ESE-3014 Lab 7 - Encrypt and decrypt with RSA

Theory

GNU Octave is a high-level language, primarily intended for numerical computations. It provides a convenient command line interface for solving linear and nonlinear problems numerically, and for performing other numerical experiments using a language that is mostly compatible with Matlab. It may also be used as a batch-oriented language.

Octave has extensive tools for solving common numerical linear algebra problems, finding the roots of nonlinear equations, integrating ordinary functions, manipulating polynomials, and integrating ordinary differential and differential-algebraic equations. It is easily extensible and customizable via user-defined functions written in Octave's own language, or using dynamically loaded modules written in C++, C, Fortran, or other languages.

Task

1. Simulate encryption communication, encrypt a message use a RSA public key, and try to decrypt it with a RSA private key.

2. Try to crack a private key with a known public key. And determine the key component to keep the security of RSA encryption communication.
   Hint: the key is find out d, we can get private key once we have d. Is it possible to derive d in the case of n and e?
   1. ed $\equiv$ (mod ϕ(n))
   2. ϕ(n) = (p-1)(q-1)
   3. n=pq