Name: ABHISHEK DUBEY Roll No: 2019005

CS3006: Network Security & Cryptography Assignment
Course Instructor: Dr. Neelam Dayal

This is a client-server application for demonstrating AES and RSA encryption. The client application is a react web application that runs in the browser window (Prefer Google Chrome).

The server runs on the NodeJS runtime environment that enables to establish communication through the express framework that is used to make APIs that connect the client with the server.

Some examples with different inputs and outputs screenshots of the server and client are attached at the bottom of this document as well as in the output folder.

Note: Please input values less than 2^{16} - 1 i.e. 65535 because the application only expects values of 16 bytes.

Installation Guide

Prerequisite

The system must have NodeJs installed. To install NodeJs on your machine visit this link

There are 2 folders, server, and client.

Installing and Running Server

Step 1: Navigate to the server folder

Step 2: Install all the dependencies by the following command in the terminal

```
npm install
```

Step 3: Run the server, pass p, q, e (RSA parameters).

Note: If the user does not pass any parameters, p=907, q=773, and e=11 will be assigned by default.

```
    npm start
        or
    npm start p q e
```

Now, the server will listen on port 4000. check the health of the server by opening localhost:4000

We can see the server's log on the terminal when the client sends any data.

Installing and Running Client

Step 1: Navigate to the client folder

Step 2: Install all the dependencies by the following command in the terminal

```
   npm install
```

Step 3: Run the client application by the following command

```
   npm start
```

Now, the client will listen on port 3000. A browser window should open at port 3000: localhost:3000 and the form will take values of the message, secret key, p, q, and e. After submitting the values, the user can see the client's output on the browser itself, and the server's output will appear on the server's terminal.

Folder and Files

Below are the files and folder architecture of the system.
Folder and files can be distinguished by looking at the extension

```
server
  functions
    index.js          // Export necessary functions used by server to decrypt
    AES.js            // Implements AES Decryption algorithm
    RSA.js            // Implements RSA Key generation and Encryption-Decryption algorithm
    HashAlgo.js        // Implements hash function to create digest
  server.js      // Main file to start server, contains express app and logic of decryption workflow
-----------------------------------
client
  src
    functions
      index.js         // Export all necessary functions to be used by server to decrypt
      AES.js           // Implements AES Decryption algorithm
      RSA.js           // Implements RSA Key generation and Encryption-Decryption algorithm
      HashAlgo.js      // Implements hash function to create digest
    components
      Display.jsx      // React component to render output
    App.jsx            // Main file containing logic of encryption workflow, takes input and
communication with server and renders the output
    App.css            // Stylesheet for the browser window
    index.css          // Stylesheet for root HTML
    index.js           // Renders React component on the browser
  public               // this folder is for React architecture. has some html, png, svg file
-----------------------------------
output
  client-1.png         // client example output 1
  server-1.png         // server example output 1
  client-2.png         // client example output 2
  server-2.png         // server example output 2
  client-3.png         // client example output 3
  server-3.png         // server example output 3
```

Functions Description

Below are the files and folder architecture of the system.
Folder and files can be distinguished by looking at the extension

Functions on the Server-side:

1. main(): Main function that handles server-side computation workflow.
2. printOutput(): Outputs all the data to the terminal
3. RSAKeyGenerator(p, q, e): Generates public key and private key
4. RSAAlgo(data, key: {n, d or e}): Encrypt-Decrypt data using RSA algorithm
5. AESDecrypt(cipherText, secretKey): Decrypts cipherText using secretKey
6. hashAlgo(text): converts text to 16 byte hash

Implementation of the last 4 functions can be found in the ‘functions’ folder

Functions on the Client-side:

1. main(): Main function that handles client-side computation workflow.
2. useEffect(): fetch server’s public key on connection through an API
3. sendDataToServer(): sends data to server using an API
4. RSAKeyGenerator(p, q, e): Generates public key and private key
5. RSAAlgo(data, key: {n, d or e}): Encrypt-Decrypt data using RSA algorithm
6. AESEncrypt(plainText, secretKey): Encrypts plainText using secretKey
7. hashAlgo(text): converts text to 16-byte hash

Implementation of the last 4 functions can be found in the ‘functions’ folder

Functions in the ‘functions’ folder:

RSAAlgo.js:

1. power(x, y, m) : calculates (x^y % m) of very large numbers using modular arithmetic
2. modInverse(a, m) : calculates modulo inverse: (1/a) % m
3. gcd(x, y) : calculates GCD of two numbers
4. lcm(n1, n2) : calculates LCM of two numbers
5. RSAKeyGenerator(p, q, e) : generates a public and a private key
6. RSAAlgo(data, key) : Encrypt/Decrypt data using public/private key

HashAlgo.js:

