Name: _____

Read the introduction, Section 1.1, The Shift Cipher, and Section 1.3 The One Time Pad. Read carefully, marking up your copy of the text and taking notes.

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 four 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? In what context is a shift cipher completely effective?

5. Try exercise 1.1.06.

6. **Note on Notation.** In this text, reduction modulo a positive integer m is denoted $\%\, m$. For example, since $16 = 5 \cdot 3 + 1$, we have: $16 \,\%\, 5 \;=\; 1$.

7. 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?

8. 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.

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

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

Math 221, Crypto: 1.6 Integers mod m, Intro to Ch 7, 7.1 Trapdoors

Name: _____

Read and take notes on Section 1.6, The Integers mod m, the introduction to Chapter 7, and Section 7.1, Trapdoors.

Reading Questions

1. In your own words, explain what the set $\mathbb{Z}/m$ is and why it is *not* a subset of $\mathbb{Z}$.

2. In your own words, explain what the set $(\mathbb{Z}/m)^\times$ is.

3. True or false (with reasons).
   (a) $\mathbb{Z}/5 = \{0, 1, 2, 3, 4\}$.

   (b) $\mathbb{Z}/5 = \{\bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$.

   (c) $(\mathbb{Z}/5)^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

4. Explain why using asymmetric ciphers greatly reduces the number of keys required to maintain a communications network.

5. Explain how an asymmetric cipher and a symmetric cipher work together in practice, through use of a session key.

6. What is the trapdoor for the RSA cipher?

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

Name: _____

Read and take notes on Section 7.2, The RSA Cipher. Focus on the first few pages, through page 98, up to but not including the "Further technical notes."

Reading Questions

1. What does Euler's theorem say? (Make sure to include a description of Euler's φ-function.)

2. To understand the set-up of the RSA cipher, we will walk through a very simple example.

   (a) Choose primes $p = 7$, $q = 19$. (In practice, these should be large primes.) Are these numbers public or private?

   (b) The RSA modulus n is $n = pq$. What is n in our example? Is this number public or private?

   (c) What is $\varphi(n)$, in our example?

   (d) What must be true about the encryption key e and the decryption key d for the decryption step to really decrypt? Which is public and which is private?

   (e) Let $e = 5$. Show that choosing $d = 65$ will work.

   (f) For $x = 6$, show that $D_{n,d}(E_{n,e}(x)) = x$. Feel free to use technology for the modular arithmetic.

3. Why is it important that exponentiation be 'easy' relative to factorization?

4. Why is it important that primality testing is 'easy' relative to factorization?

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

Name: _____

Read and take notes on Section 9.5: Exponentiation Algorithm.

Reading Questions

1. (a) How many steps (maximum) should it take to compute $2^{56} \,\%\, 10$ using the fast exponentiation algorithm?

   (b) Compute $2^{56} \,\%\, 10$ by hand, using the fast exponentiation algorithm.

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