CENG418 Assignment-1: RSA Encryption and Brute Force Attacks

Objective

In this assignment, you will work with RSA encryption and brute force attacks to observe the difficulties of performing cryptographic operations on small and large bit-length numbers. Additionally, you will design and implement a protocol to securely manage anonymous assessment submissions.

Assignment Details

1. **RSA Encryption:**
   - Generate RSA key pairs using 2-bit, 4-bit, 8-bit, 16-bit, and 32-bit prime numbers.
   - Encrypt a chosen message using these keys.
2. **Brute Force Cracking:**
   - Attempt to break the encrypted messages using brute force methods.
   - Record the time taken for each bit-length, plot them and compare the results.
3. **256-bit RSA Breaking Time Calculation:**
   - Estimate the time required to break a 256-bit RSA encryption using brute force.
   - Base your estimation on your local machine's processing power.
4. **Supercomputer Comparison:**
   - Choose a supercomputer from around the world and calculate how long it would take to crack a 256-bit RSA key.
   - Include hardware specifications (processing power, core count, FLOPS, etc.) and compare it with your local system.
5. **Protocol Coding & Testing:**
   - Describe a protocol to distribute ID numbers from an instructor to students so that each student can submit a piece of work to be graded anonymously, but the instructor can be assured that each piece of work comes from a legitimate person in the class.
   - Write the code for the protocol mentioned above. Perform the tests and report them.

Submission Format

- Prepare a PDF report for the calculations, results and comparisons.
- Report your computer's processor model, core count, clock speed, and RAM used for this assignment.
- Submit your python codes and report.
- Your submission file name must be in the format CENG418_HW1_GroupID.zip
- Last submission date: 10th April 2025, 23:59