FAQ
This file will be updated frequently:

1. **Can we use functions like isPrime() for primality testing?**
   Yes.

2. **What do you mean by a 16-bit integer?**
   A number that its binary representation is 16 bits e.g., the integer number (12) is 4-bit integer number because it is in binary (1100)

3. **Can I use Biginteger class in Java?**
   Only for primality testing.

4. **How can I generate a random number?**
   You can use the built-in random number generation in the programming language you are using.

5. **How can I encrypt my message?**
   Assume that your message is "Hello World",
   a. Divide your message into 3-byte chunks, e.g., "Hello World" -> ["Hel", "lo ", "Wor", "ld"]
   b. Convert each chunk into a hexadecimal string, e.g., ["Hel", "lo ", "Wor", "ld"] -> [0x48656c, 0x6c6f20, 0x576f72, 0x6c64]
   c. Convert each chunk into an integer number, e.g., [0x48656c, 0x6c6f20, 0x576f72, 0x6c64] -> [4744556, 7106336, 5730162, 27748]
   d. Encrypt each integer number and obtain the corresponding ciphertext in the form of a list of integers
   e. Send the list of integers to your partner.

6. **The run time of my code is very long. What should I do?**
   Make sure that your implementation of square and multiply technique are correct, e.g., you do (mod N) every time.

7. **What should I show in the video (Part 1)?**

You should run the code and show the following steps:

i. The selection of the two prime numbers and doing the primality test.
ii. The computation of N and phi (N).
iii. The computation of the public key and the private key (e, d). Then, switch to the Moodle and show your posted (N, e) on the database
iv. The message and the encryption of the message (Cipher text). Then, switch to the Moodle and show that the posted cipher on the Moodle is the same as you one you just computed.
v. Switch to the Moodle and show who is your partner and get his posted cipher and public key. Then, show the decryption of your posted cipher.

8. **What should I show in the video (Part 2)?**

Using the parameters generated and posted in part 1, i.e, public and private keys, you should run the code and show the following steps:

i. The message .
ii. The signature of the message. Then, switch to the Moodle and show your posted message and signature.
iii. On the Moodle, show your partner message and signature. Then, feeding them to your code (i.e., copy and paste is OK) run the verify algorithm on your partner message.

9. How I can prepare and upload my final deliverables?

i. Create a folder named "xxxx_yyyy" where "xxxx" is your ID and "yyyy" is your partner ID. e.g., if your ID is "1234" and your partner ID is "5678", the folder name will be "1234_5678".
ii. Store all your source code in the folder. Make sure that you include all dependencies and if your code needs to be compiled, e.g., you used c programming, include a Makefile.
iii. Include the txt file named "data.txt" in the folder. The file should summarize the data you did use and your results in fields, e.g., if your message is "Hello World!", the field called 'MY_MESSAGE = ""' should be 'MY_MESSAGE = "Hello World!"'. Please complete the fields with your data and be careful.
iv. Include your prepared video.
v. zip the folder to "xxxx_yyyy.zip", and this is your deliverable.