CSE 4000

Weekly presentation

Mazharul Islam – 1807102

```java
public static void main(String[] args) {
    int bit_length = 1024;
    Random rand = new SecureRandom();
    BigInteger p = BigInteger.probablePrime( bitLength: bit_length/8, rand);
    //BigInteger p = new BigInteger("11");
    System.out.println("P : " + p);
    BigInteger q = BigInteger.probablePrime( bitLength: bit_length/8, rand);
    //BigInteger q = new BigInteger("7");
    System.out.println("Q : "+q);
    BigInteger m = p.multiply(q);
    System.out.println("M : "+m);
    //BigInteger r = BigInteger.probablePrime(bit_length/8, rand);
    BigInteger r = new BigInteger( val: "2");
    System.out.println("R : "+r);
    BigInteger msg = new BigInteger( val: "3");

    // Encryption
    BigInteger cipher = (msg.add(r.multiply(p.pow(q.intValue()))));
    cipher = cipher.mod(m);
    System.out.println(cipher);

    // Decryption
    msg = cipher.mod(p);
    System.out.println(msg);
}
```

OUTPUT:

```
Main
"C:\Users\MAZHARUL ISLAM\.jdks\openjdk-18.0.1.1\bin\java.exe" "-javaagent:C:\Program Files\JetBrains\IntelliJ IDEA Commu
P : 26029181147526675194439830758022420173 7
Q : 33661818905356795291768199115308700686 3
M : 87618958204277011833400833383140212722153704087804292607335185661390815521031
R : 2
Message : 3
Cipher : 25
Plaintext : 3
```