Cryptography Final
Review Sheet

(1) RSA - Public Key Encryption.
Given:
n a small prime
e smallest odd integer with gcd with ϕ of 1
c an encrypted message
Needed:
p and q two prime numbers whose products are n
$\phi = (p-1) \cdot (q-1)$
$d = e^{-1}$

(a) Find the primes p and q. If you do not have a prime factorization on your calculator, then know that one of them is going to be less $\sqrt{n}$, knowing this, we can test all primes less than $\sqrt{n}$.