Ex. No : 5 Date :	RSA Algorithm

AIM:

To implement RSA (Rivest–Shamir–Adleman) algorithm by using HTML and Javascript.

ALGORITHM:

1. Choose two prime number p and q
2. Compute the value of n and **p**
3. Find the value of ***e*** (public key)
4. Compute the value of ***d*** (private key) using gcd()
5. Do the encryption and decryption
    a. Encryption is given as,
        $c = t^e \bmod n$
    b. Decryption is given as,
        $t = c^d \bmod n$

PROGRAM:

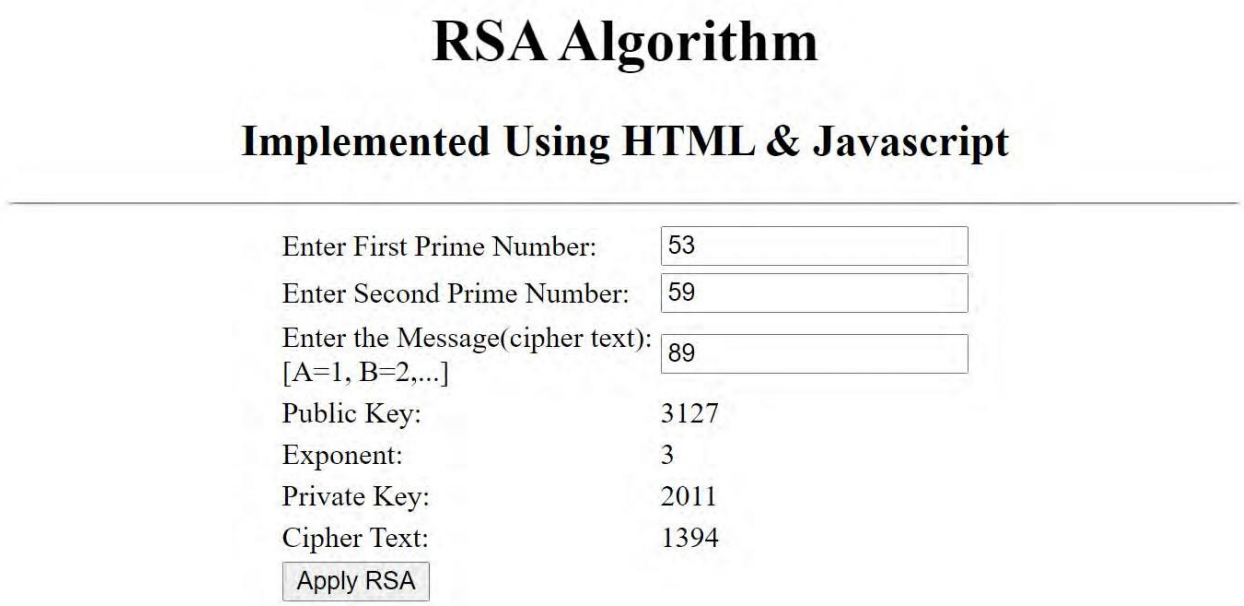
rsa.html

```
<html>

<head>
   <title>RSA Encryption</title>
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
</head>

<body>
   <center>
      <h1>RSA Algorithm</h1>
      <h2>Implemented Using HTML & Javascript</h2>
      <hr>
      <table>
         <tr>
            <td>Enter First Prime Number:</td>
            <td><input type="number" value="53" id="p"></td>
         </tr>
         <tr>
            <td>Enter Second Prime Number:</td>
            <td><input type="number" value="59" id="q"></p>
```

```
            </td>
          </tr>
          <tr>
            <td>Enter the Message(cipher text):<br>[A=1, B=2,...]</td>
            <td><input type="number" value="89" id="msg"></p>
            </td>
          </tr>
          <tr>
            <td>Public Key:</td>
            <td>
              <p id="publickey"></p>
            </td>
          </tr>
          <tr>
            <td>Exponent:</td>
            <td>
              <p id="exponent"></p>
            </td>
          </tr>
          <tr>
            <td>Private Key:</td>
            <td>
              <p id="privatekey"></p>
            </td>
          </tr>
          <tr>
            <td>Cipher Text:</td>
            <td>
              <p id="ciphertext"></p>
            </td>
          </tr>
          <tr>
            <td><button onclick="RSA();">Apply RSA</button></td>
          </tr>
        </table>
    </center>
</body>
<script type="text/javascript">
    function RSA() {
        var gcd, p, q, no, n, t, e, i, x;
```

```
        gcd = function (a, b) { return (!b) ? a : gcd(b, a % b); };
        p = document.getElementById('p').value;
        q = document.getElementById('q').value;
        no = document.getElementById('msg').value;
        n = p * q;
        t = (p - 1) * (q - 1);

        for (e = 2; e < t; e++) {
            if (gcd(e, t) == 1) {
                break;
            }
        }

        for (i = 0; i < 10; i++) {
            x = 1 + i * t
            if (x % e == 0) {
                d = x / e;
                break;
            }
        }

        ctt = Math.pow(no, e).toFixed(0);
        ct = ctt % n;

        dtt = Math.pow(ct, d).toFixed(0);
        dt = dtt % n;

        document.getElementById('publickey').innerHTML = n;
        document.getElementById('exponent').innerHTML = e;
        document.getElementById('privatekey').innerHTML = d;
        document.getElementById('ciphertext').innerHTML = ct;
    }
</script>
</html>
```

OUTPUT:



RESULT:

Thus the RSA algorithm has been implemented using HTML & CSS and the output has been verified successfully.