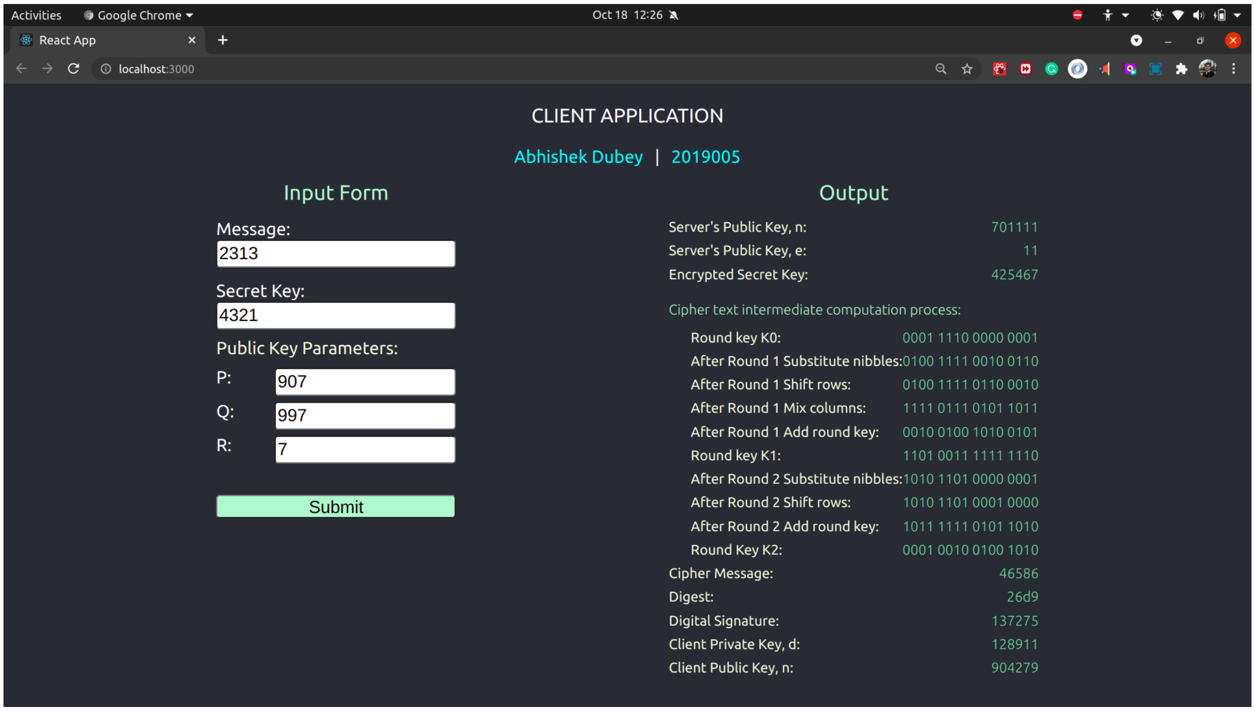
1. hashAlgo(keyString) : converts string to 16-byte hexadecimal hash value.

AES.js:

1. AESEncrypt(plainText, secretKey) : return cipherText and output log
2. AESDecrypt(cipherText, secretKey) : returns plainText and output log
3. inverseMixColumns(state) : return state after inverse mix column
4. mixColumns(state) : returns state after mix column
5. shiftRows(state) : returns state after shift row operation
6. subNibbles(sbox, state) : returns substitution nibble from sbox and state.
7. addRoundKey(key, state) : returns add round key
8. keyExpansion(key) : returns pre round key (K0), round 1 key (K1) and round 2 key (K2)

Output Screen-Shots

Client 1:



CLIENT APPLICATION

Abhishek Dubey | 2019005

Input Form

Message: 2313

Secret Key: 4321

Public Key Parameters:

