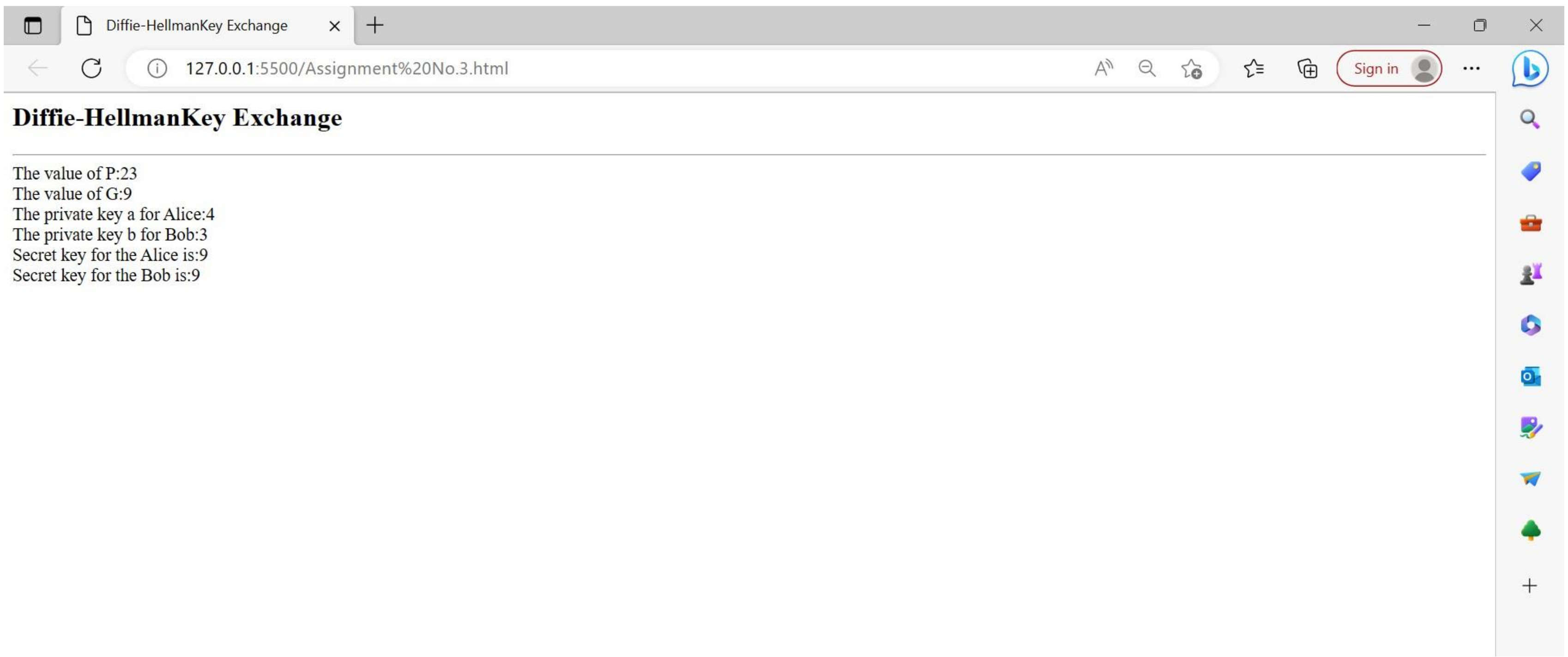
```
// COTB42 PHULE PRATHAMESH DNYANDEV
// Assignment No.4

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

<script>

function power(a, b, p)
{
if (b == 1)
return  a;
else
return((Math.pow(a, b)) % p);
}

var P, G, x, a, y, b, ka, kb;

P = 23;
document.write("The value of P:" + P + "<br>");

G = 9;
document.write("The value of G:" + G + "<br>");

a = 4;
document.write("The private key a for Alice:" +
a + "<br>");

x = power(G, a, P);

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

y = power(G, b, P);

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:



Diffie-HellmanKey Exchange
127.0.0.1:5500/Assignment%20No.3.html
Sign in

Diffie-HellmanKey Exchange

```
The value of P:23
The value of G:9
The private key a for Alice:4
The private key b for Bob:3
Secret key for the Alice is:9
Secret key for the Bob is:9
```