Name: ______________________________

Read Section 1.3, The One-Time Pad. Read carefully, marking up your copy of the text and taking notes.

Reading Questions

1. In the third paragraph, encryption and decryption for the shift cipher are described as functions from the set $\{0, 1, \ldots, 25\}$ to itself.

   (a) Look back at exercise 1.1.01. What is the formula for the function $E_k(x)$ that describes this encryption?

   (b) Look back at exercise 1.1.09. What is the formula for the function $D_k(x)$ that describes this decryption?

2. How is the key for OTP different from the key for a shift cipher? Look again at the example encrypting the word ‘impossible’ using OTP. What is the key in this example?

3. Explain what it means for the OTP to be *polyalphabetic*. Use the example in the text (encrypting ‘impossible’) to illustrate the polyalphabetic nature of the OTP.

4. In your own words, explain the advantages and disadvantages of the OTP in comparison to the shift cipher.

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