

The History of the Cypher Wheel

The Cypher Wheel, sometimes called the Cipher Wheel or Cipher Disk, was invented by Leon Battista Alberti (February 14, 1404 – April 25, 1472) an Italian author, artist, architect, poet, linguist, philosopher, and cryptographer. He was born in Genoa, Italy, the son of a wealthy merchant of Florence, Lorenzo Alberti.

Alberti was an cryptographer of the highest standard of his time, inventing the first polyalphabetic cipher. The polyalphabetic cipher was the most important advance in cryptography since before the time of Christ. Cryptography historian David Kahn has called him the "Father of Western Cryptography", and says there are three significant advances in the field of cryptography which can be assigned to Alberti: "the earliest Western exposition of cryptanalysis, the invention of polyalphabetic substitution, and the invention of enciphered code" (David Kahn (1967). *The codebreakers: the story of secret writing*. New York: MacMillan.).

Alberti made history by employing the first mechanical device aiding in the encryption process. His cipher disk is made of two circular copper plates, one on top of the other. The larger outer wheel is called the stationary disk, and the smaller inner wheel is called movable disk. The plates are divided into equal portions that contain the letters of the alphabet in their normal order. This device is known as the Alberti Cipher or Albert Cipher Disk.

During the Civil War the Confederate army used a simple two disk cipher wheel to code messages. The cipher disk was made of brass and measured just two and a quarter inches across, so small it would easily fit into your shirt pocket. There are only five Confederate Cipher Disks in existence today. Two are in the Museum of the Confederacy in Richmond, Virginia, one is in the Smithsonian Institution, and two are in private collections. They were probably made sometime after 1862 by an unknown designer and manufacturer. The letters CSA are stamped on the face of the disk and below that the letters SS. CSA stands for Confederate States of America and the SS is believed to be either Secret Service or Signal Service. In Washington D.C. the Union codebreakers in the telegraph office broke the CSA coded messages, encrypted using this cipher system, largely due to the poor techniques employed by the CSA operators.

The cipher disk was used in the field by the U.S. Army Signal Corps at the beginning of World War I. The disk enabled messages to be quickly encrypted with a simple substitution cipher by rotating the inner ring to create a code. However, later in the war more complex devices were employed to escape the aggressive deciphering techniques of the enemy.