Implementation and Assessment of RSA

Objective

This assignment aims to improve understanding of the asymmetric cryptographic algorithm RSA, its implementation, and its typical use for symmetric encryption key distribution, authentication, and digital signature.

This assignment represents **20%** of the total marks for this module.

Description of Assignment

This assignment requires you to implement the RSA algorithm using your code without calling library functions, following the steps below.

1. Select two prime numbers, p and q, such that $p \neq q$;
2. Calculate the modulus $\boldsymbol{n} = pq$, *and* $\varphi(n) = (p-1)(q-1)$;
3. Choose e, so that $1 < e < \varphi(n)$, and $gcd(\varphi(n), e) = 1$;
4. Calculate $d \equiv e^{-1} \pmod{\varphi(n)}$;
5. Output the key pair: The *private key* PR = {d, n} and *public key* PU = {e, n};
6. Validate the implementation with at least two use cases.
   a. **Encryption**: The sender encrypts a message using the public key, and the receiver decrypts the cypher text using the private key.
   b. **Signature**: The sender signs a message (or hash code of a message) with the private key, and the receiver verifies the signature with the public key.

For the security of real-life applications, the RSA modulus would be around 2048 bits (approximately 616 decimal digits), and the p and q would be around 1024 bits (about 308 decimal digits). However, the proof-of-concept implementation in this assignment does not require the magnitude of the prime numbers p and q.

Programming Language

Python is preferred; C, C++ or Java is also accepted.
Please state the language and the IDE you used in your report.

The lab report should include the Source Code

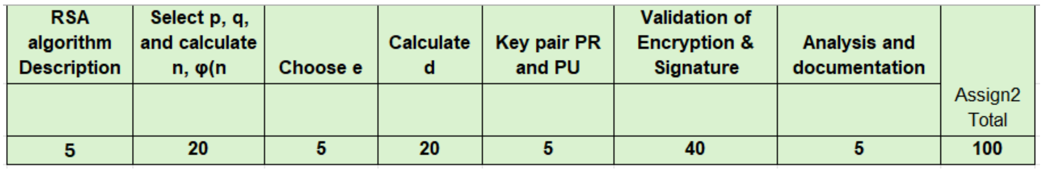
- Include code fragments in your report with a *detailed explanation*.
- Include the complete source code in an appendix of your report with appropriate comments and instructions on compiling it.

Submit *two separate files*.

1. **File 1**: A well-structured PDF format lab report named:
   Student ID Number-Full Name-EE5001 assignment2 report.PDF
2. **File2:** All source code files in a separate .zip file named:
   Student ID Number-Full Name-EE5001 assignment2 code.ZIP

[End of Assignment 2]

Marking Scheme



RSA algorithm Description	Select p, q, and calculate n, φ(n	Choose e	Calculate d	Key pair PR and PU	Validation of Encryption & Signature	Analysis and documentation	Assign2 Total
5	20	5	20	5	40	5	100