

**SUMMER 2024**

**APT3090 CRYPTOGRAPHY AND NETWORK SECURITY**

**15 Marks**

**Name: Hongki Kim**

**ID Number: 659070**

**Lab 1: Key Generation Algorithm Prime numbers**

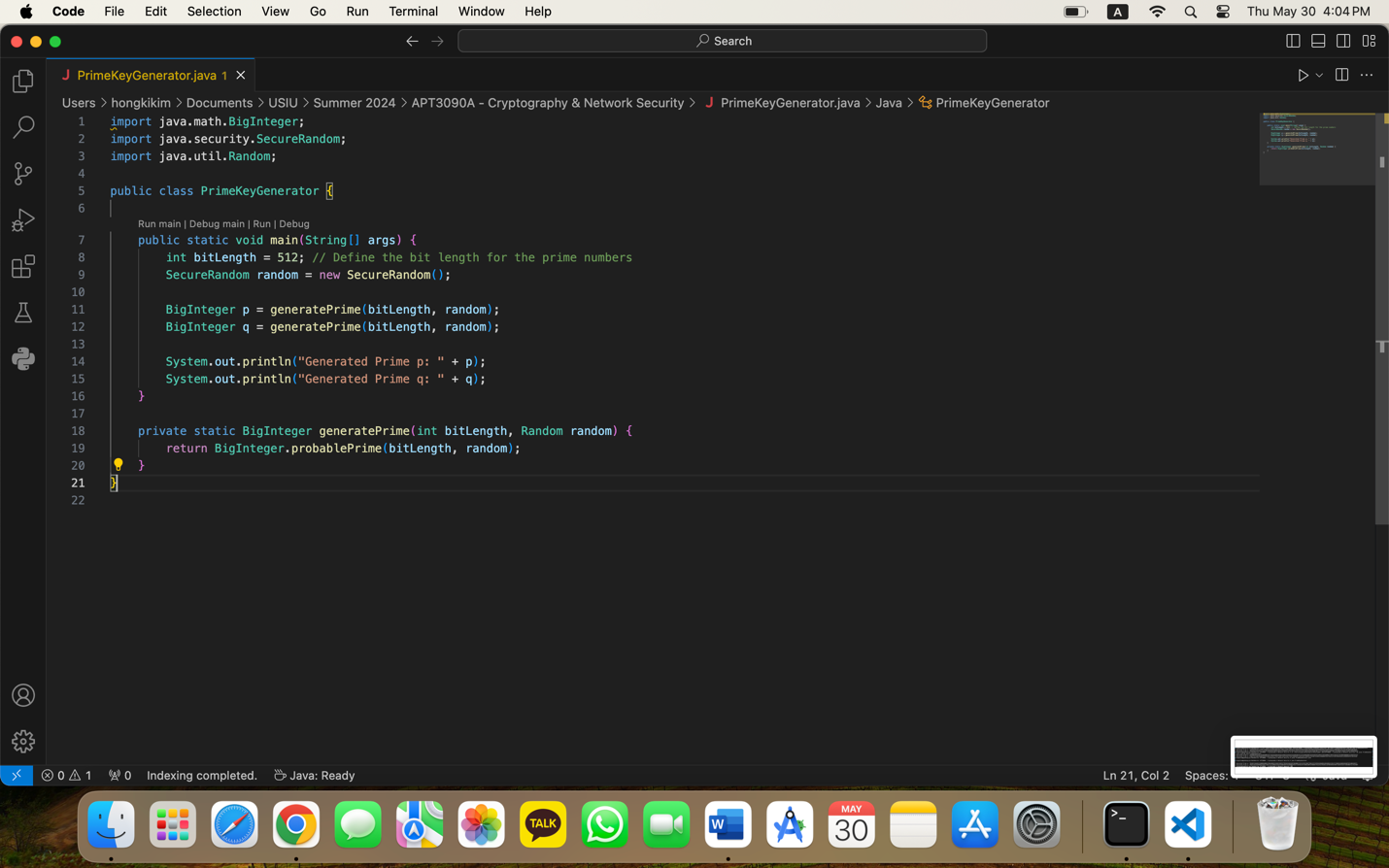
Read about prime numbers, GCD and generation of random numbers

