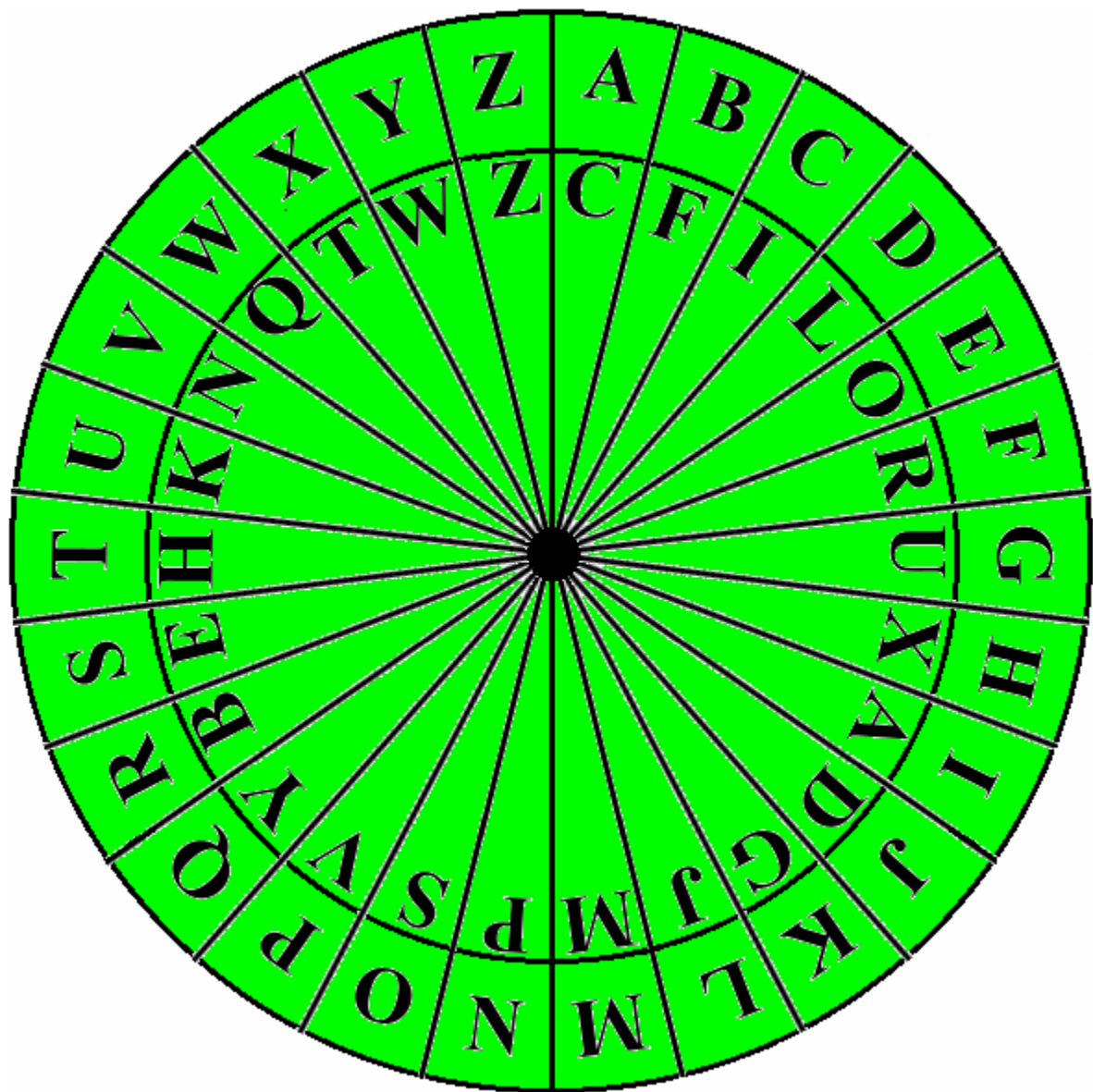


Code Wheels

A substitution code is actually very easy to crack. In a long message you can identify the three most frequent letters, e, t, and a use them to identify familiar words and figure out the code key. A code wheel key is much harder to crack: the key changes each time you rotate the wheel!

Activity: make and use your own code wheel.



History Note: The Enigma Machine

During World War II the Germans encoded military messages using a machine called Enigma. It operated on much the same principle as the code wheel. The Germans believed that they had invented a code which could not be broken, but with hard work, British and Polish cryptanalysts and mathematicians were able to decipher important information about German military operations. It was another 30 years before a truly unbreakable code was invented.



(c) 1995, Morton Swimmer

Photo courtesy of Morton Swimmer. Used with permission.

The Unbreakable Code: RSA Public Key

How can a code with a "public key" be unbreakable? The encoding key is two publicly known numbers. The person who receives the message knows another number, the secret decode key. In principle if you know the encoding key you can figure out the decode key. However, it is nearly impossible to figure out which two very large prime numbers are multiplied to make the public key. This code is widely used today for internet security as well as for more traditional code applications.