Assignment no 5

Problem statement:

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).

Roll no: 331 **Name: Rameshwar Gosavi** **Batch: B**

Solution:

HTML:

```
<!DOCTYPE html>
<html>
 <head>
  <title>Diffie-Hellman Key Exchange</title>
  <link rel="stylesheet" type="text/css" href="style.css">
 </head>
 <body>
  <div class="container">
   <h1>Diffie-Hellman Key Exchange</h1>
   <div class="prime-number">
    <label for="prime-number-input">Enter a prime number:</label>
    <input type="number" id="prime-number-input">
   </div>
   <div class="generator">
    <label for="generator-input">Enter a generator:</label>
    <input type="number" id="generator-input">
   </div>
   <div class="secret-number">
    <label for="secret-number-input">Enter a secret number:</label>
    <input type="number" id="secret-number-input">
   </div>
   <div class="public-key">
    <label>Public key:</label>
    <p id="public-key-output"></p>
   </div>
   <button id="generate-public-key-btn">Generate Public Key</button>
   <div class="shared-secret">
    <label>Shared secret:</label>
    <p id="shared-secret-output"></p>
   </div>
  </div>
  <script src="script.js"></script>
 </body>
</html>
```

CSS:

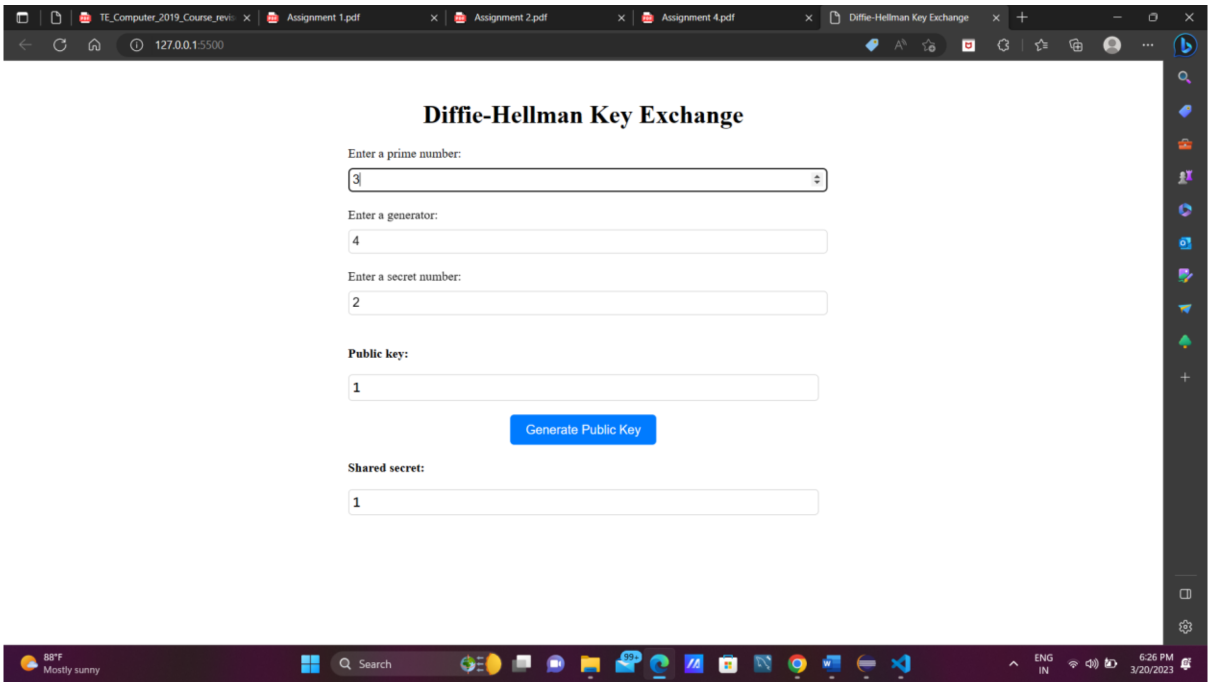
```
.container {
   max-width: 600px;
   margin: 0 auto;
   padding: 20px;
 }

 h1 {
   text-align: center;
 }

 label {
   display: block;
   margin-bottom: 10px;
 }

 input[type="number"] {
   width: 100%;
   padding: 5px;
   border: 1px solid #ccc;
   border-radius: 5px;
   font-size: 16px;
   margin-bottom: 20px;
 }

 .public-key,
 .shared-secret {
   margin-top: 20px;
 }

 .public-key label,
 .shared-secret label {
   font-weight: bold;
 }

 .public-key p,
 .shared-secret p {
   font-family: monospace;
   font-size: 18px;
   padding: 5px;
   border: 1px solid #ccc;
   border-radius: 5px;
   word-wrap: break-word;
 }

 button {
   display: block;
   margin: 0 auto;
   padding: 10px 20px;
   font-size: 16px;
```

```
    border-radius: 5px;
    background-color: #007bff;
    color: #fff;
    border: none;
    cursor: pointer;
    transition: background-color 0.3s ease;
  }

  button:hover {
    background-color: #0069d9;
  }
```