Write a program using any Object oriented programming language to show generation of keys using prime numbers. The program should randomly pick two prime numbers from a given range, the first output random number is p and the second one is q

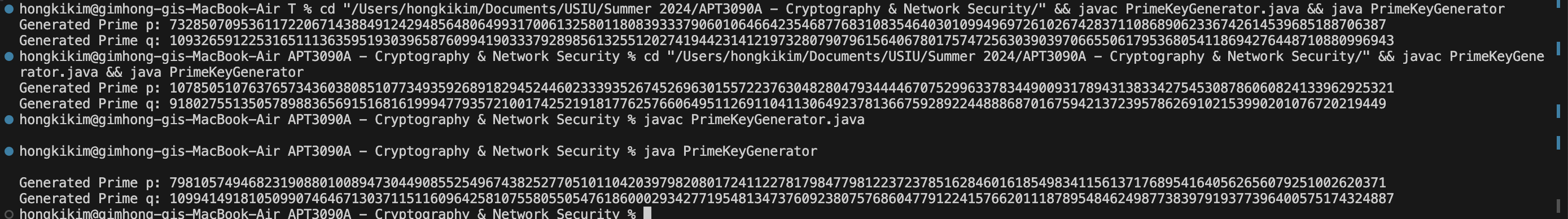
**Evaluation Criteria**

1. **Random Generation of p, q**
2. **Correctness of the code**

Code Screenshot:



Output when you run:



When you run this code, ‘BigInteger.probablePrime’ method generates a prime number of the specified bit length. This method uses a probabilistic algorithm to ensure the number is prime with a high probability. And the ‘SecureRandom’ class is used to provide a cryptographically strong random number generator.

