**Cryptography Homework #4**

**Due Date Uncertain**

**1)** Prime p = 4k+3, quadratics residue s modulo p. Find t such that s ≡ t2 (mod p).

p = 107. s = 99.

P = 1039, s = 262.

P = 2707, s = 1712.

2) Factor the number n using the "p-1 method."

n = 190 248 273 382 547 686 244 479 775 579 416 295 505 415 044 511.

[Hint: n=pq, where p and q are prime and p-1 is 37-smooth.]

3) Find the smallest primitive root modulo Psafe = 1025 + k, where k = 1879.