MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 04 DOSSIER

Deadline: Thursday, 22 September 2016 at 3:05pm
This mission covers Sections 3.1 and 3.3.

Check one:

☐ I received help from the following classmate(s) on this assignment:

_____.

☐ I did not receive any help on this assignment.

1. Graded Problems

1. Let $F_1 = 1, F_2 = 1, F_{n+1} = F_n + F_{n-1}$ define the Fibonacci numbers $1, 1, 2, 3, 5, \cdots$.
   a. List the first 15 Fibonacci numbers.

   b. Compute the greatest common divisor for the following pairs: F_{10} and F_7, F_6 and F_9, F_6 and F_{12}, F_{10} and F_{13}.

c. Look at your previous examples. It turns out that $\gcd(F_m, F_n) = F_{\gcd(m,n)}$. Write out **two** specific and detailed examples to verify that you believe this is true.

d. Play with some examples, and make a conjecture about $\gcd(F_n, F_{n-1})$ for $n \geq 1$. Are there any patterns? Describe them here.

2. You can compute a gcd using SageMath's `gcd(a,b)`. Determine the solution for the following gcd computations.
   a. $\gcd(234, 6013)$

b. $\gcd(74951, 26269)$

c. $\gcd(5223389, 188434513)$

3. In class, we started practicing writing proofs or formal mathematical arguments. In this problem, we're going to walk through the proof of a theorem.
   a. The Theorem you want to prove is: Let a, b, c, d, and n be integers with $n > 0$. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $ac \equiv bd \mod n$. First, come up with an example (with specific numbers) to convince yourself this is true.

   b. Which part of the theorem is the hypothesis? This is what you assume.

c. Which part of the theorem is the conclusion? This will be what you show is true based on the hypothesis.

d. Write out the definition of $a \equiv b \bmod n$.

e. Now write the proof. Start by assuming the hypothesis. Use the necessary definitions and work your way towards the conclusion.

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 3.13: # 1, 4, 5, 7
- Section 3.14: # 1