P: 907

Q: 997

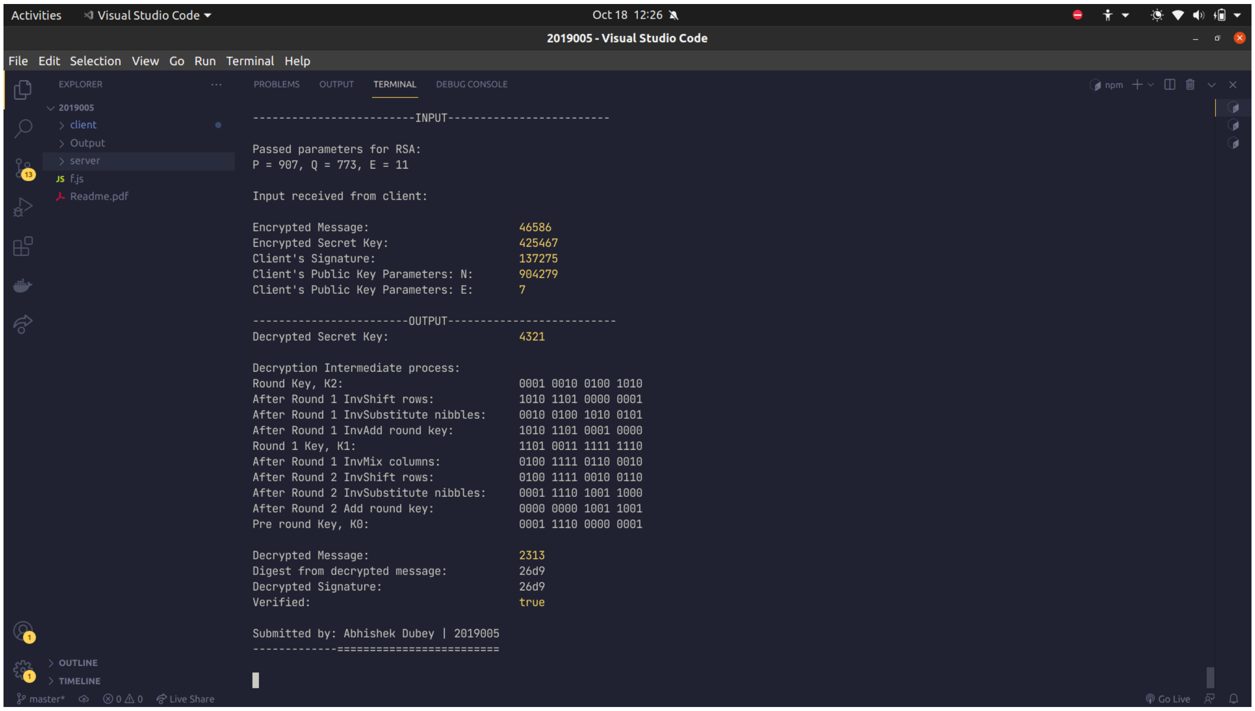
R: 7

Submit

Output

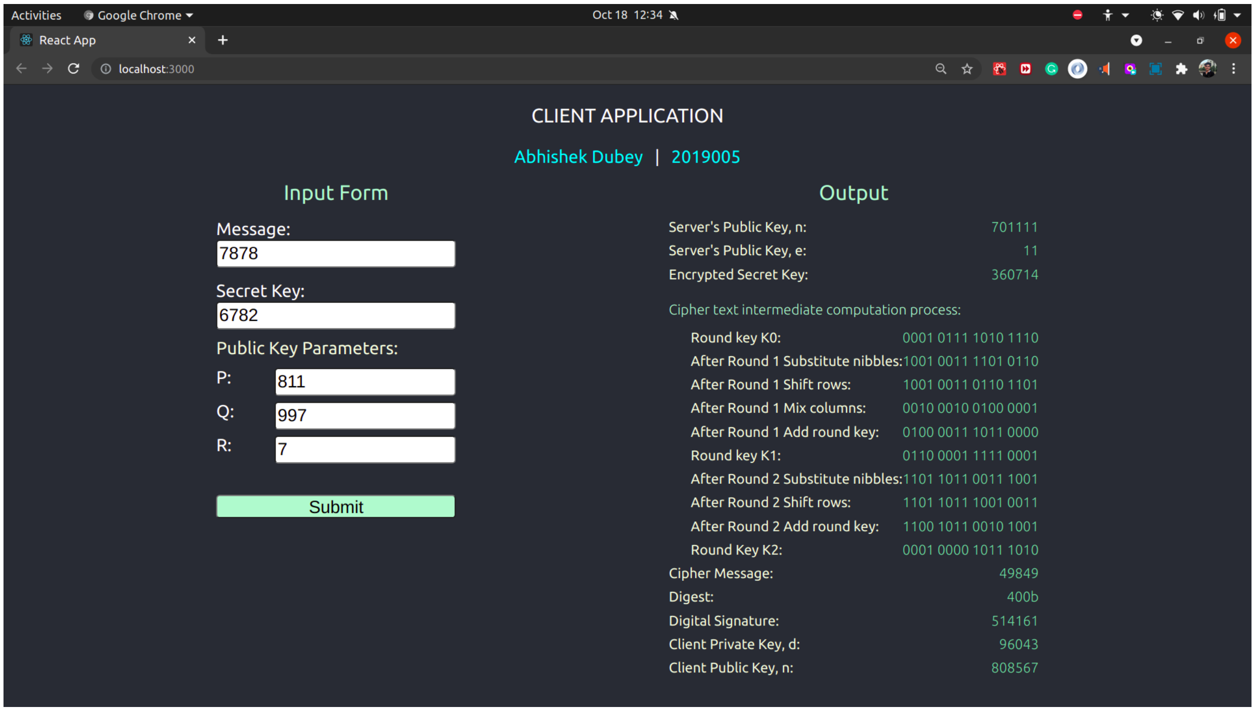
```
Server's Public Key, n:                         701111
Server's Public Key, e:                             11
Encrypted Secret Key:                           425467

Cipher text intermediate computation process:

    Round key K0:                        0001 1110 0000 0001
    After Round 1 Substitute nibbles:0100 1111 0010 0110
    After Round 1 Shift rows:            0100 1111 0110 0010
    After Round 1 Mix columns:           1111 0111 0101 1011
    After Round 1 Add round key:         0010 0100 1010 0101
    Round key K1:                        1101 0011 1111 1110
    After Round 2 Substitute nibbles:1010 1101 0000 0001
    After Round 2 Shift rows:            1010 1101 0001 0000
    After Round 2 Add round key:         1011 1111 0101 1010
    Round Key K2:                        0001 0010 0100 1010
Cipher Message:                                  46586
Digest:                                           26d9
Digital Signature:                              137275
Client Private Key, d:                          128911
Client Public Key, n:                           904279
```

Server 1:



```
------------------------INPUT------------------------

Passed parameters for RSA:
P = 907, Q = 773, E = 11

Input received from client:

Encrypted Message:                        46586
Encrypted Secret Key:                     425467
Client's Signature:                       137275
Client's Public Key Parameters: N:        904279
Client's Public Key Parameters: E:        7

-----------------------OUTPUT-------------------------
Decrypted Secret Key:                     4321

Decryption Intermediate process:
Round Key, K2:                            0001 0010 0100 1010
After Round 1 InvShift rows:              1010 1101 0000 0001
After Round 1 InvSubstitute nibbles:      0010 0100 1010 0101
After Round 1 InvAdd round key:           1010 1101 0001 0000
Round 1 Key, K1:                          1101 0011 1111 1110
After Round 1 InvMix columns:             0100 1111 0110 0010
After Round 2 InvShift rows:              0100 1111 0010 0110
After Round 2 InvSubstitute nibbles:      0001 1110 1001 1000
After Round 2 Add round key:              0000 0000 1001 1001
Pre round Key, K0:                        0001 1110 0000 0001

Decrypted Message:                        2313
Digest from decrypted message:            26d9
Decrypted Signature:                      26d9
Verified:                                 true

Submitted by: Abhishek Dubey | 2019005
-------------========================
```

Client 2:



CLIENT APPLICATION

Abhishek Dubey | 2019005

Input Form

Message: 7878

Secret Key: 6782

Public Key Parameters:

