CC 1.10 Cipher Disks

The Mexican Army Cipher Disk is a cryptographic tool used for encoding and decoding messages, predominantly in the late 19th and early 20th centuries. The device consists of two rotating disks, usually made of brass, with alphabets or numbers around their edges. By aligning the disks in a specific way, the user can encode or decode a message.

I found two resources on the Mexican Army Cipher Disk:

Fagin, B. (2018). Mexican Army Cipher Disks: A Historical Survey and How to Make One. Cryptologia, 42(3), 201-214. doi: 10.1080/01611194.2017.1414336

Singh, S. (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books.

The Mexican Army Cipher Disk was primarily used during the Mexican Revolution (1910-1920), though its usage can be traced back to the 1860s (Fagin, 2018).

Cryptographic weaknesses of the Mexican Army Cipher Disk include:

Susceptibility to frequency analysis: As it is a substitution cipher, it is vulnerable to frequency analysis, where an attacker analyzes the frequency of letters in a ciphertext and compares it to the expected frequency of letters in the plaintext language (Singh, 1999).

Lack of a secure key exchange method: Users of the cipher disk needed to exchange the initial settings or key securely, which could be intercepted by adversaries.

Noteworthy facts from the resources:

The Mexican Army Cipher Disk was used by various factions during the Mexican Revolution, including the forces of Pancho Villa and Emiliano Zapata (Fagin, 2018).

The disk's design was influenced by earlier cipher disks, such as the Confederate Cipher Disk used during the American Civil War (Fagin, 2018).

The Mexican Army Cipher Disk was used for both military and diplomatic communications (Fagin, 2018).

Fagin, B. (2018). Mexican Army Cipher Disks: A Historical Survey and How to Make One. Cryptologia, 42(3), 201-214. <https://doi.org/10.1080/01611194.2017.1414336>

Singh, S. (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books.