Cipher Tools Hints

When attempting to break a cipher code, multiple tools are available to help you. Many of the tools are online where you can type in the encrypted values, tweak some parameters and then select decrypt to see if the message makes sense. The tools listed in the readings this week are great places to start with multiple algorithms. For example:

- http://rumkin.com/tools/cipher
- https://cryptii.com/pipes/caesar-cipher
- http://practicalcryptography.com/

As you attempt to solve break the codes in the lab for this week, consider these hints:

1. Narrow down the algorithm to reduce the work. For example, I didn't mention a passphrase was needed so ciphers that need a passphrase can be eliminated.
2. Look for obvious shift and patterns. One and two-letter words are easy to spot for caesarian shifts. For example, a, I, is, it, we, on, so can be entered and shifted in the caesarian shift to zero in on how much of a shift took place. These are easy to spot and also may begin to resolve as you shift through the alphabet.
3. Experiment with decrypt/encrypt to better understand the algorithm and look for patterns close to the results. There is nothing wrong with copying the encrypted text directly into the tool, select the algorithm and then select decode.

From the https://cryptii.com/pipes/caesar-cipher, note what happens when you enter some short words. You can quickly see the encoded versions. Use the – and + options in the Cipher code to shift. (See figure 1).

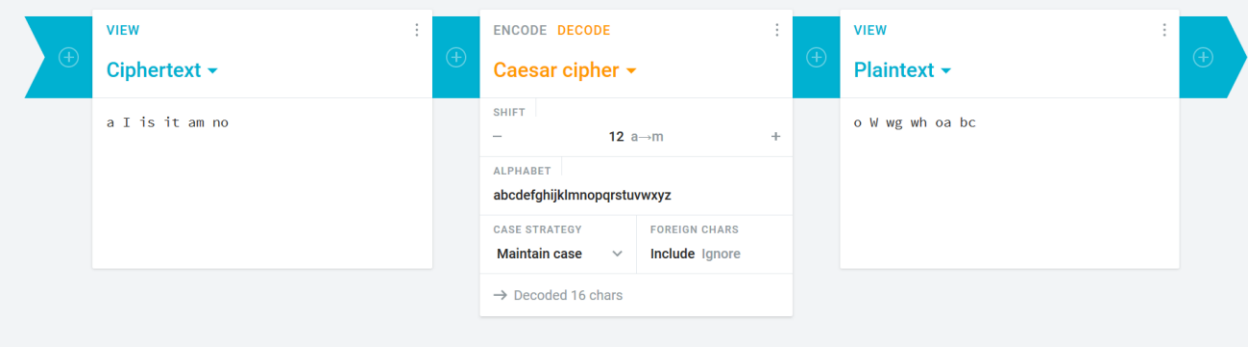

Figure 1. Using a Caesar shift of +12

Notice a->o, I->W for this example of +12 shift. If we shift +15, we see a different results (See figure 2).

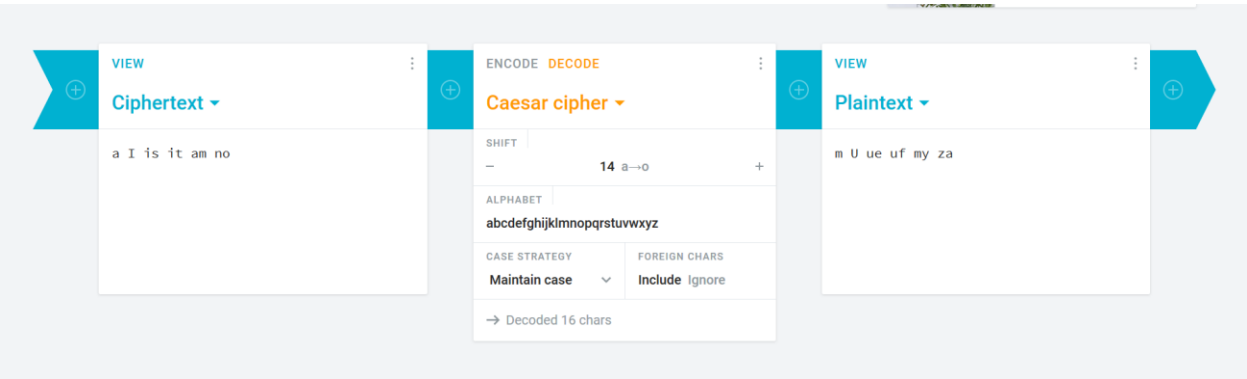

Figure 2. Using a Caesar shift of +15

You can also run the decrypt for each when you get close. Consider the following example from the rumkin site (http://rumkin.com/tools/cipher/), using the Base64 algorithm for encryption. (see figure 3)

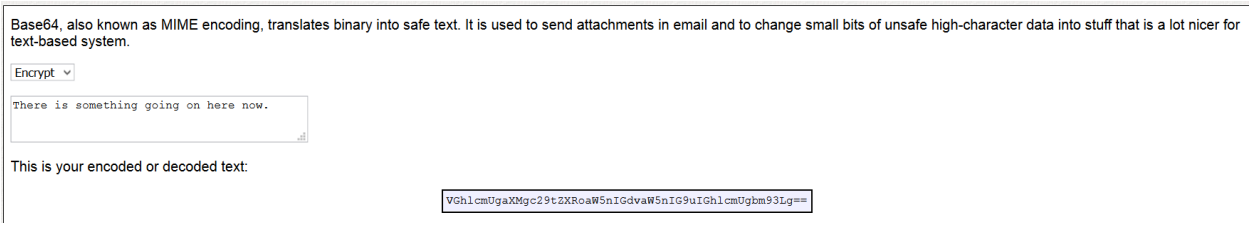

Figure 3. Base 64 Encryption of a phrase.

Similarly, if you copy and paste the encrypted phase and select decrypt, the tool will return the original phrase. See figure 4.

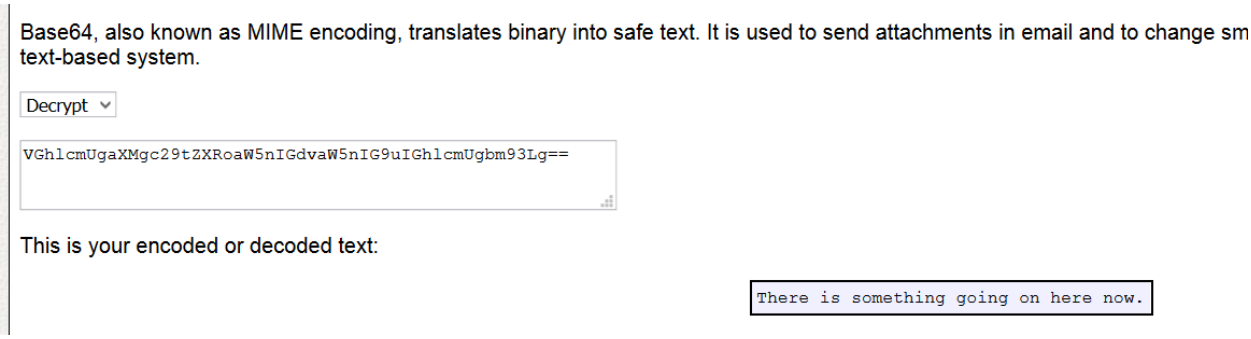

Figure 4. Decrypting the encrypted phrase

Be sure to go through each algorithm that makes sense to try when you are decrypting the phrases provided for the lab.