P: 811

Q: 997

R: 7

Submit

Output

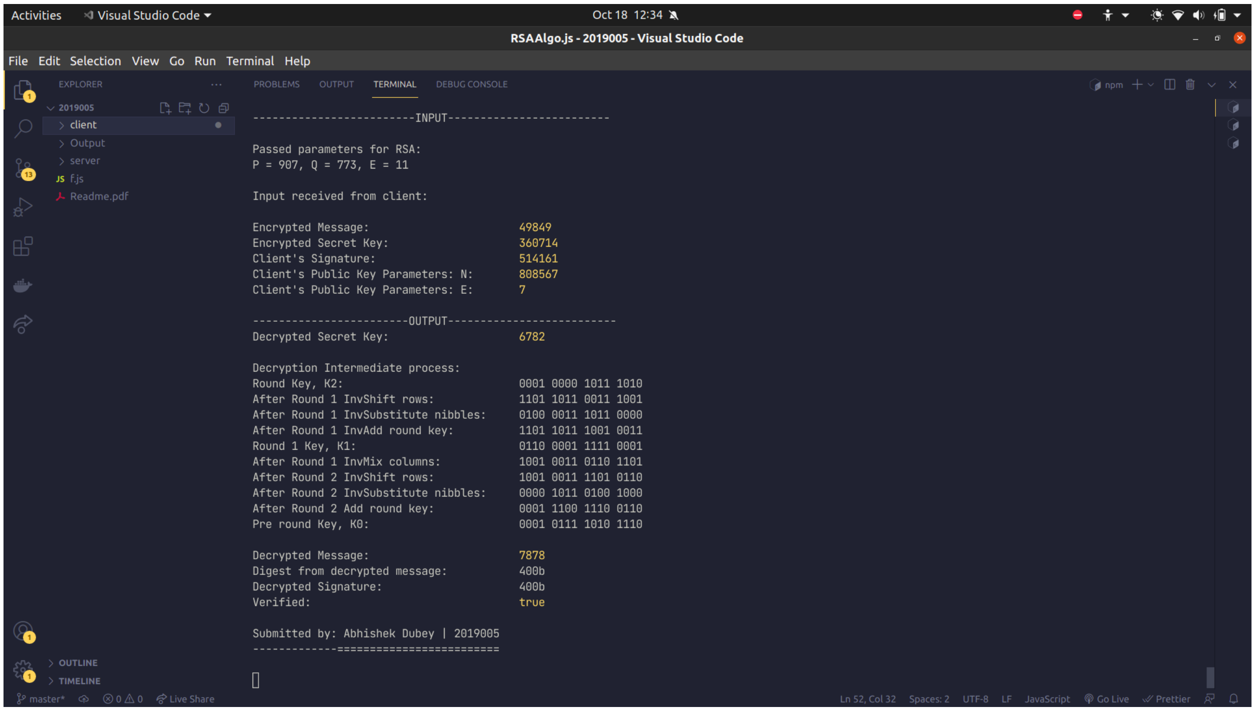
Server's Public Key, n:	701111
Server's Public Key, e:	11
Encrypted Secret Key:	360714

Cipher text intermediate computation process:

Round key K0:	0001 0111 1010 1110
After Round 1 Substitute nibbles:	1001 0011 1101 0110
After Round 1 Shift rows:	1001 0011 0110 1101
After Round 1 Mix columns:	0010 0010 0100 0001
After Round 1 Add round key:	0100 0011 1011 0000
Round key K1:	0110 0001 1111 0001
After Round 2 Substitute nibbles:	1101 1011 0011 1001
After Round 2 Shift rows:	1101 1011 1001 0011
After Round 2 Add round key:	1100 1011 0010 1001
Round Key K2:	0001 0000 1011 1010

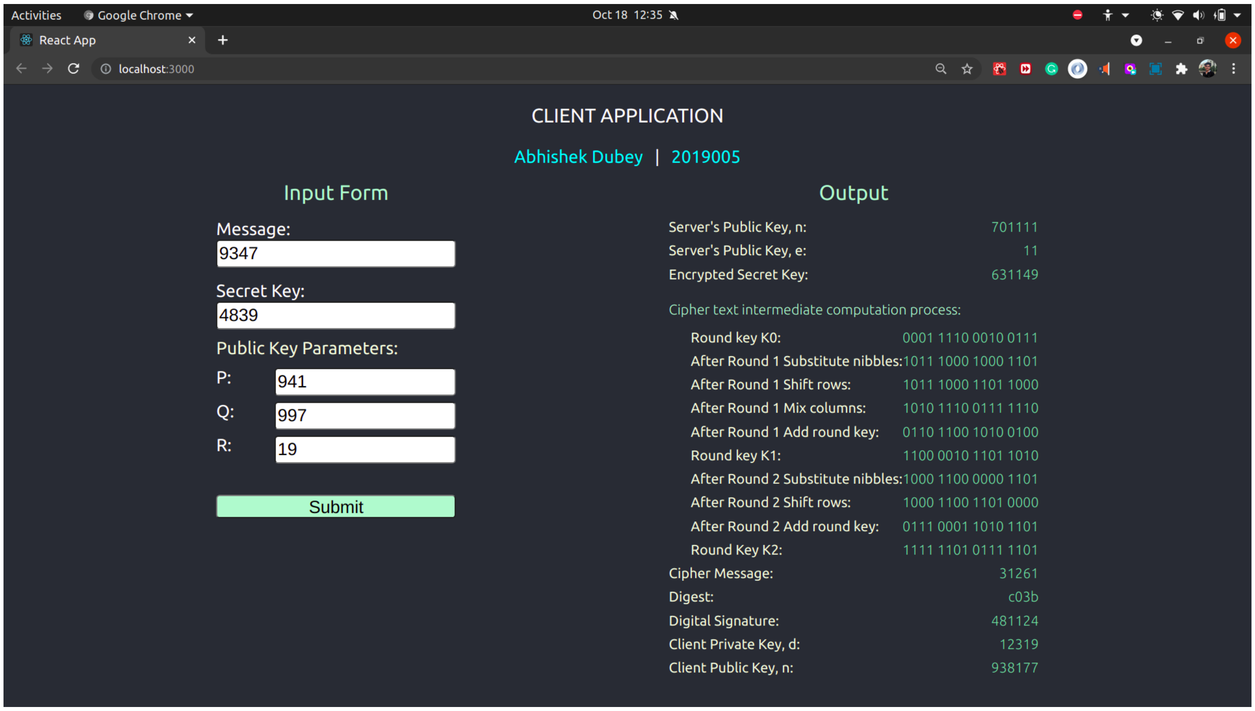
Cipher Message:	49849
Digest:	400b
Digital Signature:	514161
Client Private Key, d:	96043
Client Public Key, n:	808567

