

-

```
<html>
<head>
<title>Diffie-HellmanKey Exchange</title>
</head>
<body>
<h2>Diffie-HellmanKey Exchange</h2>
<hr>

<script>

// This program calculates the Key for two persons
// using the Diffie-Hellman Key exchange algorithm

// Power function to return value of  $a^b \bmod P$ 
function power(a, b, p)
{
if (b == 1)
return a;
else
return((Math.pow(a, b)) % p);
}

// Driver code
var P, G, x, a, y, b, ka, kb;

// Both the persons will be agreed upon the
// public keys G and P

// A prime number P is taken
P = 11;
document.write("The value of P:" + P + "<br>");

// A primitive root for P, G is taken
G = 7;
document.write("The value of G:" + G + "<br>");

// Alice will choose the private key a
// a is the chosen private key
a = 4;
document.write("The private key a for Alice:" +
a + "<br>");

// Gets the generated key
x = power(G, a, P);

// Bob will choose the private key b
// b is the chosen private key
```

```

b = 3;
document.write("The private key b for Bob:" +
b + "<br>");

// Gets the generated key
y = power(G, b, P);

// Generating the secret key after the exchange
// of keys
ka = power(y, a, P); // Secret key for Alice
kb = power(x, b, P); // Secret key for Bob

document.write("Secret key for the Alice is:" +
ka + "<br>");
document.write("Secret key for the Bob is:" +
kb + "<br>");

</script>

</body>
</html>

```

Output:-

