Assignment No 6

```
<!DOCTYPE html>
<html>
<head>
    <title>Diffie-Hellman Key Exchange</title>
</head>
<body>
    <h2>Diffie-Hellman Key Exchange</h2>
    <label for="alicePrivate">Enter Alice's Private Key:</label>
    <input type="number" id="alicePrivate" min="1" max="100">
    <button onclick="performKeyExchange()">Exchange Keys</button>

    <h3>Results:</h3>
    <p id="publicAlice"></p>
    <p id="publicBob"></p>
    <p id="sharedAlice"></p>
    <p id="sharedBob"></p>

    <script>
        // Constants: Prime number (p) and Generator (g)
        const p = 23;
        const g = 5;

        function modExp(base, exp, mod) {
            return Math.pow(base, exp) % mod;
        }

        function performKeyExchange() {
            let alicePrivate =
parseInt(document.getElementById("alicePrivate").value);
            if (isNaN(alicePrivate) || alicePrivate <= 0) {
                alert("Please enter a valid private key.");
                return;
            }

            // Alice computes public key
            let publicAlice = modExp(g, alicePrivate, p);
```

```
             // Bob generates private key
            let bobPrivate = Math.floor(Math.random() * 100) + 1;
            let publicBob = modExp(g, bobPrivate, p);

            // Compute shared secrets
            let sharedAlice = modExp(publicBob, alicePrivate, p);
            let sharedBob = modExp(publicAlice, bobPrivate, p);

            // Display results
            document.getElementById("publicAlice").innerText = `Alice's
Public Key: ${publicAlice}`;
            document.getElementById("publicBob").innerText = `Bob's Public
Key: ${publicBob}`;
            document.getElementById("sharedAlice").innerText = `Alice's
Computed Shared Key: ${sharedAlice}`;
            document.getElementById("sharedBob").innerText = `Bob's
Computed Shared Key: ${sharedBob}`;
        }
    </script>
</body>
</html>
```

Output-
Input

- Alice enters **private key = 6**

Randomly Generated by JavaScript (Bob):

- Bob’s private key = **15** (randomly generated)

Computed Public Keys:

- Alice’s Public Key: **(5^{6} mod 23) = 8**
- Bob’s Public Key: **(5^{15} mod 23) = 19**

Computed Shared Secret Key:

- Alice computes: **(19^{6} mod 23) = 2**

- Bob computes: **(8^{15} mod 23) = 2**