<!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>

<!-- CSS styles for better appearance -->

<style>

body {

font-family: Arial, sans-serif;

margin: 0;

padding: 0;

background-color: #f7f7f7;

}

.container {

max-width: 600px;

margin: 50px auto;

padding: 20px;

background-color: #fff;

border: 1px solid #ccc;

border-radius: 5px;

box-shadow: 0 2px 5px rgba(0, 0, 0, 0.1);

}

h2 {

text-align: center;

}

label {

display: block;

margin-bottom: 5px;

}

input {

width: calc(100% - 22px);

padding: 10px;

margin-bottom: 15px;

border: 1px solid #ccc;

border-radius: 5px;

box-sizing: border-box;

}

button {

width: 100%;

background-color: #4CAF50;

color: white;

padding: 10px;

border: none;

border-radius: 5px;

cursor: pointer;

transition: background-color 0.3s;

}

button:hover {

background-color: #45a049;

}

#sharedKey {

margin-top: 15px;

padding: 10px;

border: 1px solid #ccc;

border-radius: 5px;

}

</style>

</head>

<body>

<!-- Main content area -->

<div class="container">

<h2>Diffie-Hellman Key Exchange</h2>

<!-- Input fields for prime, base, and private keys -->

<label for="prime">Prime Number (p):</label>

<input type="number" id="prime" placeholder="Enter a prime number">

<label for="base">Base (g):</label>

<input type="number" id="base" placeholder="Enter a base number">

<label for="privateKeyAlice">Alice's Private Key (a):</label>

<input type="number" id="privateKeyAlice" placeholder="Enter Alice's private key">

<label for="privateKeyBob">Bob's Private Key (b):</label>

<input type="number" id="privateKeyBob" placeholder="Enter Bob's private key">

<!-- Button to trigger key calculation -->

<button onclick="calculateKeys()">Calculate Shared Key</button>

<!-- Display area for intermediate values and shared keys -->

<div id="sharedKey"></div>

</div>

<!-- JavaScript for calculating and displaying shared keys -->

<script>

// Function to calculate shared keys

function calculateKeys() {

// Get inputs from the user

const prime = parseInt(document.getElementById('prime').value);

const base = parseInt(document.getElementById('base').value);

const privateKeyAlice = parseInt(document.getElementById('privateKeyAlice').value);

const privateKeyBob = parseInt(document.getElementById('privateKeyBob').value);

// Calculate intermediate values

const intermediateAlice = power(base, privateKeyAlice, prime);

const intermediateBob = power(base, privateKeyBob, prime);

// Display intermediate values

document.getElementById('sharedKey').innerHTML = <p>Alice's Intermediate Value: ${intermediateAlice}</p><p>Bob's Intermediate Value: ${intermediateBob}</p>;

// Calculate shared keys

const sharedKeyAlice = power(intermediateBob, privateKeyAlice, prime);

const sharedKeyBob = power(intermediateAlice, privateKeyBob, prime);

// Display the shared keys

document.getElementById('sharedKey').innerHTML += <p>Shared Key (Alice's side): ${sharedKeyAlice}</p><p>Shared Key (Bob's side): ${sharedKeyBob}</p>;

}

// Power function to return value of a ^ b mod P

function power(a, b, p) {

if (b === 1) return a % p;

else return Math.pow(a, b) % p;

}

</script>

</body>

</html>