```
<!DOCTYPE html>
<head>
    <title>KEY EXCHANGE</title>
    <script >
        function shared_session(){
     var q=parseInt(document.form1.q.value);

     var a=parseInt(document.form1.a.value);
     var xa=parseInt(document.form1.xa.value);
     var xb=parseInt(document.form1.xb.value);
    var ya = (a**xa)%q;
    var yb=(a**xb)%q;
    var k1=(yb**xa)%q;
    var k2=(ya**xb)%q;
    if(k1==k2){
        alert("Shared session key is="+k1);

    }
    else{
        alert("Shared session key is not ");
        return false;

    }
}
 </script>

</head>
<body bgcolor="wheat">
    <h3><center><b>DIFFIE HELLMAN ALGORITHM FOR KEY
    EXCHANGE</b></center></h3>
    <center><br><br><table style="background-color: antiquewhite;">
        <form name="form1" onsubmit="return shared_session();"><br>
            <tr ><td><label>Enter the large prime
            integer:</label></td><td><input type="number" name="q" required
            style="border-radius: 50px;border-color: black;"></td></tr>
            <tr><td><label>Enter the primitive root of prime integer
            taken:</label></td><td><input type="number" name="a" required
            style="border-radius: 50px;border-color: black;"></td></tr>
            <tr ><td><label>Enter the private key of
            A:</label></td><td><input type="number" placeholder="should be
            less than prime integer" name="xa" required style="border-radius:
            50px;border-color: black;"></td></tr>
            <tr ><td><label>Enter the private key of B:
            </label></td><td><input type="number" placeholder="should be less
            than prime integer" name="xb" required style="border-radius:
            50px;border-color: black;"></td></tr>
            <tr><td colspan="2"><center><input type="submit" name="submit"
            style="border-radius: 30px;border-color: black;background-color:
            rgb(0, 255, 225);"></center></td></tr>
        </form>
```

```
38      </table></center>
39  </body>
```