Module: CST4136 Cybersecurity & Cloud Systems

Lab Week: 08

Objectives:

- Understand the Diffie-Hellman key generation algorithm and implementation
- Understand the RSA algorithms and implementation

Diffie-Hellman key generation algorithm implementation & utilisation

- Look through the algorithms in the weekly materials
- Determine which is the most usable and for what kind of task
- How could the keys be implemented? Develop a way of utilising

RSA algorithms implementation

- Look through the RSA algorithms in the weekly materials
- Determine which is the most usable and for what kind of task
- Implement your own RSA algorithm for text file

By the end of the session, you should:

- Appreciate how DH keys are implemented and produce a function which utilise them.
- Appreciate how RSA encryption works

Resources:

Provided MATLAB routines