Encryption and decryption using a shift cipher

Overview. You will prepare a cipher disk and use it to encrypt a few words using a key of your choice. Then you will decrypt someone else's work.

Things to do.

1. Obtain a blank cipher disk. In the spaces on the outside ring, write the (upper-case) letters `A` through `Z`, in order, going clockwise around the disk. In the spaces on the inside ring, write the (lower-case) letters `a` through `z`, in order, again going clockwise. (It doesn't matter where you start, because the disks rotate.)

   We will use the convention that ciphertext letters are written in upper case and plaintext letters in lower case.

2. On a sheet of paper (graph paper is useful for this), write, in lower-case letters

   your name
   your hometown
   two or three of your favorite hobbies

   Leave plenty of space *above* each line you write – you'll be filling in the ciphertext above the plaintext.

3. Pick a key letter for your encryption. Rotate the cipher disk so that the `a` on the inner ring lines up with your key letter on the outer ring.

4. With the cipher disk fixed in this position (use a paper clip, if you like), encrypt the information you wrote down in step 2. To avoid confusion, write the ciphertext in upper case.

5. Obtain an index card, and copy your ciphertext to the card. Write your key letter in the upper right corner of the card, and circle it.

6. We'll collect and redistribute the cards. When you get a card, set your cipher disk according to the key letter on the card, and decrypt the name, home town, and favorite hobbies of your classmate.