Name: _____

Read and take notes on the introduction to Chapter 16 Random Number Generators and Sections 16.1 Fake OTPs, 16.2 Period of a pRNG, 16.3 Congruential Generators.

Reading Questions

1. Make sure you understand the following terms: pseudo-random number generator, seed/key of a pRNG, keystream, periodic sequence, eventually periodic sequence, linear congruential generator

2. (a) Explain, in your own words, what a pseudo-random number generator is.

   (b) Name two pRNGs that are not good enough for cryptographic purposes and one that is.

3. Explain why the cryposystem described in Section 16.1 is a *fake* OTP as opposed to a genuine one.

4. Given the modulus $m = 300$, multiplier $a = 17$, and the seed $s_0 = 3$, list the first 25 numbers in the stream generated by the simplest linear congruential generator described in the second paragraph of Section 16.3. What is the period of this generator?

5. Given the modulus $m = 300$, multiplier $a = 17$, the integer $b = 67$, and the seed $s_0 = 3$, list the first 10 numbers in the stream generated by the linear congruential generator described in the third paragraph of Section 16.3. What is the period of this generator?

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