МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"

Кафедра інформаційних систем та мереж

Лабораторна робота  №4

з дисципліни “Екстремальне програмування”

Виконав студент

групи КН-311

Здробилко Н.Ю.

Прийняв:

Щербак С.С.

Львів – 2020

**Мета** навчитися розробляти Функціонал сайту з допомогою HTML і JS

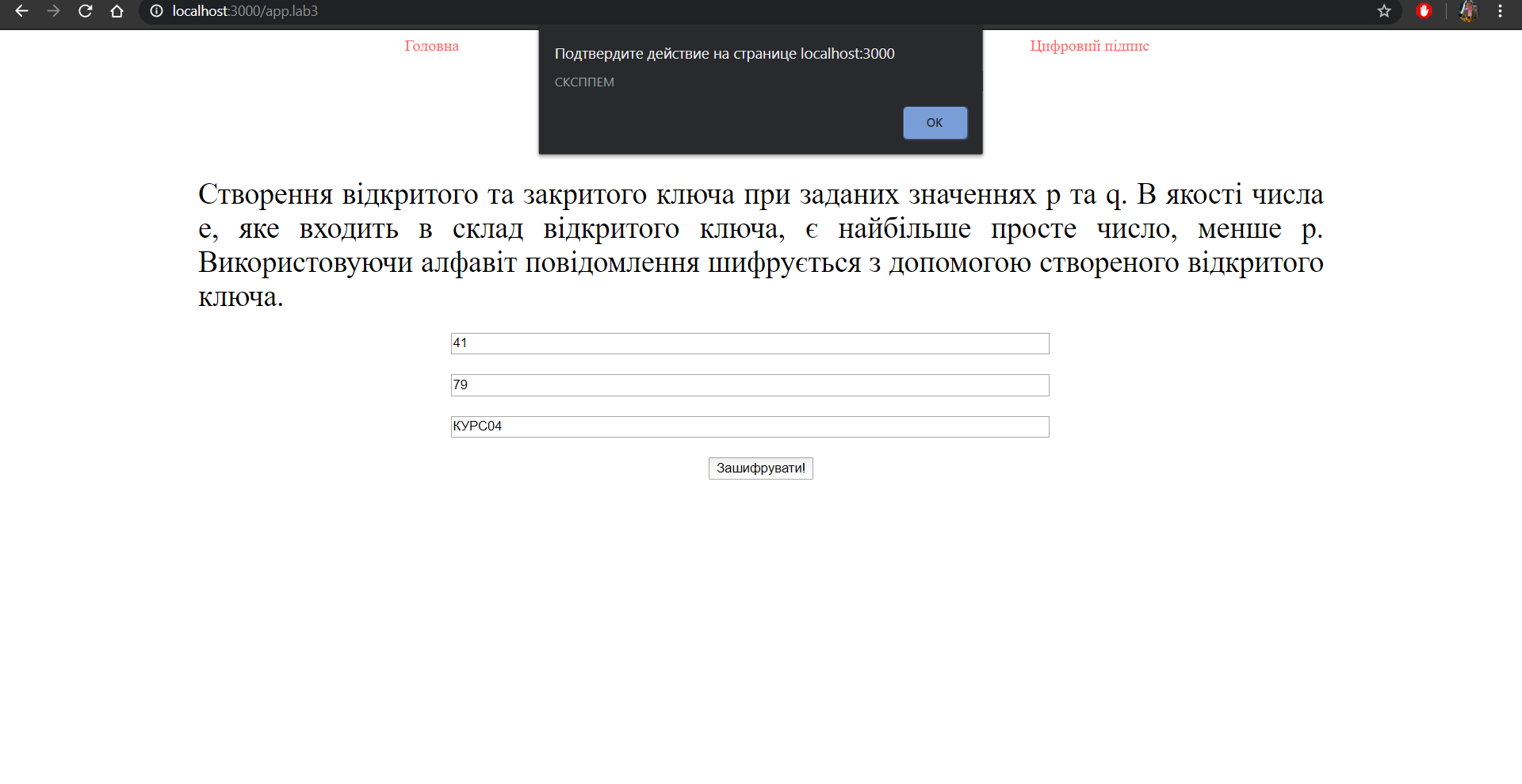
**Хід роботи**

**Lab3.html**

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  
 "http://www.w3.org/TR/html4/loose.dtd">  
<html>  
<head>  
 <meta charset="UTF-8">  
 <title>Лаборагорна робота 3</title>  
 <link rel="stylesheet" href="/app.css">  
</head>  
<body>  
<div id="menu">  
 <ul>  
 <a href="/" ><li>Головна</li></a>  
 <a href="/app.lab1" ><li>Шифр Цезаря</li></a>  
 <a href="/app.lab2" ><li>Шифр Гамми</li></a>  
 <a href="/app.lab3" ><li>Шифр RSA</li></a>  
 <a href="/app.lab4" ><li>Цифровий підпис</li></a>  
 </ul>  
</div>  
<div class="tt">  
 <div class="t"><br><br><br><br></div>  
 <div class="task">  
 Створення відкритого та закритого ключа при заданих значеннях p та q. В якості числа e, яке  
 входить в склад відкритого ключа, є найбільше просте число, менше p.  
 Використовуючи алфавіт повідомлення шифрується з допомогою створеного відкритого ключа.  
 </div>  
 <div class="imput">  
 <input id="P" type="text" value="41">  
 </div>  
 <div class="imput">  
 <input id="Q" type="text" value="79">  
 </div>  
 <div class="imput">  
 <input id="text" type="text" value="КУРС04">  
 </div>  
 <div class="button">  
 <button onclick="Click()" >Зашифрувати!</button>  
 </div>  
  
 </div>  
  
<script src="/app.js3"></script>  
</body>  
</html>

**Script.js**

function Click() {  
 let text = ***document***.getElementById("text").value;  
 let p = ***document***.getElementById("P").value;  
 let q = ***document***.getElementById("Q").value;  
 let n=p\*q, FnE=(p-1)\*(q-1);  
 let e=0,lich=0,textM=[],resM=[],resD=[];  
 let mas = " АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ\_0123456789";  
 for(let j=7;j<n-1;j++){  
