MAT 301 Problem Set 1

Posted: January 6, 2012

Due: January 16, 2012

Worth: 100 points

Problem 1: Number Theory Review (60 points)

1. **(15 points)** Compute the multiplicative inverse of $a \pmod{n}$ for the following values of a and n:

   - $a = 5$, $n = 17$.
   - $a = 21$, $n = 63$.
   - $a = 5$, $n = 24$.

2. **(15 points)** Compute the values of the Euler Totient Function (also called the Euler Phi Function) $\phi(n)$ for the following values of n: (a) $n = 2012$, (b) $n = 2011$ (c) $n = 262144$.

3. Find *all numbers* n such that:

   - **(15 points)** $\phi(n) = 13$.
   - **(15 points)** $\phi(n) = 2$.
     `[Hint: In order to limit your search space, you can use the fact that` $\phi(n) \geq \sqrt{n}$ `for all` n `except` $n = 2$ `and` $n = 6$`.]`

Problem 2: Breaking Ciphers (20 points)

The following ciphertext is encrypted under either the Caesar Cipher, the Vigenere Cipher (with a key composed of two random shifts) *or* the Scytale cipher. I am not going to tell you which. Decrypt it.

`LZAKAKSJWSDDQWSKQHJGTDWEKWL`

Which scheme was used to encrypt the message?

Problem 3: The One-Time Pad (20 points)

When using the one-time pad encryption with key $K = 0^\ell$ (namely, a string of ℓ zeroes) to encrypt a message of length ℓ bits, the ciphertext is equal to the message! In other words, the message will be transmitted in in the clear! This sounds bad.

A proposal to "strengthen" the one-time pad is to choose the key at random among all strings of ℓ ones and zeroes, except for the all-zeroes string. Formally, we write this as $K \in_R \{0,1\}^\ell \setminus \{0^\ell\}$.

Somewhat paradoxically, this modification turns out to **weaken** the security of the scheme, the exact opposite of what was intended! Argue why this is the case.