Server 2:



```
-------------------------INPUT-------------------------

Passed parameters for RSA:
P = 907, Q = 773, E = 11

Input received from client:

Encrypted Message:                       49849
Encrypted Secret Key:                    360714
Client's Signature:                      514161
Client's Public Key Parameters: N:       808567
Client's Public Key Parameters: E:       7

------------------------OUTPUT--------------------------
Decrypted Secret Key:                    6782

Decryption Intermediate process:
Round Key, K2:                           0001 0000 1011 1010
After Round 1 InvShift rows:             1101 1011 0011 1001
After Round 1 InvSubstitute nibbles:     0100 0011 1011 0000
After Round 1 InvAdd round key:          1101 1011 1001 0011
Round 1 Key, K1:                         0110 0001 1111 0001
After Round 1 InvMix columns:            1001 0011 0110 1101
After Round 2 InvShift rows:             1001 0011 1101 0110
After Round 2 InvSubstitute nibbles:     0000 1011 0100 1000
After Round 2 Add round key:             0001 1100 1110 0110
Pre round Key, K0:                       0001 0111 1010 1110

Decrypted Message:                       7878
Digest from decrypted message:           400b
Decrypted Signature:                     400b
Verified:                                true

Submitted by: Abhishek Dubey | 2019005
-------------=========================
```

Client 3:



CLIENT APPLICATION

Abhishek Dubey | 2019005

Input Form

Message: 9347

Secret Key: 4839

Public Key Parameters:

P: 941

Q: 997

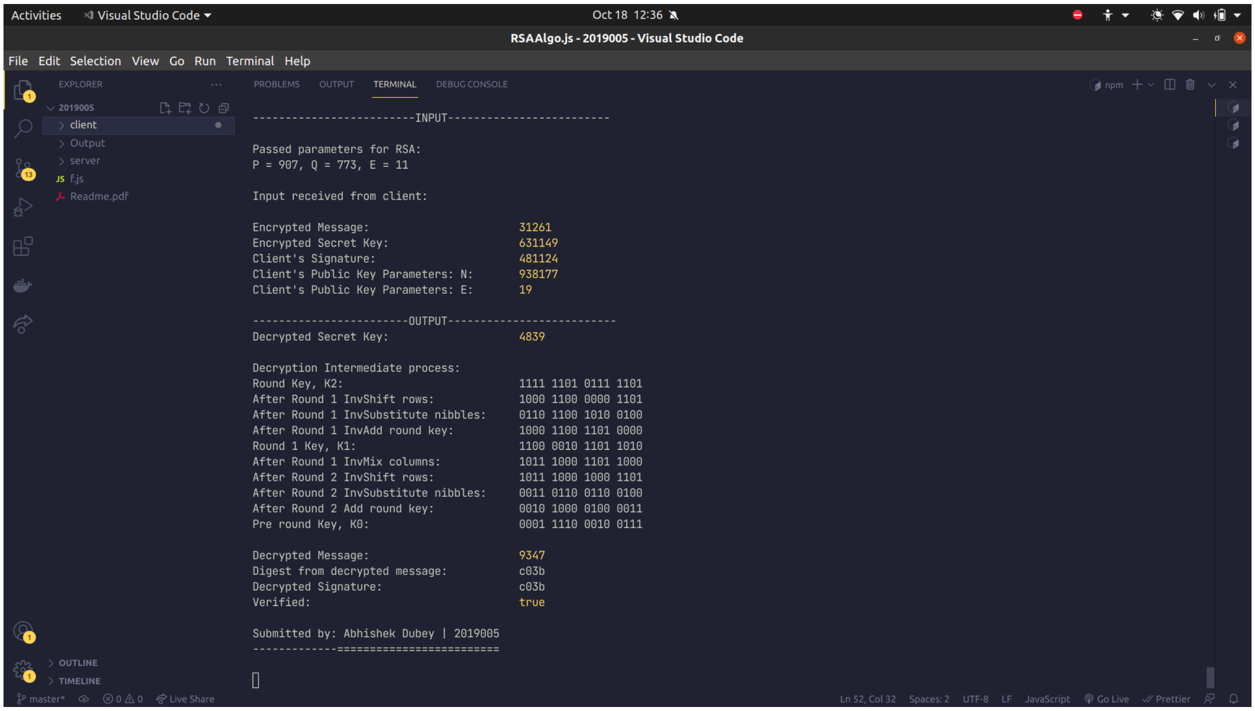
R: 19

Submit

Output

Server's Public Key, n:	701111
Server's Public Key, e:	11
Encrypted Secret Key:	631149
Cipher text intermediate computation process:	
Round key K0:	0001 1110 0010 0111
After Round 1 Substitute nibbles:	1011 1000 1000 1101
After Round 1 Shift rows:	1011 1000 1101 1000
After Round 1 Mix columns:	1010 1110 0111 1110
After Round 1 Add round key:	0110 1100 1010 0100
Round key K1:	1100 0010 1101 1010
After Round 2 Substitute nibbles:	1000 1100 0000 1101
After Round 2 Shift rows:	1000 1100 1101 0000
After Round 2 Add round key:	0111 0001 1010 1101
Round Key K2:	1111 1101 0111 1101
Cipher Message:	31261
Digest:	c03b
Digital Signature:	481124
Client Private Key, d:	12319
Client Public Key, n:	938177