 for(let i=0;i<=j;i++){  
 if(***Object***.is(j%i,0)){lich++;}  
 }  
 if(lich===2){  
 e=j;  
 break;  
 }  
 lich=0;  
 }  
 let d;  
 alert("Відкритий ключ алфавіту: ("+e+";"+n+")");  
 for(let k =1;k<10000;k++){  
 d=(k\*FnE+1)/e;  
 if(***Object***.is(d%1,0)){  
 break;  
 }  
 }  
 alert("Закрити ключ алфавіту: ("+d+";"+n+")");  
  
 for(let i=0;i<text.length;i++) {  
 for (let j = 0; j < mas.length; j++) {  
 if (***Object***.is(text[i], mas[j])) {  
 textM.push(j);  
 }  
 }  
 }  
 alert(textM);  
 for(let i=0;i<text.length;i++) {  
 resM[i] = (***Math***.pow(textM[i],e)%n);  
 }  
 alert(resM);  
 for(let i=0;i<resM.length;i++) {  
 resD[i] = (***Math***.pow(resM[i],d));  
 }  
 alert(textM);  
 let resU="";  
 let code=[17558, 2355, 1046, 2538, 1, 2561, 648];  
 for(let i =0;i<7;i++){  
 resU=resU + mas[(***Math***.pow(code[i],d)%43)];  
 }  
 alert(resU);  
}  
  
function Click1() {  
 let p=13,q=53,d=5;  
 let n=p\*q;  
 let msg="СМ5"  
 let msgv=[];  
 let msg1="179ДТВ3"  
 let msgv1=[];  
 let mas = " АБВГҐДЕЄЖЗИІЇЙКЛМНОПРСТУФХЦЧШЩЬЮЯ\_0123456789";  
 for(let i=0;i<msg.length;i++){  
 for(let j=0;j<mas.length;j++){  
 if(***Object***.is(msg[i],mas[j])){  
 msgv.push(j);  
 }  
 }  
 }  
 let text=[0];  
 for(let i=0;i<msgv.length;i++){  
 text.push(***Math***.pow(text[i]+msgv[i],2)%n)  
 }  
 alert("Хеш образ: "+text[text.length-1]);  
 let res=***Math***.pow(text[text.length-1],d)%n;  
 alert("Цифровий підпис: "+res);  
 for(let i=0;i<msg1.length;i++){  
 for(let j=0;j<mas.length;j++){  
 if(***Object***.is(msg1[i],mas[j])){  
 msgv1.push(j);  
 }  
 }  
 }  
 let text1=[0];  
 for(let i=0;i<msgv.length;i++){  
 text1.push(***Math***.pow(text1[i]+msgv1[i],2)%n)  
 }  
 alert("Обчислений хеш образ: "+text1[text1.length-1]);  
 if(text1[text1.length-1]===text[text.length-1]){  
 alert("Спотворення повідомлення не відбулось H=H'")  
  
 }  
 else{  
 alert("Спотворення повідомлення відбулось H!=H'")  
 }  
}



**Висновок** навчився розробляти Ui складову сайту з допомогою CSS і HTML