MATH 3355A Assignment 2 October 28, 2015

Due on Wednesday November 11 at 11:30am in class.
Each question is 6 marks, and a total of 30 marks.

Show all your steps clearly

1. Evaluate the following Legendre, Jacobi and Kronecker symbols:
$\left(\frac{-217}{383}\right)$, $\left(\frac{3886}{12007}\right)$, $\left(\frac{3886}{12007}\right)$.

2. Let p and q be distinct large primes and let $n = pq$.

(a) Describe how to find p and q if $\phi(n)$ is known.

(b) Let $n = 97531151$. You are given that $\phi(n) = 97511400$. Use your method in (a) to express n as a product of two distinct prime factors.

3. The ciphertext message produced by exponentiation cipher with key $(e, p) = (4771, 9901)$ is

2753 5601 8985 1755 1944 7536 1413 0996 3402 1553

(a) Find the deciphering key (d, p).

(b) Determine the plaintext message.

4. The ciphertext message produced by using RSA cryptosystem with public key $(e, n) = (4771, 9991)$ is

3209 6215 0795 4061 5233 8285 8101 3963 9819

(a) Find the private key (d, n).

(b) Determine the plaintext message.

5. Determine if $n = 161304001$ is a strong pseudoprime with respect to the base 2.