

MAKE AN ALBERTI CIPHER DISK

Different versions of Alberti's cipher disk were used through the centuries, all based on the same idea. Alberti called the larger, bottom disk the "stationary" and the smaller, top disk the "movable."

Alberti's original disk had 20 letters and four numbers. The four numbers were not used as cipher letters, so they did not appear on the movable disk. Because certain letters in the English alphabet are not used in the Italian alphabet, the disk here is somewhat different than Alberti's. For reasons that are unknown, Alberti also did not use the letters h and u.

ADULT SUPERVISION REQUIRED

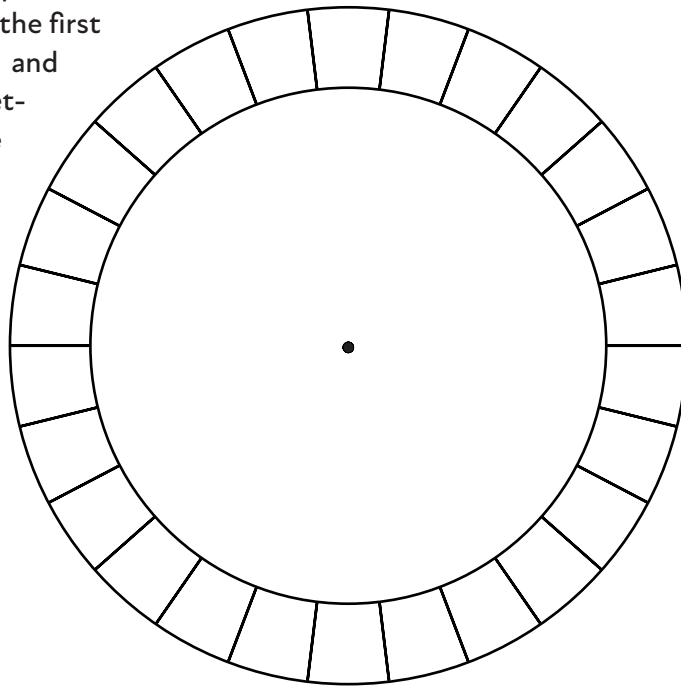
YOU'LL NEED

- Copy of the two disks shown here
- Pen or pencil
- Blank paper
- Scissors
- One brass fastener
- Adult helper

1. Copy or trace onto a sheet of paper each of the blank disks on the next page.
2. Cut out each disk, following the lines on the *outside* of the circles.
3. Write the alphabet in lowercase around the outside of the larger stationary disk. One letter should go in each square. These are your plaintext letters. To make your cipher even more challenging, write the letters in a different order.
4. Do the same for the smaller movable disk, but write the letters in uppercase in the squares around the outside of this disk.
5. Place the smaller disk on top of the larger disk, lining up the circles closely. With the pointed end of the fastener—or *carefully* with one point of the scissors (and an adult's help)—poke a small hole in the large dot in the middle of the small disk and through to the large disk. Insert the fastener, turn the disks over, and separate the two prongs until they lay flat. Your inner disk should turn easily.
6. On a sheet of paper, write a plaintext message. Pick one ciphertext letter for your starting letter. Turn the inner movable disk to line up that starting letter with the plaintext letter *a* on the outer, stationary disk.
7. Write your encrypted message on a second piece of paper. To begin with, write the enciphered letter that points to the plaintext *a*. (Remember that enciphered letters are on the inside disk and

plaintext letters are on the outside.) The starting letter is not part of the message but tells the person deciphering your message how your disks were lined up when you enciphered the first word in your message. Now write the cipher letters that are paired with the letters of the first word.

8. For the second word in your message, turn your disk again, lining up another cipher letter with the *a*. On the second piece of paper, leave a small space after the first enciphered word and then write this letter to tell where the disks line up again. Next



to it, write the second word of your message in ciphertext.

9. Continue doing this until your entire message is written in cipher. Remember, a friend deciphering your message needs to have an identical Alberti cipher disk.
10. Keep the Alberti cipher disk in your Cryptologist's Kit for future use.

