**ESE-3014 Lab2**

**Review Octave**

# **Theory**

GNU Octave is a high-level language, primarily intended for numerical com- putations. It provides a convenient command line interface for solving linear and nonlinear problems numerically, and for performing other numerical exper- iments 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 prob- lems, 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 mod- ules written in C++, C, Fortran, or other languages.

**Try to crack Asymmetric cryptography**

# **Task**

Review our slide about the process of asymmetric cryptography (like RSA

which have public key and private key), try to find an idea to crack it and

get text message between A and B.

**Encrypt and decrypt with RSA**

# **Task**

1. Simulate encryption communication, encrypt a message use an RSA public

key, and try to decrypt it with an 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 (mod φ(n)) = 1

2. φ(n) = (p-1)(q-1)

3. n=pq