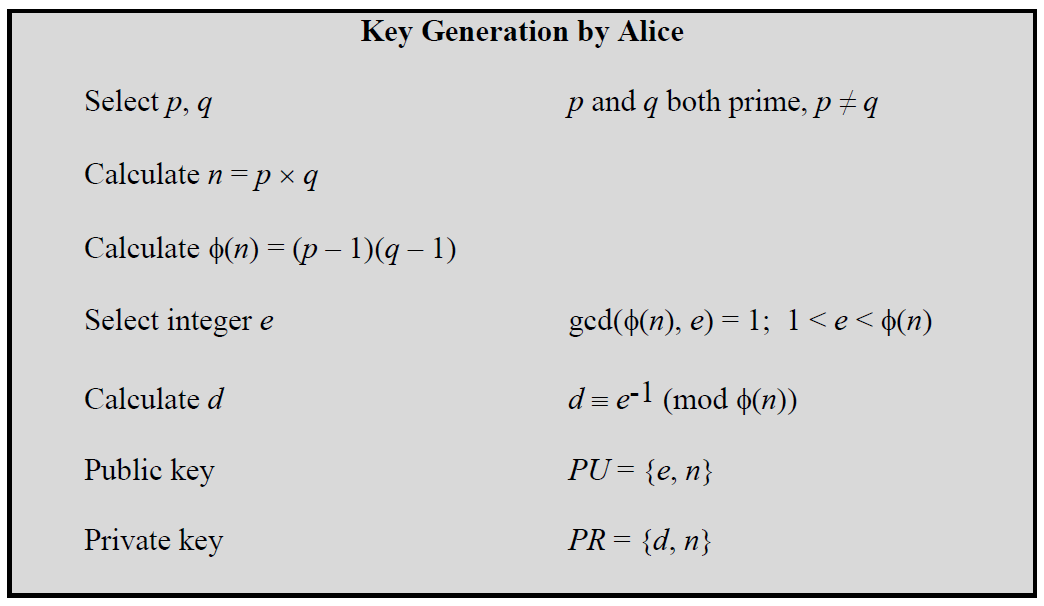


**SUMMER SEMESTER 2024**

**APT3090 CRYPTOGRAPHY AND NETWORK SECURITY**

Write a program using any Object oriented programming language to show implementation of RSA. The input p and q should be generated by randomly (15 Marks)

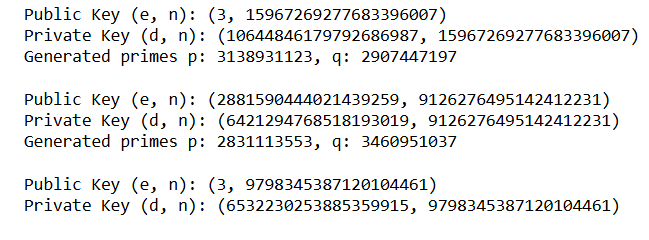


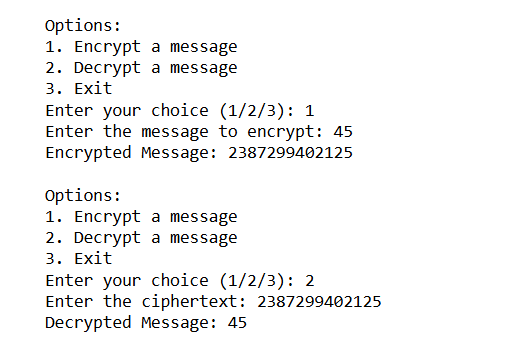
To encrypt a message, M, with the public key, create the ciphertext, C, using the equation: C = Me mod n

