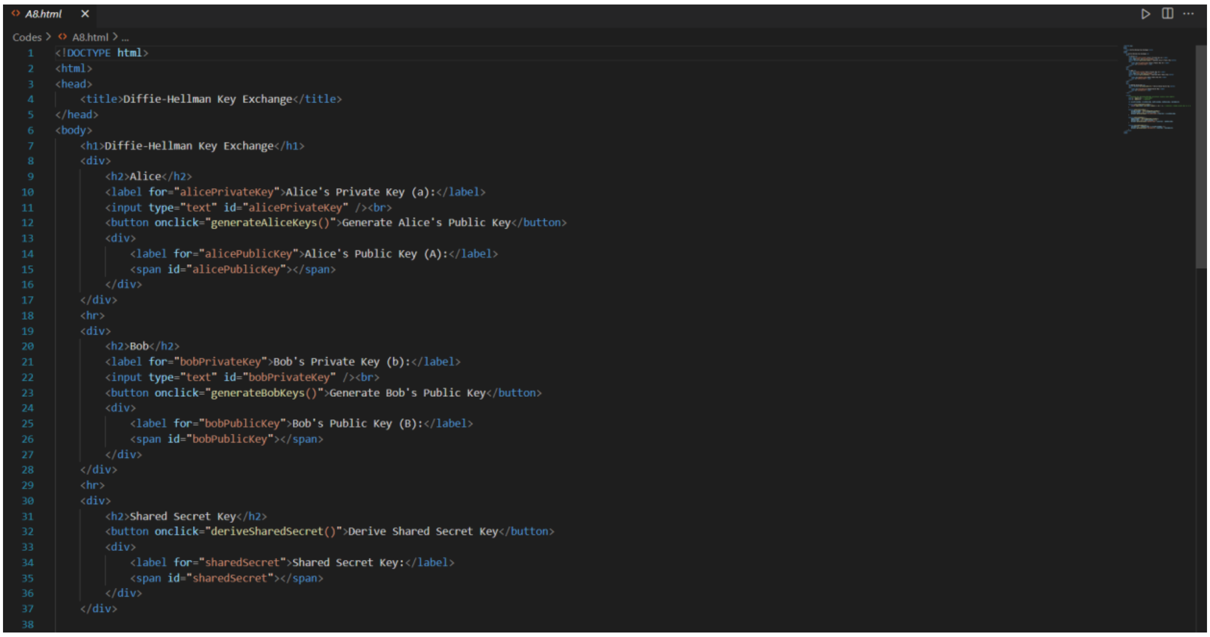
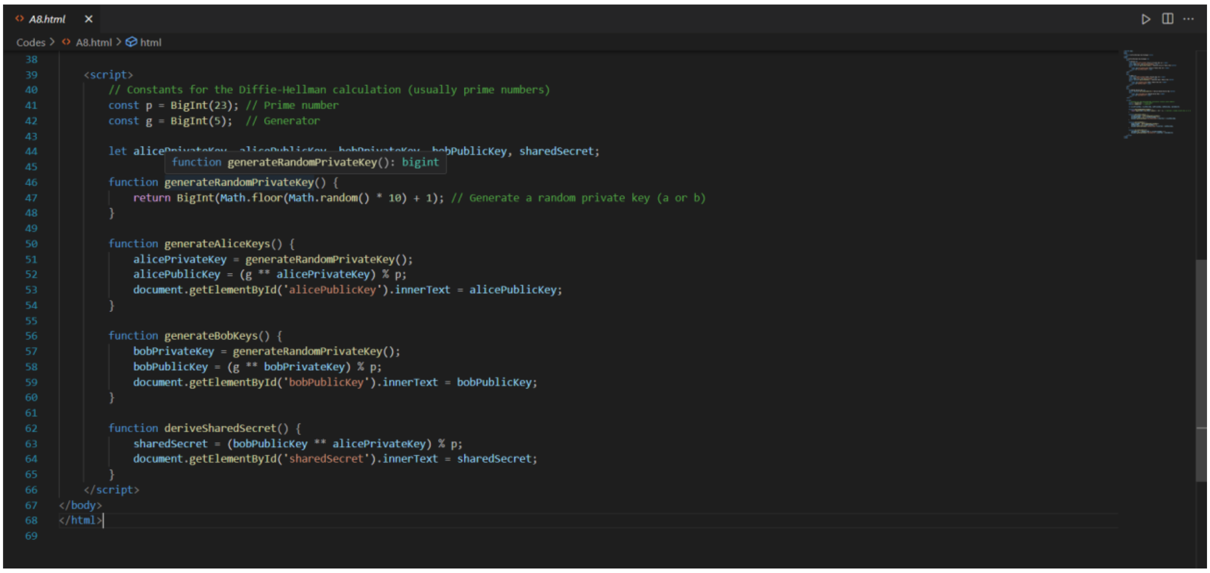
8. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. Consider the end user as one of the parties (Alice) and the JavaScript application as other party (bob).

