Name: _____

Read the introduction and Section 1.1, The Shift Cipher. Read carefully, marking up your copy of the text and taking notes. The introduction provides an overview of cryptology and defines terminology that will be used throughout the class. Section 1.1 introduces a simple cipher called the shift cipher.

Reading Questions

1. Make sure you are familiar with the following terms from the introduction: cryptosystem, cipher, encryption, decryption, plaintext, ciphertext, key, code, encode, symmetric cipher, asymmetric cipher.

2. What are the three types of attacks on a cryptosystem? Describe them in your own words.

3. Make sure you are familiar with the following terms from Section 1.1: shift cipher, Caesar cipher, monoalphabetic cipher.

4. Why is a shift cipher very easy to break?

5. In what context is a shift cipher completely effective?

6. Try exercises 1.1.01, 1.1.06, and 1.1.09.

7. What struck you in this reading? What is still unclear? What remaining questions do you have?