Example:

Step 1: Alice and Bob get public numbers P = 23, G = 9

Step 2: Alice selected a private key a = 4 and
Bob selected a private key b = 3

Step 3: Alice and Bob compute public values
Alice: x =(9^4 mod 23) = (6561 mod 23) = 6
Bob: y = (9^3 mod 23) = (729 mod 23) = 16

Step 4: Alice and Bob exchange public numbers

Step 5: Alice receives public key y =16 and
Bob receives public key x = 6

Step 6: Alice and Bob compute symmetric keys
Alice: ka = y^a mod p = 65536 mod 23 = 9
Bob: kb = x^b mod p = 216 mod 23 = 9

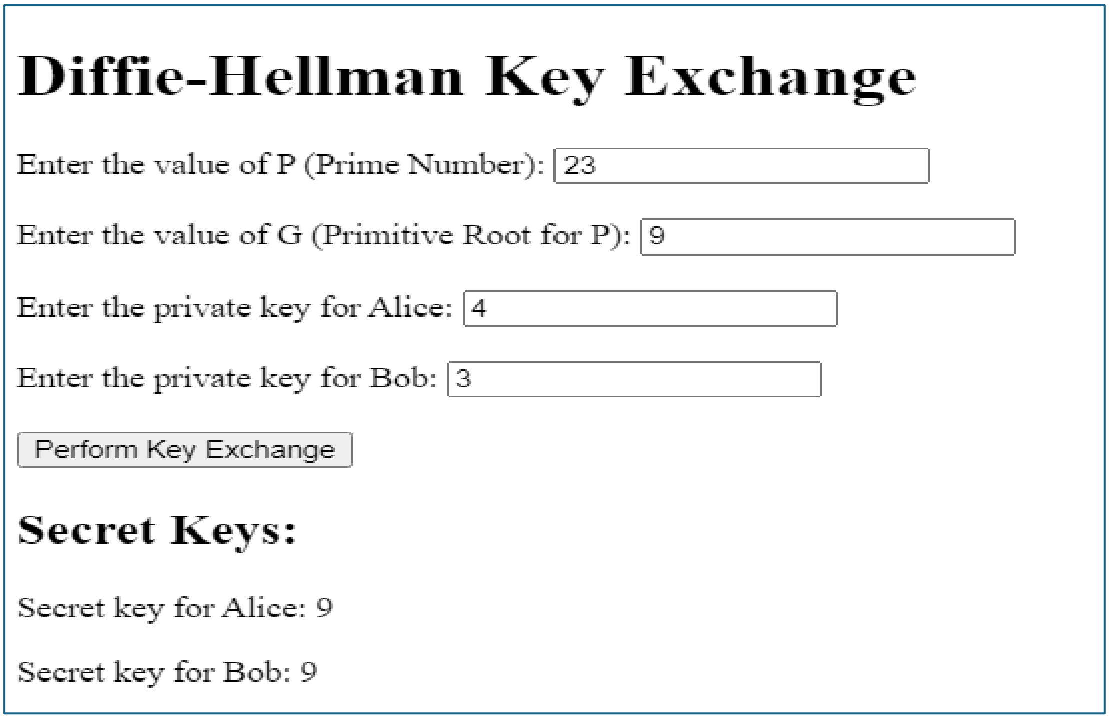
Step 7: 9 is the shared secret.

Code:

```
<!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>
  <script>
    // Power function to return value of a ^ b mod P
    function power(a, b, p) {
      if (b == 1) {
        return a;
      } else {
        return Math.pow(a, b) % p;
      }
    }

    // Function to perform key exchange
    function performKeyExchange() {
      var P = parseInt(document.getElementById('inputP').value);
      var G = parseInt(document.getElementById('inputG').value);
      var a = parseInt(document.getElementById('inputA').value);
```

```
        var b = parseInt(document.getElementById('inputB').value);

        // Calculate public keys
        var x = power(G, a, P);
        var y = power(G, b, P);

        // Generate shared secret keys
        var ka = power(y, a, P); // Secret key for Alice
        var kb = power(x, b, P); // Secret key for Bob

        // Display the secret keys
        document.getElementById('outputAlice').innerHTML = "Secret key for Alice: " +
ka;
        document.getElementById('outputBob').innerHTML = "Secret key for Bob: " + kb;
      }
  </script>
</head>
<body>
  <h1>Diffie-Hellman Key Exchange</h1>
  <label for="inputP">Enter the value of P (Prime Number):</label>
  <input type="number" id="inputP" value="23"><br><br>

  <label for="inputG">Enter the value of G (Primitive Root for P):</label>
  <input type="number" id="inputG" value="9"><br><br>

  <label for="inputA">Enter the private key for Alice:</label>
  <input type="number" id="inputA" value="4"><br><br>

  <label for="inputB">Enter the private key for Bob:</label>
  <input type="number" id="inputB" value="3"><br><br>

  <button onclick="performKeyExchange()">Perform Key Exchange</button>

  <h2>Secret Keys:</h2>
  <p id="outputAlice"></p>
  <p id="outputBob"></p>
</body>
</html>
```

OUTPUT:



Diffie-Hellman Key Exchange

Enter the value of P (Prime Number): 23

Enter the value of G (Primitive Root for P): 9

Enter the private key for Alice: 4

Enter the private key for Bob: 3

Secret Keys:

Secret key for Alice: 9

Secret key for Bob: 9