# RSA Assignment

## Install on Ubuntu 18.04

# Install dependencies  
sudo apt install cmake gcc libntl-dev  
git submodule init  
git submodule update  
  
# Build  
cmake -Bbuild -H.  
cmake --build build/  
  
# Run test cases  
bin/rsa\_tests  
  
# Print help  
bin/rsa help  
  
# Generate public-private key-pairs with 4096-bits modulo N  
bin/rsa generate --size 4096 \  
 --public-key /path/to/public-key \  
 --private-key /path/to/private-key  
  
# Encrypt a file  
bin/rsa encrypt --public-key /path/to/public-key \  
 --input /path/to/input-file \  
 --output /path/to/encrypted-file  
  
# Decrypt a file  
bin/rsa decrypt --private-key /path/to/private-key \  
 --input /path/to/encrypted-file \  
 --output /path/to/decrypted-file  
  
# Encrypt and decrypt using pipe command  
echo 'Hello World!' | \  
bin/rsa encrypt --public-key /path/to/public-key | \  
bin/rsa decrypt --private-key /path/to/private-key  
# Should print 'Hello World!'