

```
1 <!DOCTYPE html >
2 <head>
3   <title>KEY EXCHANGE</title>
4   <script >
5     function shared_session(){
6       var q=parseInt(document.form1.q.value);
7
8       var a=parseInt(document.form1.a.value);
9       var xa=parseInt(document.form1.xa.value);
10      var xb=parseInt(document.form1.xb.value);
11      var ya = (a**xa)%q;
12      var yb=(a**xb)%q;
13      var k1=(yb**xa)%q;
14      var k2=(ya**xb)%q;
15      if(k1==k2){
16        alert("Shared session key is="+k1);
17
18      }
19      else{
20        alert("Shared session key is not ");
21        return false;
22
23      }
24    }
25  </script>
26
27 </head>
28 <body bgcolor="wheat">
29   <h3><center><b>DIFFIE HELLMAN ALGORITHM FOR KEY
30   EXCHANGE</b></center></h3>
31   <center><br><br><table style="background-color: antiquewhite;">
32     <form name="form1" onsubmit="return shared_session();"><br>
33     <tr ><td><label>Enter the large prime
34     integer:</label ></td><td><input type="number" name="q" required
35     style="border-radius: 50px;border-color: black;"></td></tr>
36     <tr><td><label>Enter the primitive root of prime integer
37     taken:</label ></td><td><input type="number" name="a" required
38     style="border-radius: 50px;border-color: black;"></td></tr>
39     <tr ><td><label>Enter the private key of
40     A:</label ></td><td><input type="number" placeholder="should be
41     less than prime integer" name="xa" required style="border-radius:
42     50px;border-color: black;"></td></tr>
43     <tr ><td><label>Enter the private key of B:
44     </label ></td><td><input type="number" placeholder="should be less
45     than prime integer" name="xb" required style="border-radius:
46     50px;border-color: black;"></td></tr>
47     <tr><td colspan="2"><center><input type="submit" name="submit"
48     style="border-radius: 30px;border-color: black;background-color:
49     rgb(0, 255, 225);"></center></td></tr>
50   </form>
```

```
38     </tabl e></center>  
39 </body>
```