

Pract 6

```
<!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">
    <h2>Alice (End User)</h2>
    <button onclick="generateKeys()">Generate Alice's Keys</button>
    <div>Public Key: <span id="alice-public"></span></div>
  </div>
  <div id="bob">
    <h2>Bob (JavaScript Application)</h2>
    <button onclick="calculateSecret()">Calculate Shared Secret</button>
    <div>Shared Secret: <span id="shared-secret"></span></div>
  </div>

  <script>
    // Prime number and generator for Diffie-Hellman
    const prime = 23;
    const generator = 5;

    let alicePrivateKey, alicePublicKey, bobPrivateKey, bobPublicKey, sharedSecret;

    // Function to generate keys for Alice
    function generateKeys() {
      alicePrivateKey = Math.floor(Math.random() * (prime - 2)) + 1; // Random number between 1
and prime - 2
      alicePublicKey = Math.pow(generator, alicePrivateKey) % prime; // Calculate public key
      document.getElementById("alice-public").innerText = alicePublicKey;
    }

    // Function to calculate shared secret for Bob
    function calculateSecret() {
      bobPrivateKey = Math.floor(Math.random() * (prime - 2)) + 1; // Random number between 1
and prime - 2
      bobPublicKey = Math.pow(generator, bobPrivateKey) % prime; // Calculate public key

      const sharedSecret = Math.pow(alicePublicKey, bobPrivateKey) % prime; // Calculate shared
secret
      document.getElementById("shared-secret").innerText = sharedSecret;
    }
  </script>
</body>
</html>
```