Code:

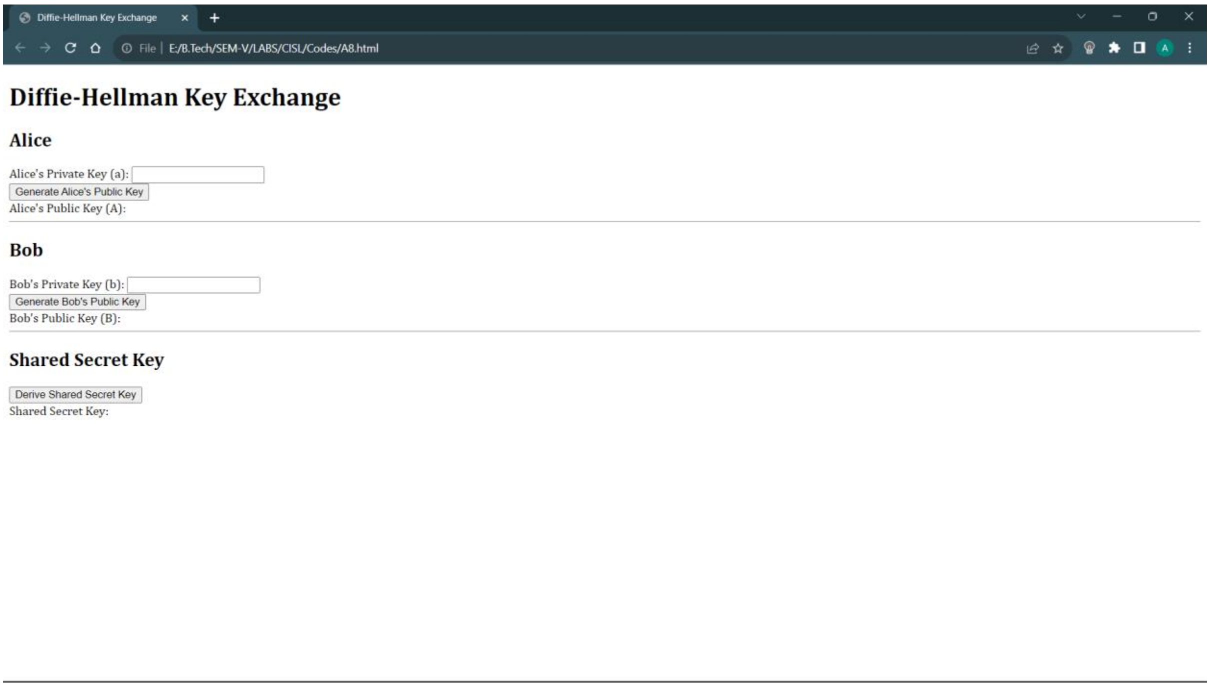


```html
<!DOCTYPE html>
<html>
<head>
    <title>Diffie-Hellman Key Exchange</title>
</head>
<body>
    <h1>Diffie-Hellman Key Exchange</h1>
    <div>
        <h2>Alice</h2>
        <label for="alicePrivateKey">Alice's Private Key (a):</label>
        <input type="text" id="alicePrivateKey" /><br>
        <button onclick="generateAliceKeys()">Generate Alice's Public Key</button>
        <div>
            <label for="alicePublicKey">Alice's Public Key (A):</label>
            <span id="alicePublicKey"></span>
        </div>
    </div>
    <hr>
    <div>
        <h2>Bob</h2>
        <label for="bobPrivateKey">Bob's Private Key (b):</label>
        <input type="text" id="bobPrivateKey" /><br>
        <button onclick="generateBobKeys()">Generate Bob's Public Key</button>
        <div>
            <label for="bobPublicKey">Bob's Public Key (B):</label>
            <span id="bobPublicKey"></span>
        </div>
    </div>
    <hr>
    <div>
        <h2>Shared Secret Key</h2>
        <button onclick="deriveSharedSecret()">Derive Shared Secret Key</button>
        <div>
            <label for="sharedSecret">Shared Secret Key:</label>
            <span id="sharedSecret"></span>
        </div>
    </div>

```



```html

    <script>
        // Constants for the Diffie-Hellman calculation (usually prime numbers)
        const p = BigInt(23); // Prime number
        const g = BigInt(5);  // Generator

        let alicePrivateKey, alicePublicKey, bobPrivateKey, bobPublicKey, sharedSecret;

        function generateRandomPrivateKey() {
            return BigInt(Math.floor(Math.random() * 10) + 1); // Generate a random private key (a or b)
        }

        function generateAliceKeys() {
            alicePrivateKey = generateRandomPrivateKey();
            alicePublicKey = (g ** alicePrivateKey) % p;
            document.getElementById('alicePublicKey').innerText = alicePublicKey;
        }

        function generateBobKeys() {
            bobPrivateKey = generateRandomPrivateKey();
            bobPublicKey = (g ** bobPrivateKey) % p;
            document.getElementById('bobPublicKey').innerText = bobPublicKey;
        }

        function deriveSharedSecret() {
            sharedSecret = (bobPublicKey ** alicePrivateKey) % p;
            document.getElementById('sharedSecret').innerText = sharedSecret;
        }
    </script>
</body>
</html>

```

Output:


Diffie-Hellman Key Exchange
File | E:/B.Tech/SEM-V/LABS/CISL/Codes/A8.html
Generate Alice's Public Key
Generate Bob's Public Key
Derive Shared Secret Key

Diffie-Hellman Key Exchange

Alice

Alice's Private Key (a):

Alice's Public Key (A):

Bob

Bob's Private Key (b):

Bob's Public Key (B):

Shared Secret Key

Shared Secret Key: