1. **input.py**

<!DOCTYPE html>

<html lang="en">

<head>

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

    <style>

body {

            font-family: Arial, sans-serif;

            background-color: #f8f9fa;

            margin: 0;

            padding: 0;

            display: flex;

            justify-content: center;

            align-items: center;

            height: 100vh;

        }

        .container {

            background: #ffffff;

            padding: 20px;

            border-radius: 10px;

            box-shadow: 0 2px 10px rgba(0, 0, 0, 0.1);

            width: 100%;

            max-width: 400px;

            text-align: center;

        }

        h2 {

            color: #007bff;

        }

        label {

            display: block;

            font-weight: bold;

            margin-top: 10px;

            text-align: left;

        }

        input {

            width: 100%;

            padding: 8px;

            margin-top: 5px;

            border: 1px solid #ddd;

            border-radius: 5px;

            font-size: 1rem;

        }

        button {

            margin-top: 15px;

            width: 100%;

            padding: 10px;

            background: #007bff;

            color: white;

            border: none;

            border-radius: 5px;

            font-size: 1rem;

            cursor: pointer;

        }

        button:hover {

            background: #0056b3;

        }

        p {

            margin-top: 10px;

            font-weight: bold;

            color: #333;

        }

        #result {

            margin-top: 15px;

            padding: 10px;

            border-radius: 5px;

            font-weight: bold;

        }

    </style>

</head>

<body>

    <div class="container">

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

        <label for="pKey">Enter P Value:</label>

        <input type="number" id="pKey" required>

        <label for="gKey">Enter G Value:</label>

        <input type="number" id="gKey" required>

        <label for="alicePrivateKey">Alice's Private Key:</label>

        <input type="number" id="alicePrivateKey" required>

        <label for="bobPrivateKey">Bob's Private Key:</label>

        <input type="number" id="bobPrivateKey" required>

        <button onclick="exchangeKeys()">Exchange Keys</button>

        <p>Alice's Public Key: <span id="alicePublicKey"></span></p>

        <p>Bob's Public Key: <span id="bobPublicKey"></span></p>

        <p>Alice's Shared Secret: <span id="sharedSecretAlice"></span></p>

        <p>Bob's Shared Secret: <span id="sharedSecretBob"></span></p>

        <p id="result"></p>

    </div>

    <script>

        function exchangeKeys() {

        const p = parseInt(document.getElementById("pKey").value);

        const g = parseInt(document.getElementById("gKey").value);

        function modExp(base, exponent, mod) {

            let result = 1;

            base = base % mod;

            while (exponent > 0) {

            if (exponent % 2 === 1) {

                result = (result \* base) % mod;

            }

            exponent = Math.floor(exponent / 2);

            base = (base \* base) % mod;

            }

            return result;

        }

        function isPrimitiveRoot(p, g) {

            if (p <= 1 || g <= 1 || g >= p) {

            return false;

            }

            let remainders = new Set();

            for (let k = 1; k < p; k++) {

            let remainder = modExp(g, k, p);

            if (remainders.has(remainder)) {

                return false;

            }

            remainders.add(remainder);

            }

            return true;

        }

        const result = isPrimitiveRoot(p, g);

        if (result) {

            document.getElementById("result").textContent = "The shared secrets match! Key exchange successful.";

            let alicePrivateKey = parseInt(document.getElementById("alicePrivateKey").value);

            let bobPrivateKey = parseInt(document.getElementById("bobPrivateKey").value);

            let alicePublicKey = Math.pow(g, alicePrivateKey) % p;

            let bobPublicKey = Math.pow(g, bobPrivateKey) % p;

            document.getElementById("alicePublicKey").textContent = alicePublicKey;

            document.getElementById("bobPublicKey").textContent = bobPublicKey;

            let sharedSecretAlice = Math.pow(bobPublicKey, alicePrivateKey) % p;

            let sharedSecretBob = Math.pow(alicePublicKey, bobPrivateKey) % p;

            document.getElementById("sharedSecretAlice").textContent = sharedSecretAlice;

            document.getElementById("sharedSecretBob").textContent = sharedSecretBob;

            if (sharedSecretAlice === sharedSecretBob) {

                document.getElementById("result").textContent = "The shared secrets match! Key exchange successful.";

            } else {

                document.getElementById("result").textContent = "Something went wrong. The shared secrets do not match.";

            }

        } else {

            document.getElementById("result").textContent = "P is not a Primitive Root for G";

        }

        }

    </script>

</body>

</html>

1. **Output**



