German International University

Faculty of Informatics and Computer Science

Information Security

Dr. Marwa Zamzam

Thomas Safwat

Peter Wafik

Salma Abu Zaid

Mohamed Wael

Spring 2025
Assignment 2

Deadline: Saturday May 5, 2025

Requirements

You are required to implement the RSA algorithm. Your implementation should do the following:

- Generate a public-private key pair such that the length of the modulus n is at least 256 bits.
- Read a file from the hard disk, encrypt it with the encryption key, and store the encrypted text on the hard disk.
- Decrypt the encrypted file in order to obtain the original file again.

Rules:

- You should upload your code in zip folder on Google Drive that contains:
    1. Source Code
    2. RSA Decryption text file: Your Full Name
    3. RSA Encryption text file: Your Full Name After Encryption

  N.B: A sample of the targeted submission files is included in the project description zip folder for reference.
- You are allowed to use any Java or C++ libraries as long as the library only skips the basic steps but the main logic of the RSA Algorithm should be implemented.
- You should work in groups of 3 to 5 persons.
- Submission link: https://forms.gle/3SRGTahTZLqKvv9E7
- Deadline is 5/5 at 11:59 pm and the evaluations will start Tuesday 6/5 in the tutorials.