MATH 3540 **Name:** _____
Day 5

Directions

1. Complete the following questions.

1. Which of the following is NOT a drawback of the one-time pad?

   (a) A given key can only be used to encrypt one message

   (b) The key is as long as the message

   (c) The key must be chosen uniformly

   (d) The scheme is insecure against chosen-plaintext attacks

2. Let π =(Gen,Enc,Dec) be an encryption scheme over a message space. Then π is perfectly indistinguishable if and only of π is perfectly secret.

3. Which of the following attackers can be used to demonstrate that the shift cipher for 3-character messages does not satisfy perfect indistinguishability?

   (a) Output m0 = 'aaa' and m1 = 'bbb'. Given challenge ciphertext C, output 0 if the first character of C is 'a'.

   (b) Output m0 = 'aaa' and m1 = 'abc'. Given challenge ciphertext C, output 1 if the three characters of C are all different.

   (c) Output m0 = 'abc' and m1 = 'bcd'. Given challenge ciphertext C, output 1 if the three characters of C are all different.

   (d) Output m0 = 'aaa' and m1 = 'abc'. Given challenge ciphertext C, output 0 if the first character of C is 'a'

4. Which of the following is a negligible function? (Check all that apply.)

   (a) $f(n) = 1/n$

   (b) $f(n) = 1/2$

   (c) $f(n) = 1/2^n$

   (d) $f(n) = n/2^n$

5. Which of the following is true about computational secrecy?

   (a) Computational secrecy allows an attacker to learn information about the message with small probability.

   (b) Computational secrecy only ensures secrecy against attackers running in some bounded amount of time.

   (c) Computational secrecy means that it is trivial for an attacker to always learn the entire message.

   (d) Computational secrecy currently relies on unproven assumptions.

   (e) Write a python script to complete the following:

      i. The hex encoded string: '1b37373331363f78151b7f2b783431333d 78397828372d363c78373e783a393b3736' ... has been XOR'd against a single character. Find the key, decrypt the message.

      ii. One of the 60-character strings at https://cryptopals.com/static/challenge-data/4.txt has been encrypted by single-character XOR. Find it.