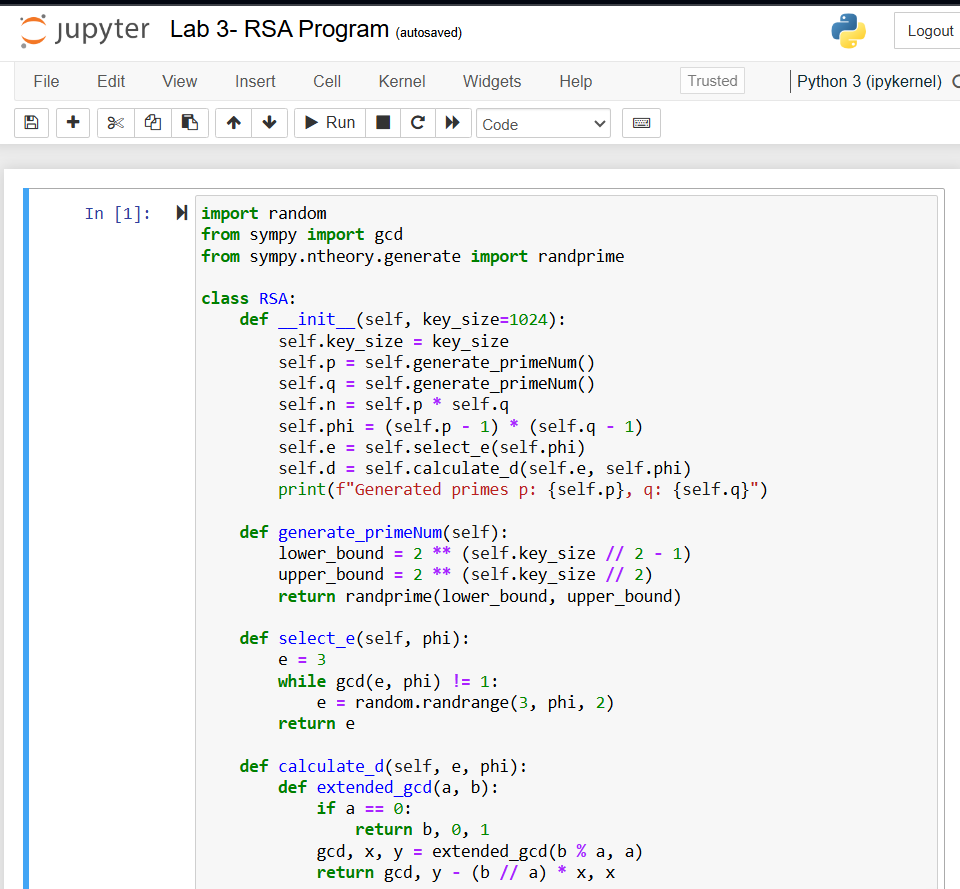
The receiver then decrypts the ciphertext with the private key using the equation: M = Cd mod n