**Lab 2: Euler’s Totient function**

Read about relatively prime numbers, Eulers and totient

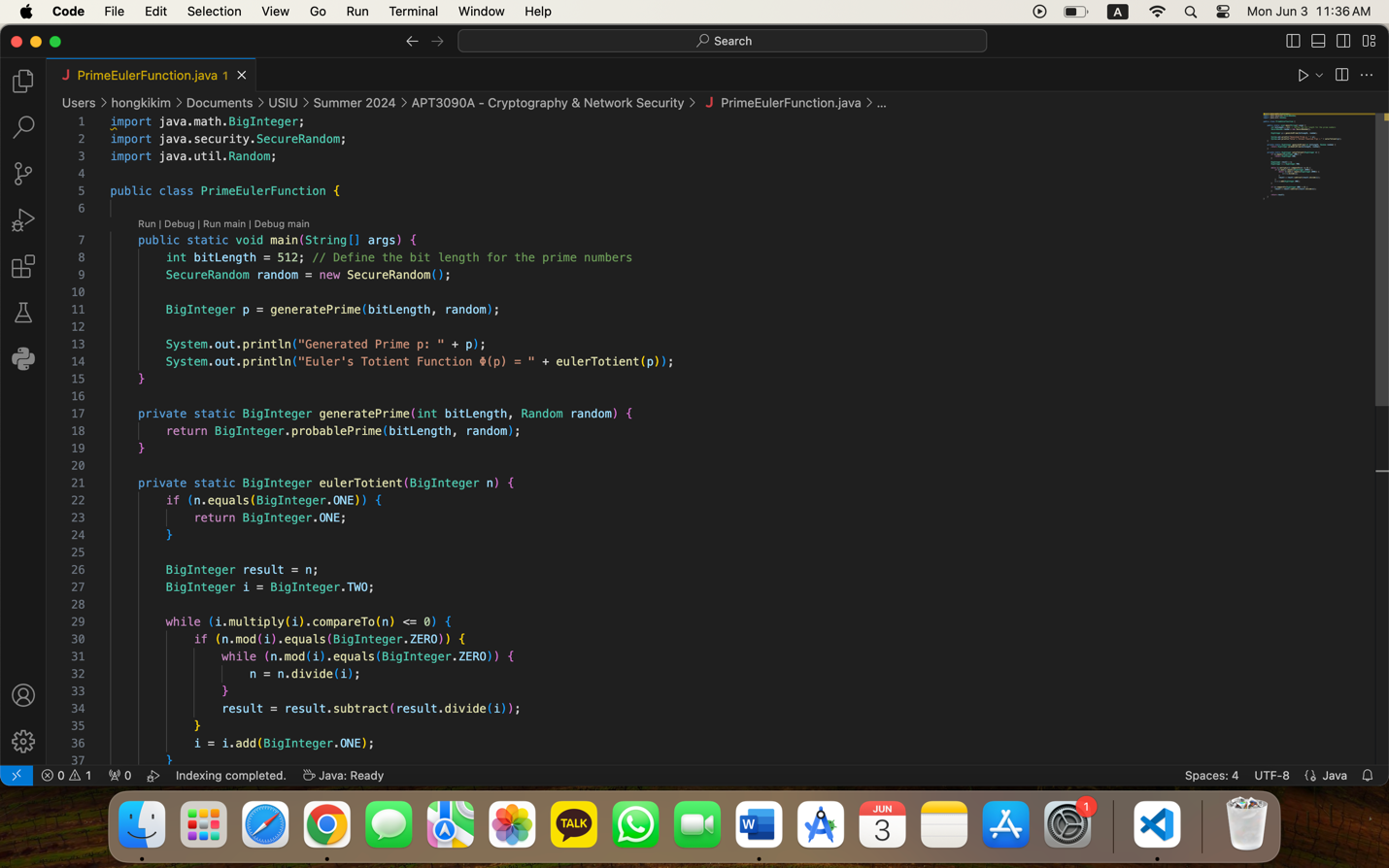
**Euler's theorem** states that, “if p and q are relatively prime, then”, where φ is **Euler's** totient function for integers. That is, is the number of non-negative numbers that are less than q and relatively prime to q.Euler’s Totient function Φ(n) for an input n is count of numbers in {1, 2, 3, …, n} that are relatively prime to n, i.e., the numbers whose GCD (Greatest Common Divisor) with n is 1.