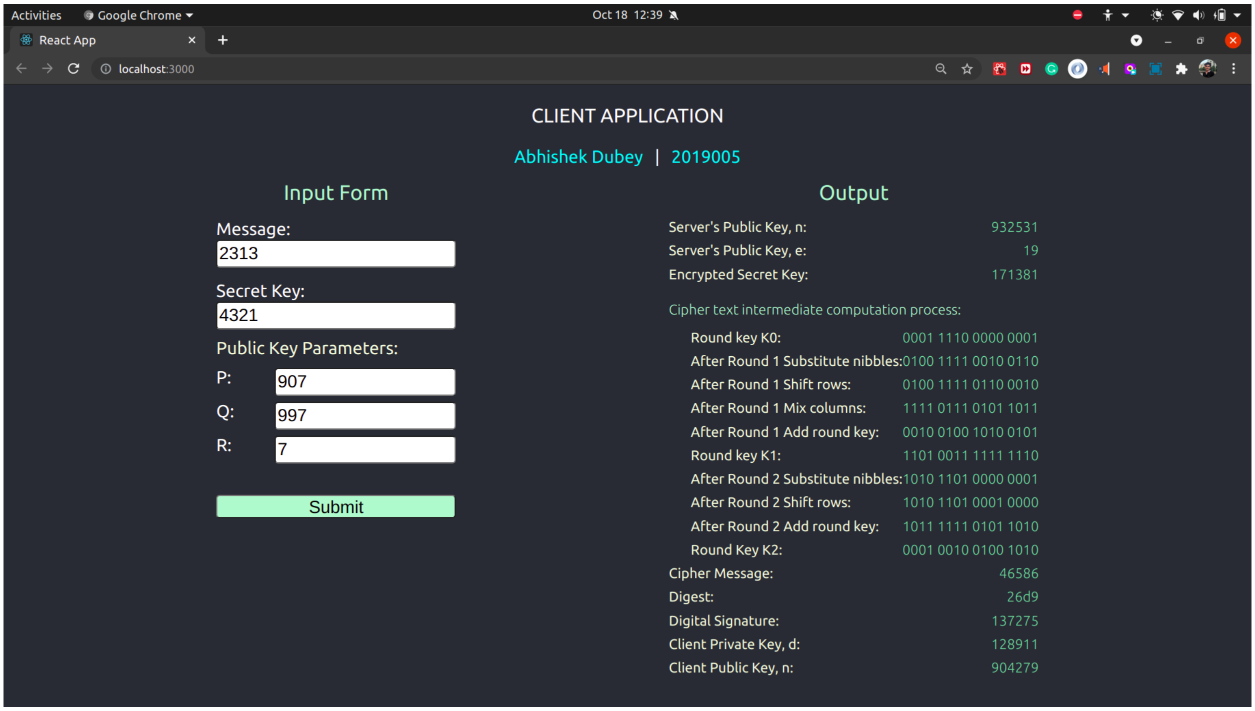
Server 3:



Activities
Visual Studio Code
Oct 18 12:36
RSAAlgo.js - 2019005 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
2019005
client
Output
server
f.js
Readme.pdf
PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE
OUTLINE
TIMELINE
master*
Live Share
Ln 52, Col 32 Spaces: 2 UTF-8 LF JavaScript Go Live Prettier

```
-------------------------INPUT------------------------

Passed parameters for RSA:
P = 907, Q = 773, E = 11

Input received from client:

Encrypted Message:                        31261
Encrypted Secret Key:                     631149
Client's Signature:                       481124
Client's Public Key Parameters: N:        938177
Client's Public Key Parameters: E:        19

------------------------OUTPUT-------------------------
Decrypted Secret Key:                     4839

Decryption Intermediate process:
Round Key, K2:                            1111 1101 0111 1101
After Round 1 InvShift rows:              1000 1100 0000 1101
After Round 1 InvSubstitute nibbles:      0110 1100 1010 0100
After Round 1 InvAdd round key:           1000 1100 1101 0000
Round 1 Key, K1:                          1100 0010 1101 1010
After Round 1 InvMix columns:             1011 1000 1101 1000
After Round 2 InvShift rows:              1011 1000 1000 1101
After Round 2 InvSubstitute nibbles:      0011 0110 0110 0100
After Round 2 Add round key:              0010 1000 0100 0011
Pre round Key, K0:                        0001 1110 0010 0111

Decrypted Message:                        9347
Digest from decrypted message:            c03b
Decrypted Signature:                      c03b
Verified:                                 true

Submitted by: Abhishek Dubey | 2019005
-------------=========================
```

Client 4:



CLIENT APPLICATION

Abhishek Dubey | 2019005

Input Form

Message: 2313

Secret Key: 4321

Public Key Parameters:

P: 907

Q: 997

R: 7

Submit

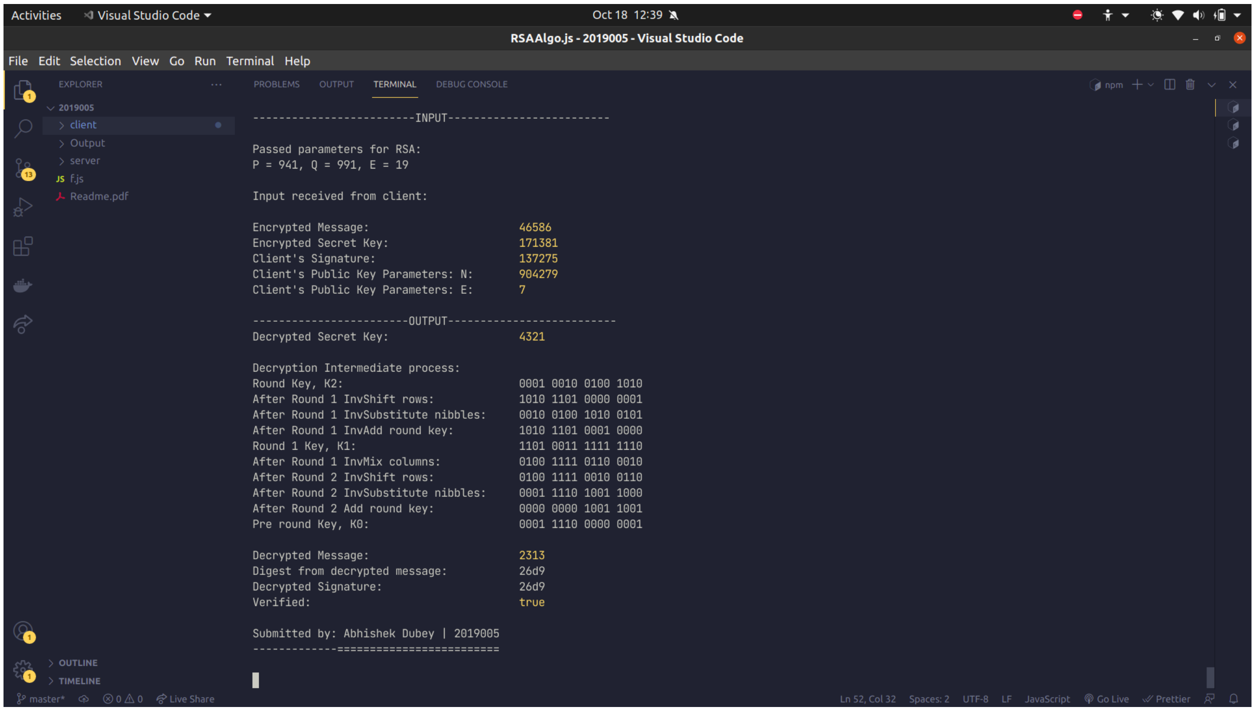
Output

Server's Public Key, n:	932531
Server's Public Key, e:	19
Encrypted Secret Key:	171381

Cipher text intermediate computation process:

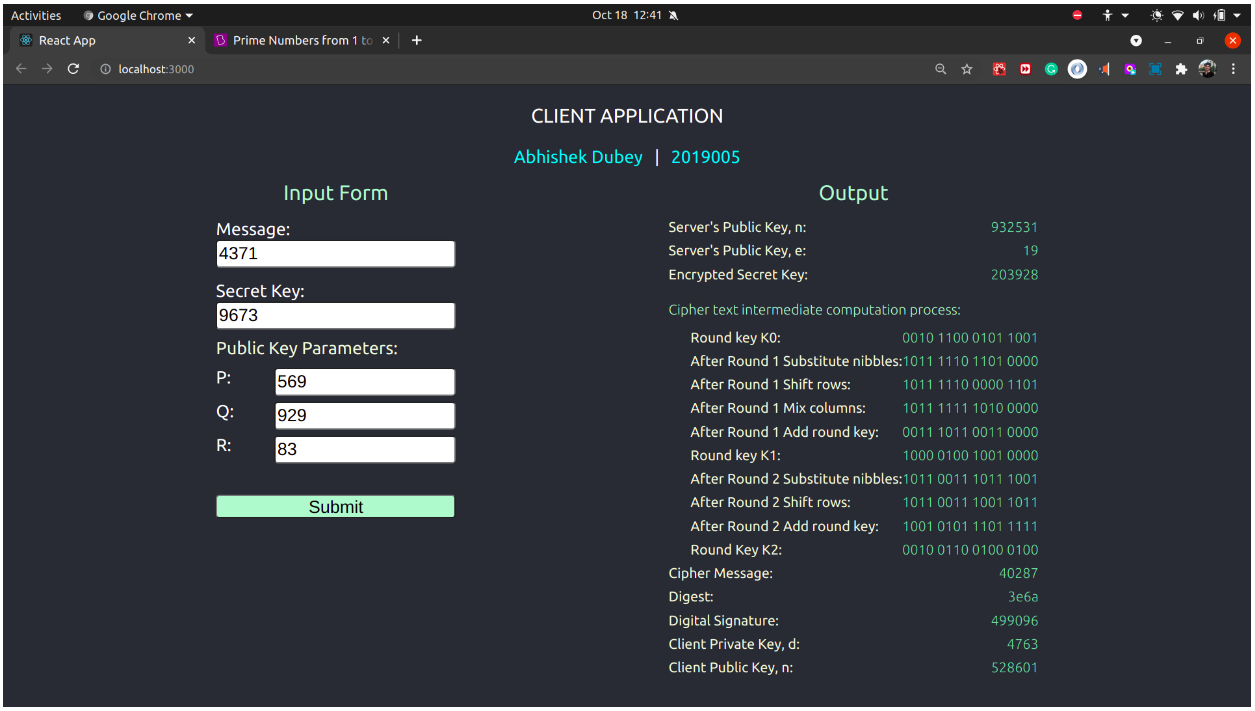
Round key K0:	0001 1110 0000 0001
After Round 1 Substitute nibbles:	0100 1111 0010 0110
After Round 1 Shift rows:	0100 1111 0110 0010
After Round 1 Mix columns:	1111 0111 0101 1011
After Round 1 Add round key:	0010 0100 1010 0101
Round key K1:	1101 0011 1111 1110
After Round 2 Substitute nibbles:	1010 1101 0000 0001
After Round 2 Shift rows:	1010 1101 0001 0000
After Round 2 Add round key:	1011 1111 0101 1010
Round Key K2:	0001 0010 0100 1010
Cipher Message:	46586
Digest:	26d9
Digital Signature:	137275
Client Private Key, d:	128911
Client Public Key, n:	904279

Server 4:



```
------------------------INPUT------------------------

Passed parameters for RSA:
P = 941, Q = 991, E = 19

Input received from client:

Encrypted Message:                        46586
Encrypted Secret Key:                     171381
Client's Signature:                       137275
Client's Public Key Parameters: N:        904279
Client's Public Key Parameters: E:        7

-----------------------OUTPUT-------------------------
Decrypted Secret Key:                     4321

Decryption Intermediate process:
Round Key, K2:                            0001 0010 0100 1010
After Round 1 InvShift rows:              1010 1101 0000 0001
After Round 1 InvSubstitute nibbles:      0010 0100 1010 0101
After Round 1 InvAdd round key:           1010 1101 0001 0000
Round 1 Key, K1:                          1101 0011 1111 1110
After Round 1 InvMix columns:             0100 1111 0110 0010
After Round 2 InvShift rows:              0100 1111 0010 0110
After Round 2 InvSubstitute nibbles:      0001 1110 1001 1000
After Round 2 Add round key:              0000 0000 1001 1001
Pre round Key, K0:                        0001 1110 0000 0001

Decrypted Message:                        2313
Digest from decrypted message:            26d9
Decrypted Signature:                      26d9
Verified:                                 true

Submitted by: Abhishek Dubey | 2019005
-------------=========================
```

