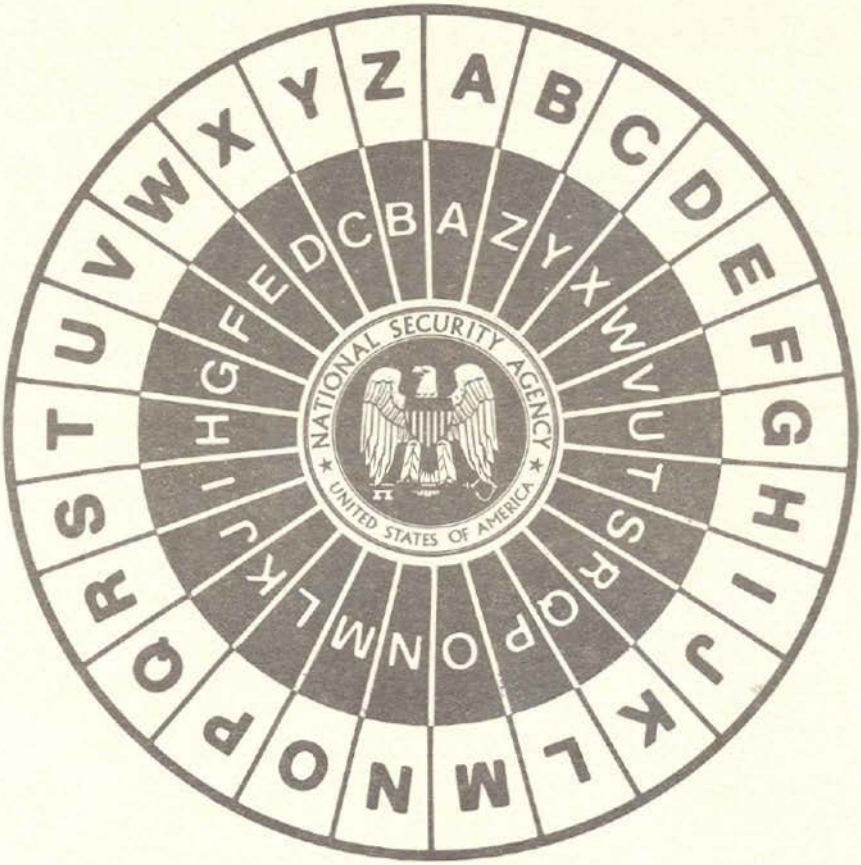

The Cipher Disk

This simple device has a distinguished history. Ever since its first invention it has been repeatedly re-invented in forms only slightly different from the original. Its story shows that man has sought to put the wheel to use in secret communications wherever possible, even as he also does in mechanics.

As invented in Italy sometime before 1470, it had similar concentric disks with the exception that one contained a "mixed" (scrambled) alphabet. Also, in some of the earlier versions, one of the two alphabets was composed of arbitrary symbols in lieu of conventional characters.

The appeal of the disk lay in the fact that with it, encipherment and decipherment could be performed without carrying bulky or compromising written materials.

The cipher disk came into large-scale use in the United States for the first time in the Civil War. The Federals' Chief Signal Officer patented a version of it, very similar to the original Italian disk, for use in flag signaling. Since his flag stations were within the view of Confederate signalmen as often as not, he prescribed frequent changes of setting.

About a half-century later the U.S. Army adopted a simplified version, very similar to this device, in which one alphabet was "standard" and the other "reverse-standard." Although technically this was a step backward, there were compensating advantages since the regularity of the alphabets tended to reduce error. During the period of the First World War and for several years afterward, the Army issued the disk in this form to units that needed a cipher which could be carried and used easily and which would give a few hours' protection to tactical messages.

In using this device you could leave the two disks in the same setting for an entire message, thus producing the simplest possible cryptogram. Or their setting could be changed with every letter of the message and, if the pattern of the setting-changes were complex enough, you would have an extremely secure cipher.