HW2: RSA

Due: Thursday, April 6 at 11:59 PM

Goals

Implement the RSA algorithm in any language, including Key generation algorithm, Encryption, and Decryption.

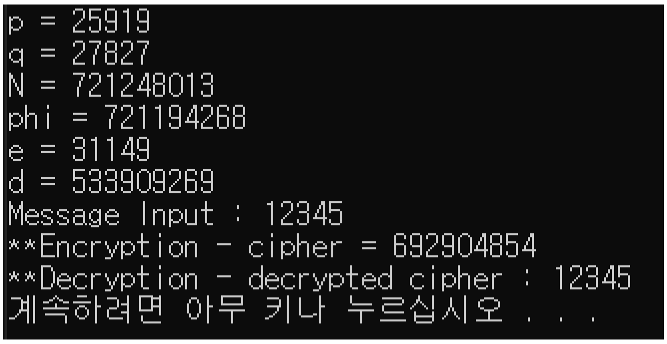
Requirements

1. The maximum size of n is 32 bits. ($n = p \times q$)

2. The key generation algorithm must generate a different key each time it runs.

3. Provide a program that verifies the **Key generation algorithm/Encryption/Decryption**.

3. The example output of the program is shown below.



```
p = 25919
q = 27827
N = 721248013
phi = 721194268
e = 31149
d = 533909269
Message Input : 12345
**Encryption - cipher = 692904854
**Decryption - decrypted cipher : 12345
계속하려면 아무 키나 누르십시오 . . .
```

Submission

1. Zip file containing all required files below.
   - Document (**pdf format only**)
     - a simple description of your implementation/code.
     - a screenshot of the output
   - Source codes & **Executable file**
     - Codes with comments about what the program does.
2. **The zip file and pdf file** should be named "<student ID>_<name>".
   (ex: 12345678_홍길동.zip)

About plagiarism

You must work alone for the assignment. The penalty for cheating is a grade of 0% on the assignment.