Network Security Project - Option 1

RSA Encryption and Decryption

Total 20 points

(Due on Apr 22 11:59 pm, 2025)

Stage 1 (8 points) – Key Generation

- Implement your own **RSA method** to generate a pair of public and private keys.
  - **16 binary digits is the minimum requirement for the key length.**

Stage 2 (12 points) – Encryption/Decryption

- Encryption Process
  - Read an existing "**plaintext.txt**" file (meaningful, at least 50 words. I'll provide one for the project demo but feel free to select any one to test the program during the implementation).
  - Encrypt the content using your RSA program with your private key and save it as "**ciphertext.txt**".
  - You can use a **character-by-character encryption**.
- Decryption Process
  - Read and decrypt the "**ciphertext.txt**" using your corresponding public key and save it as "**decoded.txt**"

Requirements

a. You are given the flexibility to choose one of your favorite programming languages for implementation either in a Windows or Linux environment.

b. You must submit
   a) all the **source code** of your program
   b) **executable files and Makefile**(if using c/c++)
   c) **ReadMe file** that describes
      i. the use of your program
      ii. how to execute it

c. You will need to **demonstrate your project in class on Zoom on Apr 24. Otherwise, 10 out of total 20 points will be deducted from your project.**