**Ex.No: 5 RSA ALGORITHM**

**Date:**

**Aim:**

To implement RSA Algorithm using HTML and Javascript.

**Algorithm:**

1. Start the program
2. Get the prime values from the user
3. Computer the n and Φ(n) values.
4. Given the value of e, computer the value of d
5. Generate the public key and the private keys

**Program:**

<html>

<head>

<title>RSA Encryption Algorithm</title>

<style>

button {

background-color: #f15640;

border: none;

color: white;

padding: 15px 32px;

text-align: center;

text-decoration: none;

display: inline-block;

font-size: 16px;

}

</style>

</head>

<body>

<center>

<h1>RSA Encryption Algorithm</h1>

<hr>

<table>

<tr>

<td>Enter Number 1:</td>

<td><input type="text" ></td>

</tr>

<tr>

<td>Enter Number 2:</td>

<td><input type="text" ></td>

</tr>

<tr>

<td>Enter Public Key:</td>

<td><input type="text"></td>

</tr>

<tr>

<td>Enter the Text</td>

<td><input type="text"></td>

</tr>

<tr>

<td>Composite Number:</td>

<td>

<p id="composite"></p>

</td>

</tr>

<tr>

<td>Private Key:</td>

<td>

<p id="privatekey"></p>

</td>

</tr>

<tr>

<td><button onclick="RSA(1); id="button1"">Encrypt</button></td>

<td>

<p id="ciphertext" data-inline="true"></p>

</td>

</tr>

<tr>

<td><button onclick="RSA(2); id="button2">Decrypt</button></td>

<td>

<p id="plaintext" data-inline="true"></p>

</td>

</tr>

</table>

</center>

</body>

<script type="text/javascript">

function RSA(choice) {

var gcd, p, q, msg, n, t, e,d,i;

gcd = function (a, b) { return (b!=0) ? gcd(b, a % b) :a ; };

p = document.getElementById('p').value;

q = document.getElementById('q').value;

msg = document.getElementById('msg').value;

e = document.getElementById('publickey').value;

n = p \* q;

t = (p - 1) \* (q - 1);

for (d = 2; d < t; d++) {

if ( (e\*d)%t == 1) {

break;

}

}

var ct=msg;

for(i=2;i<=e;i++)

ct=(ct\*msg)%n;

var pt=msg;

for(i=2;i<=d;i++)

pt=(pt\*msg)%n;

document.getElementById('composite').innerHTML = n;

document.getElementById('privatekey').innerHTML = d;

if(choice==1)

document.getElementById('ciphertext').innerHTML = ct;

else

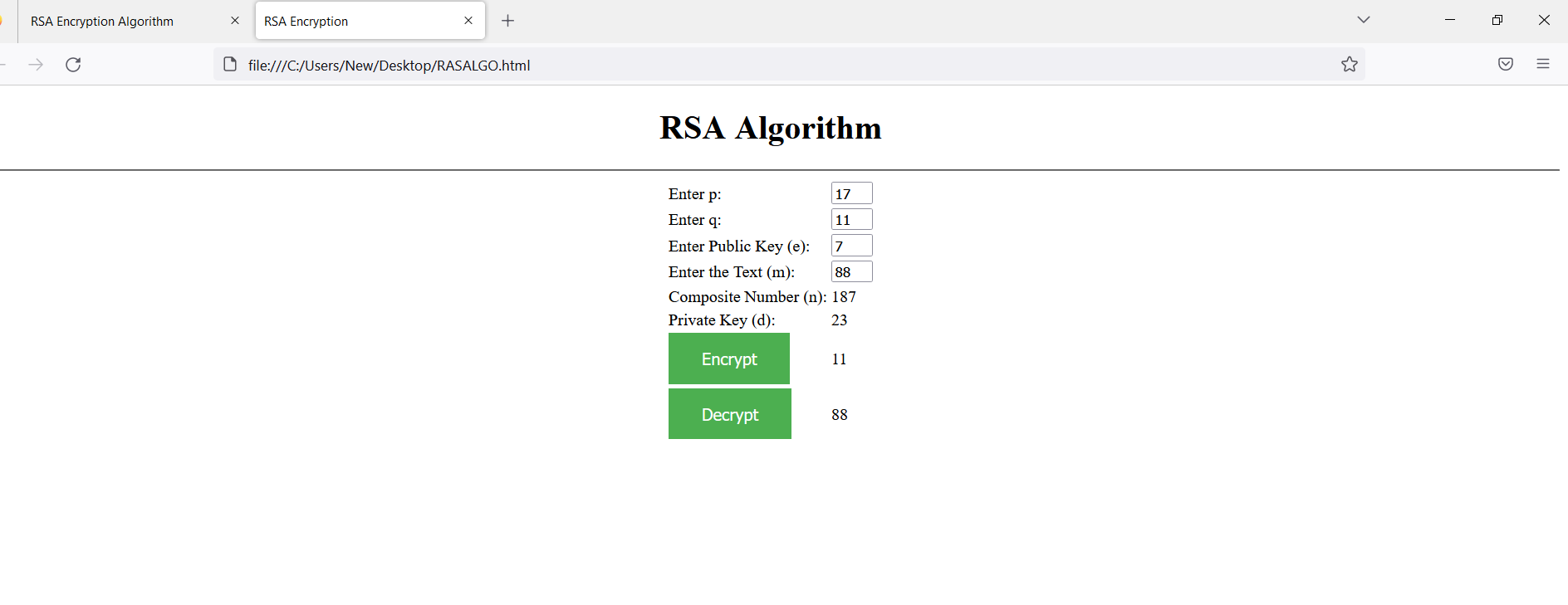
document.getElementById('plaintext').innerHTML = msg;

}

</script>

</html>

**Output:**



**Result:**

Thus, RSA algorithm has been implemented and verified successfully.