Name: Faraz Pathan

Rollno: COTB 70

/\*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) \*/

<!DOCTYPE html>

<html lang="en">

<head>

    <meta charset="UTF-8">

    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <title>Diffie-Hellman Key Exchange</title>

</head>

<body>

    <h1>Diffie-Hellman Key Exchange</h1>

    <div id="alice-keys">

        <h2>Alice</h2>

        <p>Private Key: <input type="number" id="alice-private-key-input"></p>

        <p>Public Key: <span id="alice-public-key"></span></p>

    </div>

    <div id="bob-keys">

        <h2>Bob</h2>

        <p>Private Key: <input type="number" id="bob-private-key-input"></p>

        <p>Public Key: <span id="bob-public-key"></span></p>

    </div>

    <div id="shared-key">

        <h2>Shared Secret Key</h2>

        <p><span id="shared-secret-key"></span></p>

    </div>

    <button onclick="calculateKeys()">Calculate Keys</button>

    <script>

        function calculateKeys() {

            // Prime number and generator (usually agreed upon in advance)

            const prime = 23;

            const generator = 5;

            // Get private keys from input fields

            const alicePrivateKey = parseInt(document.getElementById("alice-private-key-input").value);

            const bobPrivateKey = parseInt(document.getElementById("bob-private-key-input").value);

            // Calculate public keys for Alice and Bob

            const alicePublicKey = Math.pow(generator, alicePrivateKey) % prime;

            const bobPublicKey = Math.pow(generator, bobPrivateKey) % prime;

            // Calculate shared secret key for Alice and Bob

            const sharedSecretKeyAlice = Math.pow(bobPublicKey, alicePrivateKey) % prime;

            const sharedSecretKeyBob = Math.pow(alicePublicKey, bobPrivateKey) % prime;

            // Display keys

            document.getElementById("alice-public-key").innerText = alicePublicKey;

            document.getElementById("bob-public-key").innerText = bobPublicKey;

            document.getElementById("shared-secret-key").innerText = sharedSecretKeyAlice === sharedSecretKeyBob ? sharedSecretKeyAlice : "Keys do not match!";

        }

    </script>

</body>

</html>

**OUTPUT:**