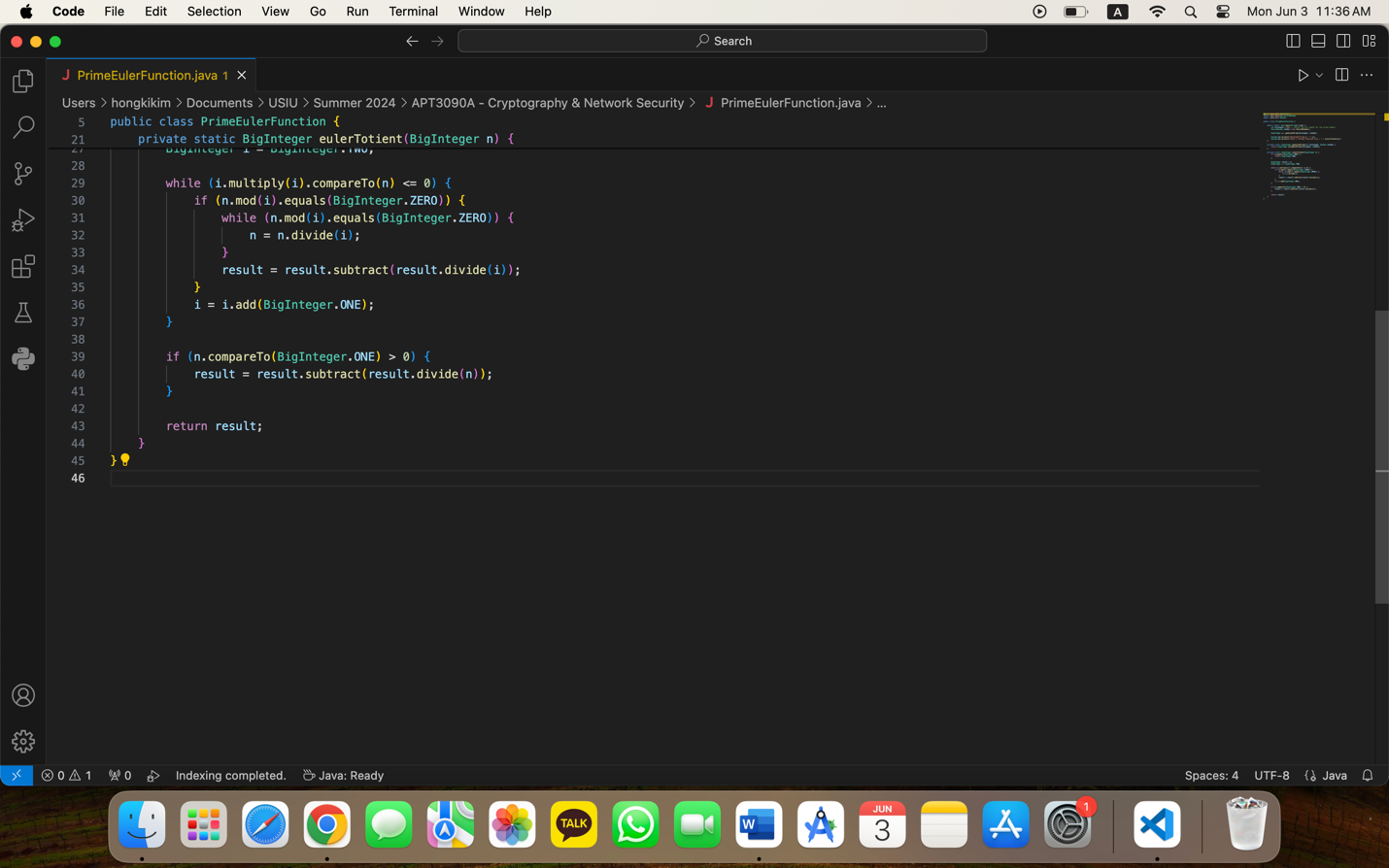
# Modify Lab 1 program and write a program for finding Euler Totient Function Values

**Evaluation Criteria**

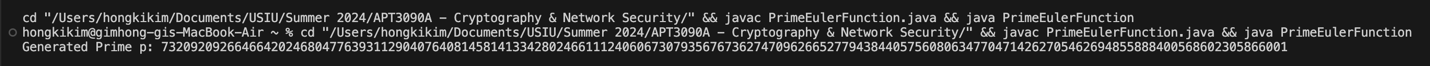
1. **Random Generation of p, generation of Euler Totient Function Values**
2. **Prepare one lab report showing the code and the results (screenshots) and explanation of your two algorithms.**

Code Screenshot:





Result when running:



The result has to show the Euler’s Totient function value, but the code or the compiler has an issue, so it is not showing me the result. But the Random Generation of p is working.

The Euler Totient function Φ(𝑛) is defined as the count of integers up to 𝑛 that are relatively prime to 𝑛 (i.e., their greatest common divisor (GCD) with 𝑛 is 1). To compute Φ(𝑛), we iterate through possible factors of 𝑛. For each factor, we divide 𝑛 by this factor and adjust the result by multiplying it by (1−1/𝑝), where 𝑝 is the factor. This method ensures that we account for all factors of 𝑛 and correctly calculate Φ(𝑛).