JavaScript:

```
const primeNumberInput = document.getElementById("prime-number-input");
const generatorInput = document.getElementById("generator-input");
const secretNumberInput = document.getElementById("secret-number-input");
const publicKeyOutput = document.getElementById("public-key-output");
const sharedSecretOutput = document.getElementById("shared-secret-output");
const generatePublicKeyBtn = document.getElementById("generate-public-key-btn");

generatePublicKeyBtn.addEventListener("click", () => {
  const p = parseInt(primeNumberInput.value);
  const g = parseInt(generatorInput.value);
  const a = parseInt(secretNumberInput.value);

  const A = Math.pow(g, a) % p;

  publicKeyOutput.textContent = A;

  const B = parseInt(prompt("Enter public key from other party:"));


  const publicKeyOutputb = Math.pow(g,B)%p;
  const sharedSecret = Math.pow(publicKeyOutputb, a) % p;
  const sharedSecretB = Math.pow(A,B)%p;


if(sharedSecretB == sharedSecretB)
{
  sharedSecretOutput.textContent = sharedSecret;
}
else
{
    alert("key's are different");
}
});
```

Output:



Diffie-Hellman Key Exchange

Enter a prime number:

3

Enter a generator:

4

Enter a secret number:

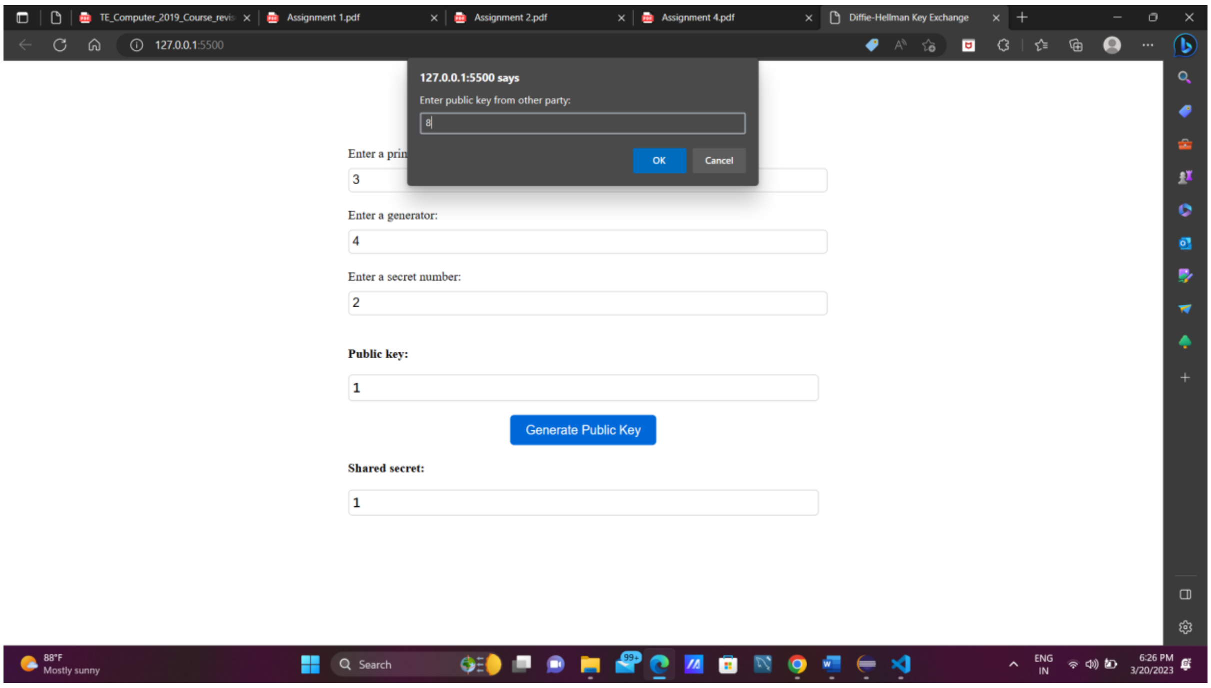
2

Public key:

1

Shared secret:

1



127.0.0.1:5500 says

Enter public key from other party:

8

Enter a prin

3

Enter a generator:

4

Enter a secret number:

2

Public key:

1

Shared secret:

1