Civil War Cypher Disk

Recommended grade level: 4th Grade
Time required: 45-60 minutes
Setting: Classroom

Materials:

- Cypher disk sheet
- Scissors
- Brass round head fasteners

Objectives:

1. Students will gain a basic understanding of the purpose of a cypher.
2. Students will learn how cyphers are used to ensure secure communications.
3. Students will learn different methods used to encrypt and decrypt messages.

Background:
Today, **cypher** is synonymous with "code," as they are both a set of steps that encrypt a message. **Encryption** is the process of altering messages or information in such a way that only authorized parties can read it. The reverse, **decryption**, is the process of returning messages or information back to its original state so the authorized parties can read the message.

A cypher (also spelled cipher) is a procedure using a series of well-defined steps that can be followed to perform the encryption or decryption of a message to hide its true meaning. There are two methods to send messages. First is called **plaintext** or cleartext, which is information transmitted or stored unencrypted ("in the clear"). The big issue, especially in military operation, is anyone knowing your encryption and decryption system can easily read your message. The second method to send messages is to create a cypher ensuring greater security by hiding the message.

When using a cypher, the original information is known as plaintext and the encrypted form as **cyphertext**. The cyphertext message contains all the information of the plaintext message but is not in a format readable by a human or computer without the proper mechanism to decrypt it. To decrypt a cypher, a **key** is needed which is usually a piece of information to understand the cyphertext. The key must be selected by the message sender and receiver before using a cypher to encrypt a message. Without knowledge of the key, it will be extremely difficult, if not impossible, to decrypt the resulting cyphertext into readable plaintext. Cyphering devices could come in multiple formats, but one of the most common was a cypher disk.

A cypher disk consists of a minimum of two discs with a smaller disc on top of a larger disc and pinned together in the center. The two discs have letters or numbers in a random pattern on the top of each disk. In order to create a ciphered message, the smaller disc would be turned to correspond to a different letter or combination of numbers. This process was random but both signaling parties needed to use the same combination.

Procedures:

1. Collect the materials.
2. Go over the background information on cyphers.

    a. Include the key words to help understand that process:
        i. Cypher
        ii. Encryption
        iii. Decryption
        iv. Plaintext
        v. Cyphertext
        vi. Key
    b. A good way to get kids to think of cyphers are using current ext messaging abbreviations they use every day.
        i. First, see if they can think of any. Offer the following as cyphers:
            1. LOL – laugh out loud
            2. TLDR – too lazy, didn't read
            3. LMK – let me know
            4. IDK – I don't know

3. Next divide the class into groups of 2 and pass out cypher disk sheets to everyone. These partners will encode and decode messages to each other.
4. Have them put the cypher disks together making sure the line of the two wheels match up.
5. Ask students to light up the letter "A" on each wheel and notice that one when goes from left to right and the other from right to left.
6. Now the groups can start sending cyphered notes to each other.
7. Give each group time to send basic words to each other then write longer messages.
8. Students will quickly learn the key is important.

Closure:
Questions to help with closure:

1. Once you got comfortable with the cypher, how long did it take you to code and decode a message?
2. Would this be an easy job for someone to have?
3. What would you do if your code was broken?

Students may also encrypt a message for a group in the next class to decrypt.