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).

Program:

```
<!DOCTYPE html>

<html>

 <head>

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

 </head>

 <body>

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

  <p>Enter a prime number (p): <input type="number" id="p"></p>

  <p>Enter a primitive root of p (g): <input type="number" id="g"></p>

  <p>Enter Alice's secret key (a): <input type="number" id="a"></p>

  <p>Click the button to generate Alice's public key (A): <button
onclick="generatePublicKey()">Generate A</button></p>

  <p>Alice's public key (A): <span id="A"></span></p>

  <p>Enter Bob's secret key (b): <input type="number" id="b"></p>

  <p>Click the button to generate Bob's public key (B): <button
onclick="generatePublicKey()">Generate B</button></p>

  <p>Bob's public key (B): <span id="B"></span></p>

  <p>Click the button to generate the shared secret key: <button
onclick="generateSharedSecret()">Generate Shared Secret Key</button></p>

  <p>The shared secret key: <span id="sharedSecret"></span></p>

  <script>

    const pEl = document.getElementById('p');

    const gEl = document.getElementById('g');
```

```
const aEl = document.getElementById('a');
const bEl = document.getElementById('b');
const AEl = document.getElementById('A');
const BEl = document.getElementById('B');
const sharedSecretEl = document.getElementById('sharedSecret');

function generatePublicKey() {
  const p = parseInt(pEl.value);
  const g = parseInt(gEl.value);
  const a = parseInt(aEl.value);
  const b = parseInt(bEl.value);
  const A = Math.pow(g, a) % p;
  const B = Math.pow(g, b) % p;
  AEl.textContent = A;
  BEl.textContent = B;
}

function generateSharedSecret() {
  const p = parseInt(pEl.value);
  const a = parseInt(aEl.value);
  const b = parseInt(bEl.value);
  const B = parseInt(BEl.textContent);
  const sharedSecret = Math.pow(B, a) % p;
  sharedSecretEl.textContent = sharedSecret;
}
```

```
  </script>
 </body>
</html>
```

Output: