MEMORIAL UNIVERSITY OF NEWFOUNDLAND

DEPARTMENT OF MATHEMATICS AND STATISTICS

Fall 2005

Pure Mathematics 3370
Assignment 8

Due: Monday
November 14, 2005

Marks

[5] 1. Let E be the function from $\mathbf{Z}^*_{6499}$ to $\mathbf{Z}^*_{6499}$ defined by $E(\overline{x}) = \overline{x}^{3017}$. Find the inverse D of the function E.

[6] 2. (a) Given that $n = 4386607$ is the product of two primes and $\phi(n) = 4382136$, find the two primes. (Hint: Let the primes be p and q. Prove that $p + q = n - \phi(n) + 1$. Now, solve an appropriate quadratic equation.)

[6] (b) The RSA public key for a secret agency is $n = 3030583$ with encryption exponent $e = 3971$. The private key d has been leaked to you and is $d = 2140331$. Determine the prime factors of n. (Hint: Note that n and $\phi(n)$ are close together in size with $\phi(n) < n$.)

[8] 3. Find all the primitive Pythagorean triple (a, b, c) for which one of a, b or c is 420. (You should list the primitive Pythagorean triples in the form $a = u^2 - v^2,\ b = 2uv,\ c = u^2 + v^2$ where $u > v,\ (u, v) = 1$ and u and v have opposite parity.)

[25]

The Final Exam in PM 3370 is Wednesday, December 14, 2005 at 9am in HH-3017.