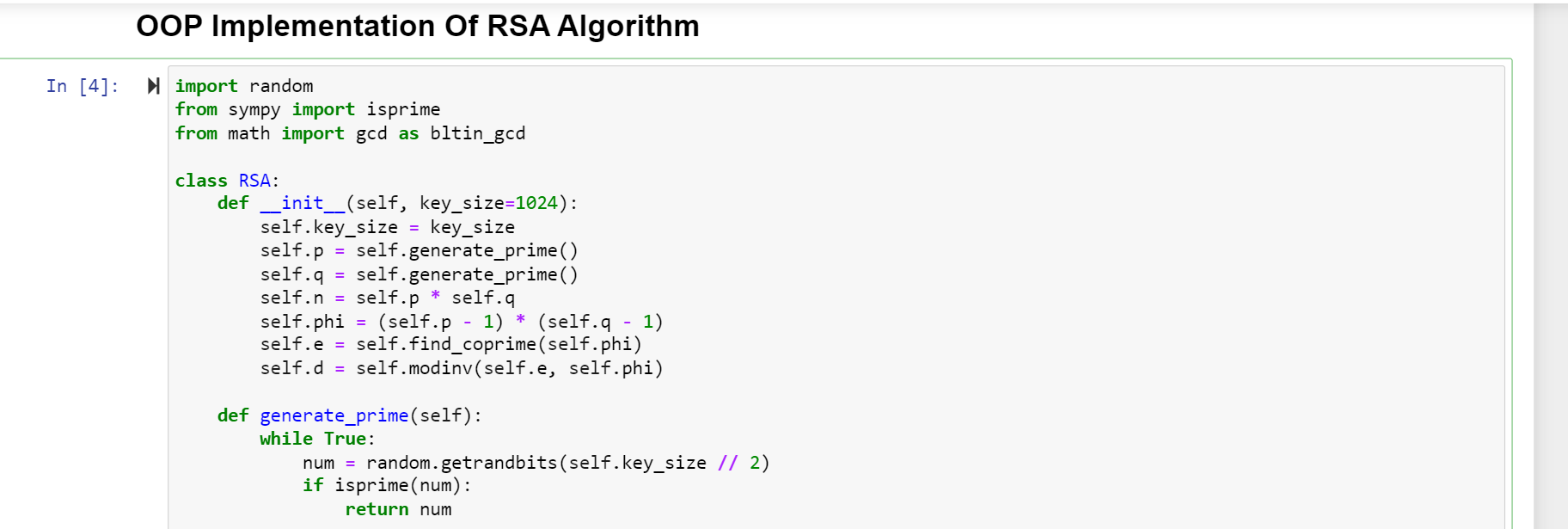


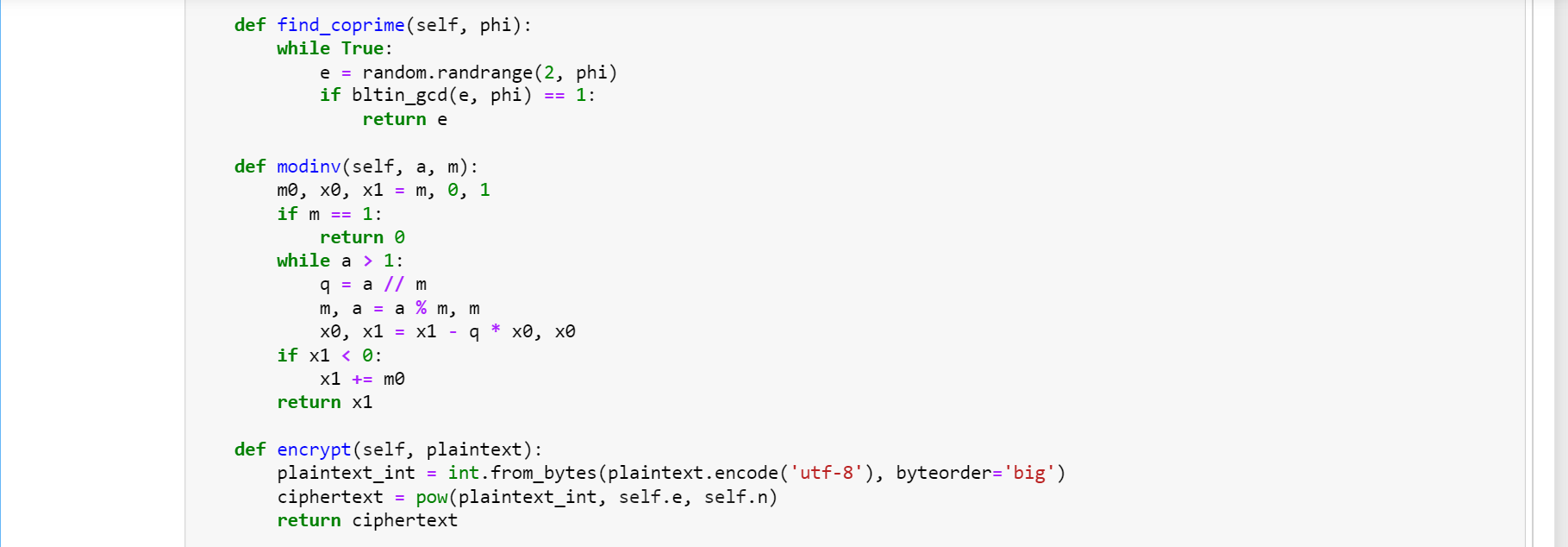
**SUMMER SEMESTER 2024**

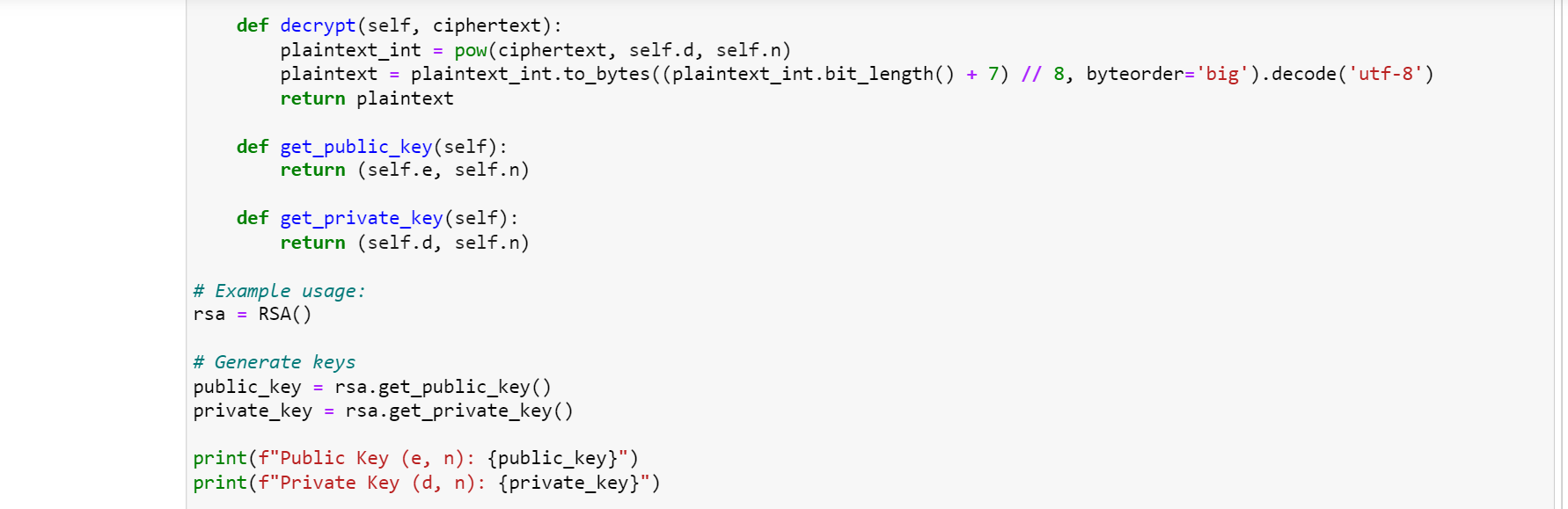
**APT3090 CRYPTOGRAPHY AND NETWORK SECURITY**

**Joy Kirui-664830**

**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)**







 **Initialization of Class (\_\_init\_\_)**: It initializes the RSA object with a key size, then generates two prime numbers ppp and qqq, calculates nnn and ϕ(n)\phi(n)ϕ(n), and generates the public and private keys eee and ddd respectively.

