**RSA** (**Rivest–Shamir–Adleman**)

**CODE:**

<html>

<head>

<title>Input</title>

<script language="JavaScript">

<!-- hide from old browsers

function gcd (a, b)

{

var r;

while (b>0)

{

r=a%b;

a=b;

b=r;

}

return a;

}

function rel\_prime(phi)

{

var rel=5;

while (gcd(phi,rel)!=1)

rel++;

return rel;

}

function power(a, b)

{

var temp=1, i;

for(i=1;i<=b;i++)

temp\*=a;

return temp;

}

function encrypt(N, e, M)

{

var r,i=0,prod=1,rem\_mod=0;

while (e>0)

{

r=e % 2;

if (i++==0)

rem\_mod=M % N;

else

rem\_mod=power(rem\_mod,2) % N;

if (r==1)

{

prod\*=rem\_mod;

prod=prod % N;

}

e=parseInt(e/2);

}

return prod;

}

function calculate\_d(phi,e)

{

var x,y,x1,x2,y1,y2,temp,r,orig\_phi;

orig\_phi=phi;

x2=1;x1=0;y2=0;y1=1;

while (e>0)

{

temp=parseInt(phi/e);

r=phi-temp\*e;

x=x2-temp\*x1;

y=y2-temp\*y1;

phi=e;e=r;

x2=x1;x1=x;

y2=y1;y1=y;

if (phi==1)

{

y2+=orig\_phi;

break;

}

}

return y2;

}

function decrypt(c, d, N)

{

var r,i=0,prod=1,rem\_mod=0;

while (d>0)

{

r=d % 2;

if (i++==0)

rem\_mod=c % N;

else

rem\_mod=power(rem\_mod,2) % N;

if (r==1)

{

prod\*=rem\_mod;

prod=prod % N;

}

d=parseInt(d/2);

}

return prod;

}

function openNew()

{

var p=parseInt(document.Input.p.value);

var q=parseInt(document.Input.q.value);

var M=parseInt(document.Input.M.value);

var N=p \* q;

var phi=(p-1)\*(q-1);

var e=rel\_prime(phi);

var c=encrypt(N,e,M);

var d=calculate\_d(phi,e);

var T=decrypt(c,d,N);

document.getElementById("N").value=N;

document.getElementById("phi").value=phi;

document.getElementById("e").value=d;

document.getElementById("c").value=c;

document.getElementById("d").value=d;

document.getElementById("T").value=T;

}

// end scripting here -->

</script>

</head>

<body>

<p><font size="6">Input Form</font></p>

<hr>

<form name="Input">

<table border="0" width="100%" height="109">

<tr>

<td width="24%" height="23">

<font color="#0000FF">Enter P</font></td>

<td width="76%" height="23">

<input type="text" name="p" size="20"></td>

</tr>

<tr>

<td width="24%" height="23"><font color="#0000FF">

Enter Q</font></td>

<td width="76%" height="23">

<input type="text" name="q" size="20"></td>

</tr>

<tr>

<td width="24%" height="20">

<font color="#0000FF">Enter any Number ( M )</font></td>

<td width="76%" height="20"><input type="text" name="M" size="20">

<font size="1" color="#FF0000">(1-1000)</font></td>

</tr>

<tr>

<td width="24%" height="19"><input type="button"

value="Submit" name="Submit" onClick="openNew()"></td>

<td width="76%" height="19"><input type="reset"

value="Reset" name="Reset"></td>

</tr>

<tr>

<td width="22%"><font color="#0000FF">N

</font></td>

<td width="78%"><input type="text" name="N" id="N"size="20"></td>

</tr>

<tr>

<td width="22%"><font color="#0000FF">Phi</font></td>

<td width="78%"><input type="text" name="phi"id="phi" size="20"></td>

</tr>

<tr>

<td width="22%"><font color="#0000FF">e

</font></td>

<td width="78%">

<input type="text" name="e" id="e" size="20"></td>

</tr>

<tr>

<td width="22%"><font color="#0000FF">Encrypted Text

</font></td>

<td width="78%"><font color="#FF0000">

<input type="text" name="c"id="c" size="20"></font></td>

</tr>

<tr>

<td width="22%"><font color="#0000FF">d

</font></td>

<td width="78%"><input type="text" name="d" id="d"size="20">

</td>

</tr>

<tr>

<td width="22%"><font color="#0000FF">

Decrypted Text</font></td>

<td width="78%"><font color="#FF0000"><input type="text" name="T" id="T"size="20"></font></td>

</tr>

</table>

</form>

<p>&nbsp;</p>

</body>

</html>

**ScreenShot:**

