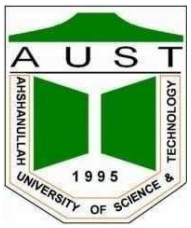
Ahsanullah University of Science & Technology
Department of Computer Science & Engineering

FALL 2020



Assignment – 01
(RSA)

Data Communication

CSE 3211

Submitted To

Mr. H M Zabir Haque

Assistant Professor
Department of CSE, AUST

Submitted By:

Name: Atanu Saha

ID: 17.02.04.003
Section: A

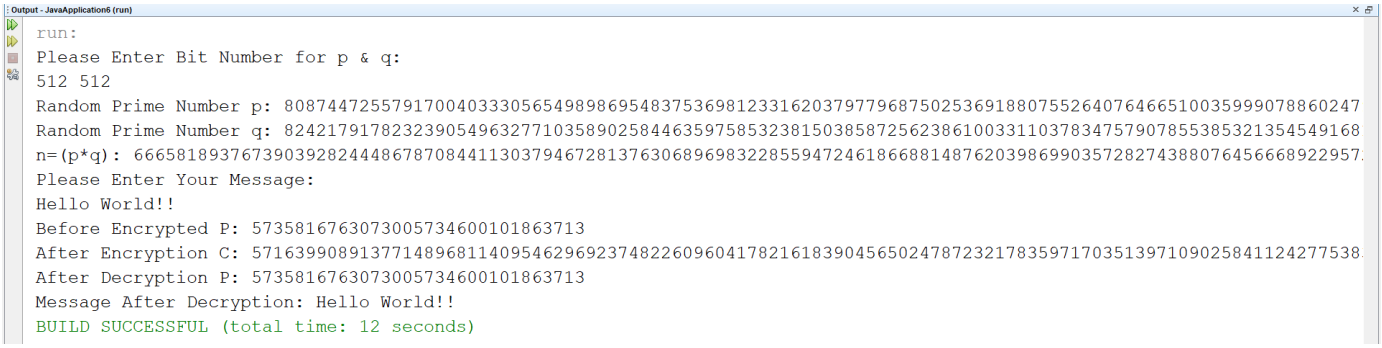
Date of submission:11-09-2021

```
package javaapplication6;

import java.math.BigInteger;
import java.util.Random;
import java.util.Scanner;

/**
 *
 * @author Atanu saha
 */
public class JavaApplication6 {


    public static void main(String[] args) {
        BigInteger p, q;
        Integer bit;
        System.out.println("Please Enter Bit Number for p & q: ");
        Scanner s = new Scanner(System.in);
        bit = s.nextInt();
        p = BigInteger.probablePrime(bit, new Random());
        q = BigInteger.probablePrime(bit, new Random());
        System.out.println("Random Prime Number p: " + p);
        System.out.println("Random Prime Number q: " + q);
        BigInteger n;
        n = p.multiply(q);
        System.out.println("n=(p*q): " + n);
        BigInteger one = BigInteger.ONE;
        BigInteger psub, qsub;
        psub = p.subtract(one);
        qsub = q.subtract(one);
```

```
        BigInteger phi;
        phi = psub.multiply(qsub);



       BigInteger e1 = BigInteger.TEN;
        while (e1.compareTo(phi) < 0) {
           if (e1.gcd(phi).equals(BigInteger.ONE)) {
              break;
           } else {
              e1 = e1.add(BigInteger.ONE);
           }
        }


         BigInteger d = e1.modInverse(phi);
        //System.out.println("d = e^-1 mod phi: " + d);
        BigInteger PP, C, PD;
        System.out.println("Please Enter Your Message: ");
        s.nextLine();
        String message = s.nextLine();
        PP = new BigInteger(message.getBytes());
        System.out.println("Before Encrypted P: " + PP);
        C = PP.modPow(e1, n);
        System.out.println("After Encryption C: " + C);
        PD = C.modPow(d, n);
        System.out.println("After Decryption P: " + PD);
        System.out.println("Message After Decryption: " + new
String(PD.toByteArray()));
    }
```

}

Output:


Output - JavaApplication6 (run)
run:
Please Enter Bit Number for p & q:
512 512
Random Prime Number p: 8087447255791700403330565498986954837536981233162037977968750253691880755264076466510035999078860247
Random Prime Number q: 8242179178232390549632771035890258446359758532381503858725623861003311037834757907855385321354549168
n=(p*q): 6665818937673903928244486787084411303794672813763068969832285594724618668814876203986990357282743880764566689229577
Please Enter Your Message:
Hello World!!
Before Encrypted P: 573581676307300573460010186 3713
After Encryption C: 571639908913771489681140954629692374822609604178216183904565024787232178359717035139710902584112427753 8
After Decryption P: 573581676307300573460010186 3713
Message After Decryption: Hello World!!
BUILD SUCCESSFUL (total time: 12 seconds)