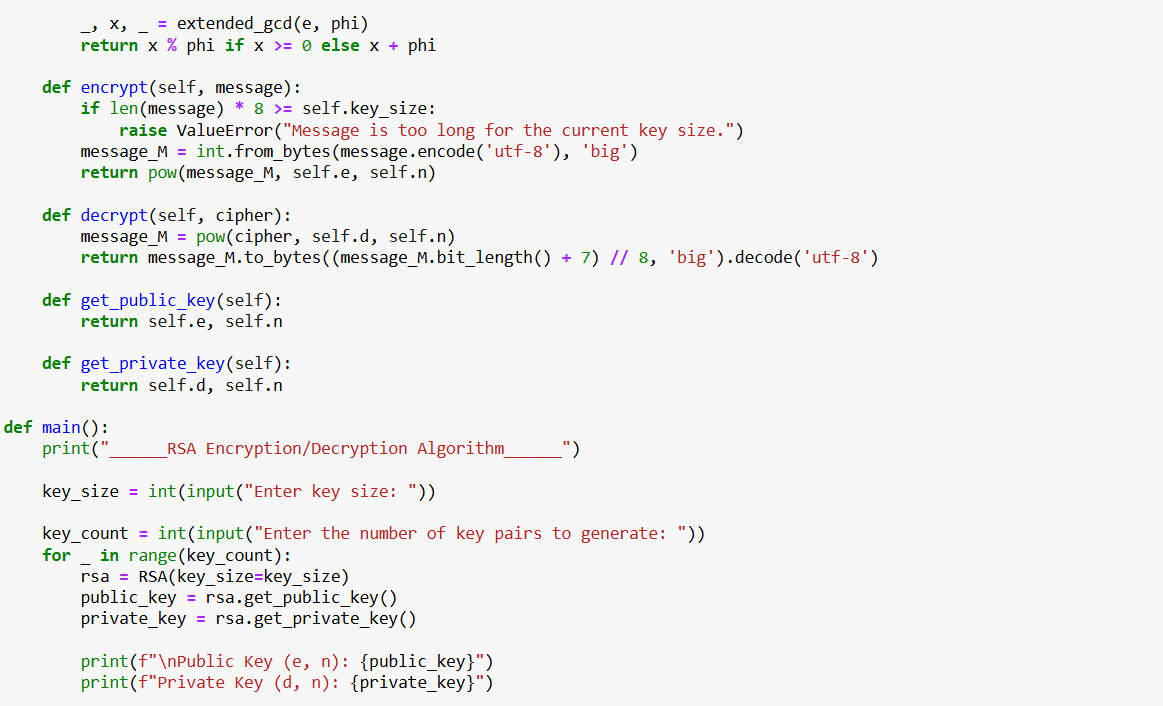
**Evaluation Criteria**

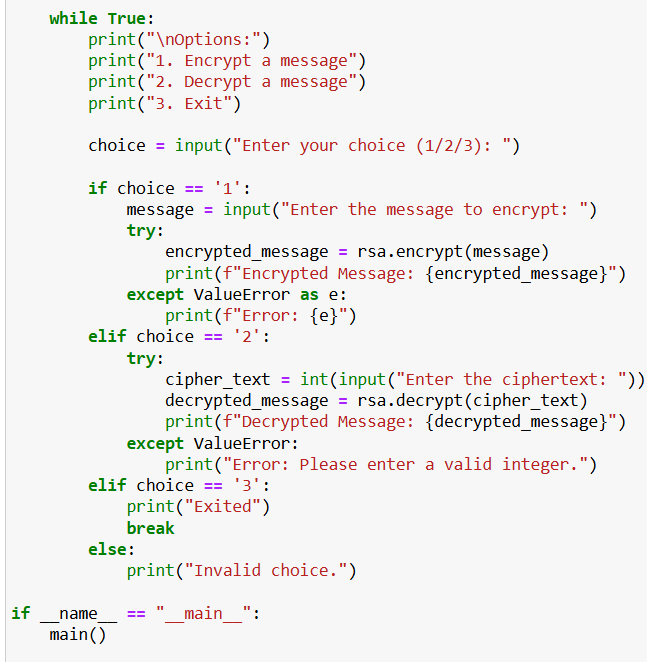
1. Correctness of code
2. Random number Generation of p, q
3. Generation of multiple pairs of PU ( e,n) and PR Keys (d,n)
4. Encryption and Decryption of input message
5. A lab report showing your code , sample outputs and code explanation

