INSE6110 project

Part 1: Simple RSA (Encryption and Decryption)
Project objective:

1. Understand the RSA and write a simple implementation. **Don't use readymade modules (i.e. RSA module in python).**

Parameter Selection:

write a small program that:

1. Randomly select two prime numbers, denoted by p and q (16 bits each)(Please refer to FAQ)
2. Compute N=p*q
3. Compute Phi(N)=(p-1)*(q-1)
4. Randomly select a public-key, e, such that e < Phi(N); and e and Phi(N) are relative prime numbers (gcd(e, Phi(N)) =1).
5. Find the corresponding private-key d such that (e*d) mod Phi(N)=1
6. Publish your public-key (N, e) on the designated data base on Moodle.

Encryption/Decryption:

Write a function to encrypt or decrypt messages using square and multiply. (simply, you can pass to the function (N, e or d, m or c).

A) Encryption: Send an encrypted message to your Project partner

1. Check your partner name on Moodle.
2. Check your partner public-key (N, e)
3. Choose a small message. Keep in mind that the encrypted message m must be smaller than N.
4. Encrypt the message using your partner public-key (Please refer to FAQ)
5. Publish the encrypted message on the designated data base on Moodle.

B) Decryption: Decrypt the message received from your Project partner:

1. Check your partner's database and get the encrypted message.
2. Using your private-key (d), decrypt the message received from your partner
3. Publish the decrypted message on the designated data base on Moodle.

Part 2: Signature/Verification

Write a function to sign or verify messages using square and multiply. (simply, you can pass to the function (N, d or e, m or sig).

You can use your already selected parameters (N, e, and d)

A) Signature:

1. Sign your name without hashing using your private-key (d)
2. Publish the signature along with your name on the designated data base on Moodle.

B) Verification:

1. Use your partner public-key (N, e) and his/her name to verify his/her signature

Project Final Deliverables: (Please refer for FAQ)

All the code should be uploaded to the Moodle. **(Any Plagiarism will not be tolerated)**

1. A short video (~ 5 minutes max), you should show all your running steps.

2. The file "data.txt" filed with your data.

   The file "data_example.txt" is a dummy example of how to format your data as fields. Please follow the same format and do not change the field names or their orders.

Important due dates:

Nov. 15th at 11:59 pm (N, e are published on the database)

Nov. 22th at 11:59 pm (Encrypted Message published on the database)

Dec. 6th at 11:59 pm (Signature along with your name published on the database)

Dec. 13th at 11:59 pm (Final Deliverables are due)