**Assignment No: 6 Roll No: 37**

<!DOCTYPE html>

<html>

<head>

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

<script>

function modExp(base, exp, mod) {

let result = 1;

base = base % mod;

while (exp > 0) {

if (exp % 2 === 1) {

result = (result \* base) % mod;

}

exp = Math.floor(exp / 2);

base = (base \* base) % mod;

}

return result;

}

function calculateKeys() {

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

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

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

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

if (isNaN(P) || isNaN(G) || isNaN(a) || isNaN(b)) {

alert("Please enter valid numbers for all fields.");

return;

}

let x = modExp(G, a, P);

let y = modExp(G, b, P);

let ka = modExp(y, a, P);

let kb = modExp(x, b, P);

document.getElementById("result").innerHTML =

"<b>Public key for Alice:</b> " + x + "<br>" +

"<b>Public key for Bob:</b> " + y + "<br>" +

"<b>Secret key for Alice:</b> " + ka + "<br>" +

"<b>Secret key for Bob:</b> " + kb;

}

</script>

<style>

body {

font-family: Arial, sans-serif;

text-align: center;

margin: 50px;

}

input, button {

margin: 10px;

padding: 8px;

font-size: 16px;

}

button {

cursor: pointer;

background-color: #007bff;

color: white;

border: none;

border-radius: 5px;

}

button:hover {

background-color: #0056b3;

}

</style>

</head>

<body>

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

<input type="number" id="P" placeholder="Enter prime number (P)"><br>

<input type="number" id="G" placeholder="Enter primitive root (G)"><br>

<input type="number" id="a" placeholder="Enter private key for Alice"><br>

<input type="number" id="b" placeholder="Enter private key for Bob"><br>

<button onclick="calculateKeys()">Compute Keys</button>

<h3>Results:</h3>

<div id="result"></div>

</body>

</html>

