UNIVERSITI TEKNOLOGI MARA
FACULTY OF COMPUTER AND MATHEMATICAL SCIENCES

Course Name	:	Cryptography Algorithm
Lecturer	:	Assoc. Prof. Dr. Suriyani Ariffin
Lab Exercise	:	Group Project (3 members)
Topic	:	**Interactive RSA Game**
Submission Date	:	6 February 2026

This project is to develop an interactive game that demonstrates the concepts of RSA key generation, encryption, and decryption. The game will teach users how RSA works through challenges involving prime number selection, public/private key generation, and message decryption.

You are required to design and develop a game that demonstrates how the RSA cryptographic algorithm works. The game should be interactive and teach users the following steps of RSA in a fun way:

1. Prime Number Selection
2. Key Pair Generation (Public and Private keys)
3. Encryption of Messages
4. Decryption of Messages

Your game must have its **own unique identity** and may be developed as either a text-based (CLI) or GUI-based using Python, Java, or any other programming language you're comfortable with.
By completing this assignment, you will:

- Understand the steps in RSA algorithm: Prime numbers, modulus, public/private key, encryption, and decryption.
- Apply programming skills to develop an interactive game.
- Gain hands-on experience in implementing secure encryption methods.

PROJECT REQUIREMENTS

Your RSA game must include the following features:

Stage 1: Prime Number Selection (Challenge 1)

- The game will ask the player to select two large prime numbers (p and q) **generated by random function.**
- The game should have a feature to validate if the selected numbers are prime.

Stage 2: Key Generation (Challenge 2)

- Once the player selects two prime numbers, the game should:
  - Compute n = p * q
  - Compute $\phi(n) = (p-1)(q-1)$
  - Ask the player to choose an appropriate public key exponent (e) from the list of possible values.
  - Calculate the private key (d) using modular multiplicative inverse.

Stage 3: Encryption (Challenge 3)

- The player will enter a plain text message, and the game will:
  - Convert the text to numerical values (ASCII codes).

- Encrypt the message using the public key (n, e).
- Display the encrypted message.

Stage 4: Decryption (Challenge 4)

- The game will provide the encrypted message back to the player, and they must:
  - Use the private key (n, d) to decrypt it.
  - Verify if the decrypted message matches the original plain text.

FEATURES

1. Time Attack Mode:
   - Give players a limited time to solve each challenge.
2. Difficulty Levels:
   - Provide different levels (Easy, Medium, Hard) with increasing prime number sizes.
3. Leaderboard:
   - Keep a scoreboard to track the fastest players.

SAMPLE GAME FLOW

1. Welcome to the RSA Game!
   - Choose your difficulty level: [Easy / Medium / Hard]
2. Stage 1: Prime Number Selection
   - Enter your first prime number (p):
   - Enter your second prime number (q):
3. Stage 2: Key Generation
   - Calculating n and $\phi(n)$...
   - Select a public key exponent (e):
   - Private key (d) calculated!
4. Stage 3: Encryption
   - Enter a message to encrypt:
   - Your encrypted message: [Encrypted Text]
5. Stage 4: Decryption
   - Decrypt the following message: [Encrypted Text]
   - Enter your private key (d):
   - Your decrypted message is: [Decrypted Text]

REPORT (20 MARKS)

1. Source code of your game.
2. Documentation explaining:
   - How the game works.
   - Steps to run the game.
   - Screenshots of the game.
3. Reflection report (1 page) on what you learned from this project.

DEMO AND PRESENTATION (20 MARKS)

For the project submission and demo presentation, each of members of the group needs to be attended, it is mandatory

SUBMISSION DATELINE

The project online demonstration will take place in **7 February 2026 (Saturday)** ,or on another agreed date.