Client 5:



CLIENT APPLICATION

Abhishek Dubey | 2019005

Input Form

Message:
4371

Secret Key:
9673

Public Key Parameters:

P: 569

Q: 929

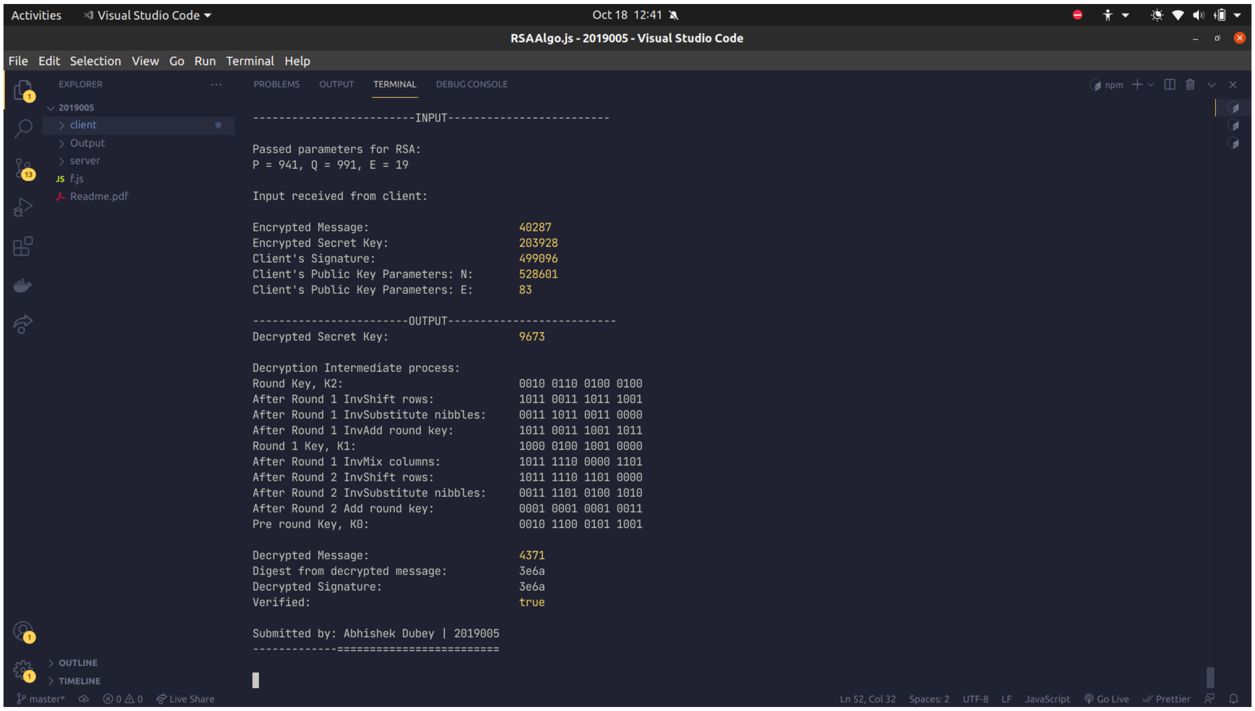
R: 83

Submit

Output

```
Server's Public Key, n:                          932531
Server's Public Key, e:                              19
Encrypted Secret Key:                            203928

Cipher text intermediate computation process:

    Round key K0:                       0010 1100 0101 1001
    After Round 1 Substitute nibbles:1011 1110 1101 0000
    After Round 1 Shift rows:           1011 1110 0000 1101
    After Round 1 Mix columns:          1011 1111 1010 0000
    After Round 1 Add round key:        0011 1011 0011 0000
    Round key K1:                       1000 0100 1001 0000
    After Round 2 Substitute nibbles:1011 0011 1011 1001
    After Round 2 Shift rows:           1011 0011 1001 1011
    After Round 2 Add round key:        1001 0101 1101 1111
    Round Key K2:                       0010 0110 0100 0100
Cipher Message:                                   40287
Digest:                                            3e6a
Digital Signature:                               499096
Client Private Key, d:                             4763
Client Public Key, n:                            528601
```

Server 5:



```
------------------------INPUT------------------------

Passed parameters for RSA:
P = 941, Q = 991, E = 19

Input received from client:

Encrypted Message:                      40287
Encrypted Secret Key:                   203928
Client's Signature:                     499096
Client's Public Key Parameters: N:      528601
Client's Public Key Parameters: E:      83

-----------------------OUTPUT-------------------------
Decrypted Secret Key:                   9673

Decryption Intermediate process:
Round Key, K2:                          0010 0110 0100 0100
After Round 1 InvShift rows:            1011 0011 1011 1001
After Round 1 InvSubstitute nibbles:    0011 1011 0011 0000
After Round 1 InvAdd round key:         1011 0011 1001 1011
Round 1 Key, K1:                        1000 0100 1001 0000
After Round 1 InvMix columns:           1011 1110 0000 1101
After Round 2 InvShift rows:            1011 1110 1101 0000
After Round 2 InvSubstitute nibbles:    0011 1101 0100 1010
After Round 2 Add round key:            0001 0001 0001 0011
Pre round Key, K0:                      0010 1100 0101 1001

Decrypted Message:                      4371
Digest from decrypted message:          3e6a
Decrypted Signature:                    3e6a
Verified:                               true

Submitted by: Abhishek Dubey | 2019005
------------========================
```