 **Random Generation of Prime (generate\_prime)**: It generates a random prime number of specified bit size.

 **Finding the CoPrime (find\_coprime)**: Finds a coprime integer eee to ϕ(n)\phi(n)ϕ(n).

 **Inverse of the Modular (modinv)**: Calculates the inverse of the modular of eee under modulo ϕ(n)\phi(n)ϕ(n).

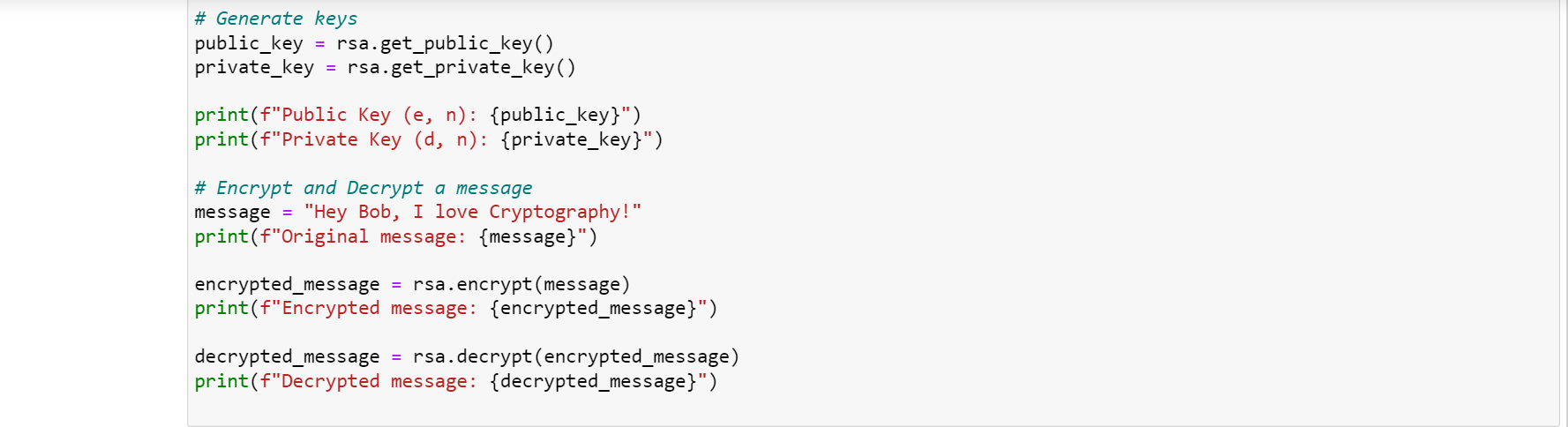
 **The Encryption (encrypt)**: It converts a plaintext message to its integer representation, then encrypts it using the public key.

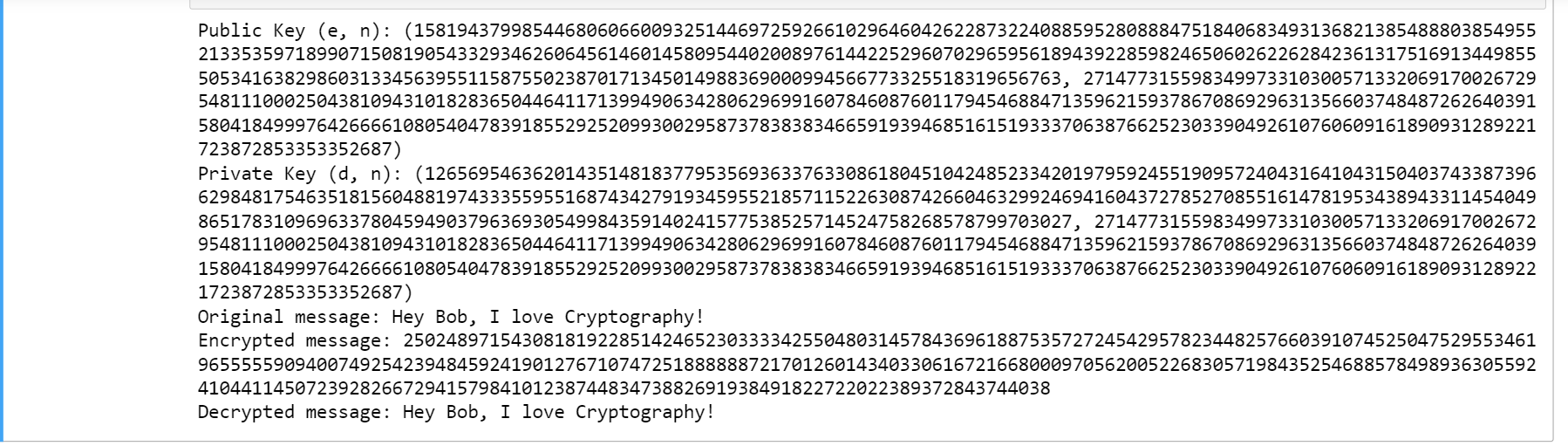
 **The Decryption (decrypt)**: It decrypts the integer ciphertext back to the plaintext message using the private key.

 **The Retrieval of the Key (get\_public\_key, get\_private\_key)**: It retrieves the public and the private keys.

## Results

In this scenario, Alice is sending Bob a message. The message is encrypted using the two randomly generated numbers p and q. The private key of Alice is generated and the shared public key is also generated.





## Second Scenario



Here Bob is replying to message is encrypted using the two randomly generated numbers p and q. The private key of Bob is generated and the shared public key is also generated.

