

# Project 1 - Implement the Public Key Encryption Scheme: RSA

## 1 Tasks to be Performed

- Implement the RSA key generation function that takes a positive integer  $k$  as an input and outputs the public key  $(N, e)$  and the private values  $p, q, d$  such that  $N = pq$ , a  $k$ -bit integer.
- Implement the RSA encryption and decryption functions.
- Implement the RSA encryption and decryption functions that support PKCS#1v1.5 message padding scheme.
- Implement a main program to produce the expected outcomes discussed next.

## 2 Expected Outcomes

When the main program is executed, here is the expected output:

1. Enter the name of the file that contains  $p, q$  and  $e$ :
2. Enter the output file name to store  $d$  and  $N$ :
3. Enter the name of the file that contains  $x$  to be encrypted using  $(N, e)$ :
4. Enter the output file name to store  $E(x)$ :
5. Enter the name of the file that contains  $c$  to be decrypted using  $d$ :
6. Enter the output file name to store  $D(c)$ :

## 3 Programming Language and Library Requirements

This project needs to be implemented in C/C++ and uses the GMP library (The GNU Multiple Precision Arithmetic Library, <https://gmplib.org/>) to manipulate big numbers.

## 4 Deliverables

- README: describe the purpose of your files and provide instructions on how to compile and execute your program.
- Well-documented source code.
- Submit the source code on Canvas and demo the project via Zoom.