messages secure. Nearly all ciphers use some sort of substitution methodology. A single substitution cipher where an encoded letter always represents the same text letter can be fairly easy to solve using frequency analysis techniques. However, by using key words or key phrases any encrypted letter will change within the message to represent a wide range of possible text letters. The more complex the keyword or keyphrase, the tougher the message is to crack. The Enigma Slide Cipher illustrates the use of this technique in an easy to understand and easy to encode way.

Inspiration for this design came from the 1939 Dick Tracy Secret Code Maker built by Lawrence Engineering. Encoded messages are also written in blocks of 4 letters. This greatly increases the complexity as it makes discerning word lengths impossible for the person attempting to crack the code.

Union Army Cipher

Used for the encryption of messages of the Union Army during the American Civil War (1861-1865). It was a system primarily used for flag signals where there was a line of sight or for encrypted morse code messages. Each Union Army Cipher has a unique serial number.

The letters A.J.M. on the disk are for Albert J Meyer, the inventor and Chief Signal Officer of the Union Army. His system was called Flag Telegraphy or “Wigwag”.

The Union Cipher Disk was primarily used for flag signaling during the American Civil War. The numbers on the outside of the disk would go along with a certain motion of the flag. For example, when signaling a 1, you may wave the flag left, and to signal an 8 you would wave the flag to the right. In some versions of this disk, the numbers 1 and 2 were used, but 2 was later replaced with 8 so that the numbers could be more easily read from any direction. There was a third flag signal which was represented by waving the flag or torch from above the head downwards in front of the flagman. A common use of this was to signal end of letter, word, or end of sentence.

This cipher allowed military personnel within view of each other to communicate using flag or torch signals, even if they have never actually met, as long as they have the same disk and keys to reference. This cipher method can also be used for telegraphs and Morse code. The 1 and 8 would represent the long and short sounds.

Confederate Army Cipher

Use for the encryption of secret messages of the Confederacy during the of the Confederacy during the American Civil War (1861-1865). It was originally created by Francis LaBarre, a gold and silver worker, in Richmond, VA. And was based on the Vigenere Cipher.

The smaller disc carries the text **CSA SS**. The **CSA** stands for Confederate States of America and the **SS** stands for Signal Service. Not many real Confederate Cipher Discs survived and there are only five known to exist today. Two of these are in the hands of private collectors, one is part of the collection of the Smithsonian Institute and two are at the Museum of the Confederacy in Richmond (Virginia, USA).

Mexican Army Cipher

The cipher was state of the art during the time of conflict between Mexico and the USA shortly before World War I. It uses 5 disks that convert letters into 2 digit numbers based on a key that is used to initially set the wheels.

Alberti Cipher

The Alberti Cipher Disk was invented over five centuries ago by the famous Italian scholar Leon Battista Alberti in 1647. Alberti was an amazingly brilliant Renaissance genius whose talents covered a wide range of fields. He was a renowned architect, a dedicated linguist, a Latin language expert, a poet, a priest, a philosopher, an educated lawyer, an astounding mathematician, an engineer, author, astronomer, a master horseman, and a cryptographer! The Alberti Cipher Disk is the first example of a true "polyalphabetic" cipher device using two dissimilar alphabets.

The Alberti Cipher Disk consists of two disks, the stationary outer, originally called by Alberti – the "Stabilis", and the rotating inner – which he named the "Mobilis". The outer disk is called the "plain text" disk and it is where you find the symbols you wish to encode. It is made up of 24 symbols consisting of 20 upper case letters and 4 numbers. The six letters missing are H, J, K, U, W, and Y. The Inner disk is called the "cipher disk", and is made up of 24 symbols as well. These consist of 23 lower case letters and the ampersand sign. The three letters missing are J, U, and W. Letters are missing because the disk was designed to be used with the 15th century Latin language and Alberti removed H, K, and Y because he felt they were unnecessary.

Jefferson Cipher Wheel

While serving as George Washington's secretary of state (1790-1793), Thomas Jefferson devised an ingenious and secure method to encode and decode messages: the cipher wheel. During the American Revolution, Jefferson had relied primarily on messengers to hand-carry sensitive letters, but codes became an essential part of his correspondence when he was

America’s minister to France (1784-1789) since European postmasters opened and read all letters passing through their command.