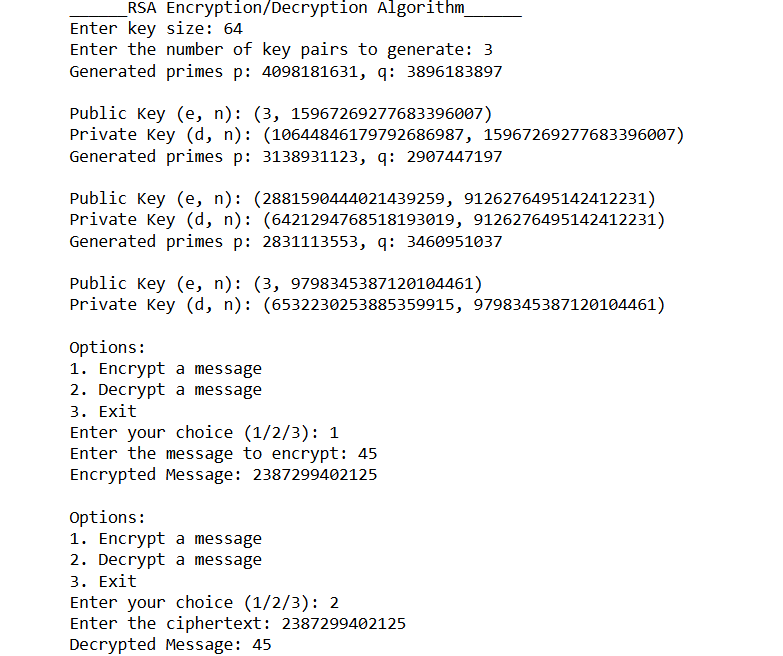


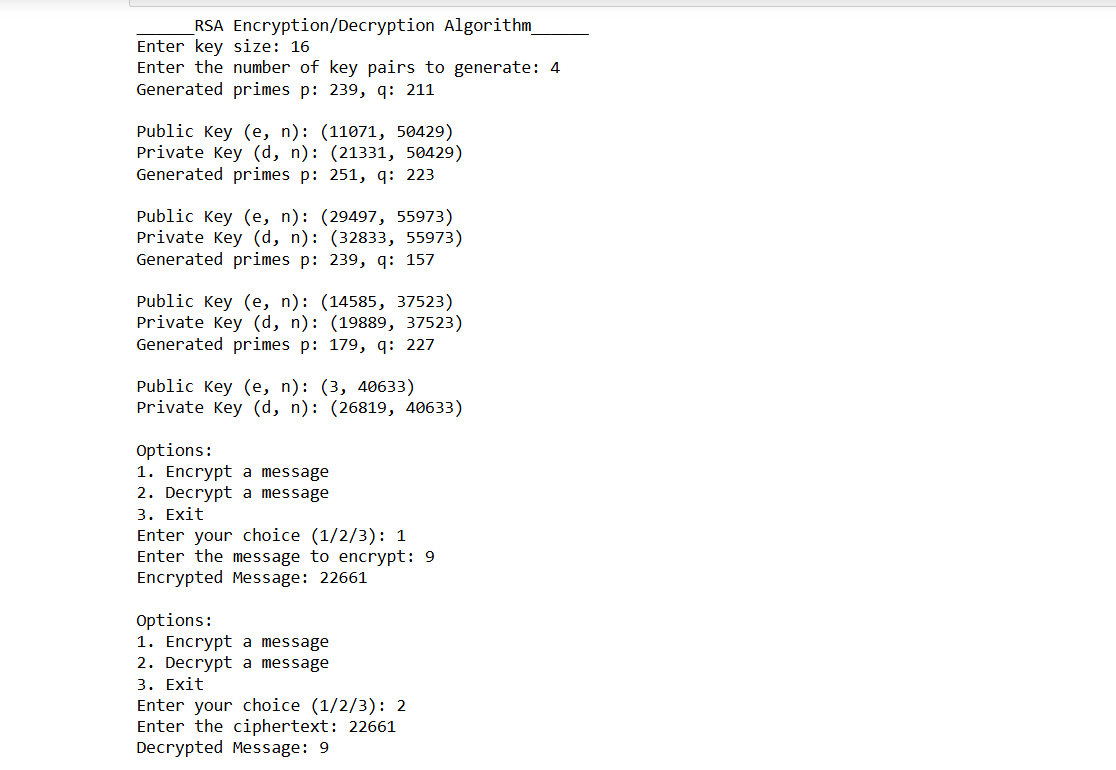












* "random" function: Used for generating random numbers.
* "gcd" function: Computes the greatest common divisor.
* "randprime" function: Generates a random prime number within a specified range.
* "\_\_init\_\_" function: Initializes the RSA object with a given key size. This function generates two prime numbers (p and q), calculates n (the product of p and q), computes phi (Euler's totient function), selects e (public exponent), and calculates d (private exponent). It also displays the generated prime numbers.
* "generate\_primeNum" function: Generates a random prime number between the lower and upper bounds based on the key size.
* "select\_e" function: Chooses a public exponent e such that gcd(e, phi) == 1. It starts with e = 3 and increments until it finds a suitable e.
* "calculate\_d" function: Compute the private exponent d such that d \* e ≡ 1 (mod phi).
* "encrypt" function: Encrypts a message, converts the message to an integer, checks if it's too long for the key size, and computes the ciphertext using pow.
* "decrypt" function: Decrypts a ciphertext, computes the original message integer using pow, and converts it back to a string.
* "get\_public\_key" and "get\_private\_key" functions: Return the public and private key pairs.
* "main()" function:
* Prompts the user for the key size and the number of key pairs to generate.
* Generates the specified number of RSA objects, displaying the public and private keys for each.
* Provides a menu for encrypting and decrypting messages or exiting the program.
* Encrypts a user-input message and displays the encrypted result.
* Decrypts a user-input ciphertext and displays the decrypted message.
* Continues until the user chooses to exit.