Лабораторна робота №1

Тема: мануальний, напівавтоматичний й автоматичний криптоаналіз найпростіших шифрів: Цезаря і Віженера.

Мета роботи: навчитися класифікувати найпростіші шифри зі зрушеннями: Цезаря і Віженера. Вміти вказати шляхи побудови криптоаналітичних алгоритмів для відкриття найпростіших шифрів і провести криптоаналіз.

Хід роботи

Код програми для шифрів Цезаря та Віженера.

Index.html:

<!DOCTYPE html>

<html lang="en">

    <head>

        <meta charset="UTF-8" />

        <meta name="viewport" content="width=device-width, initial-scale=1.0" />

        <title>Шифр цезаря и Виженера</title>

        <style>

            #CodeString,

            #CodeStringV {

                width: 500px;

            }

            form {

                border: 1px solid black;

                padding: 10px;

                width: 520px;

            }

        </style>

    </head>

    <body>

        <form>

            <h2>Шифр Цезаря</h2>

            <div>

                <input

                    type="text"

                    id="CodeString"

                    placeholder="Строка для шифрования/дешифровки"

                />

            </div>

            <div>

                <input type="radio" id="encrypt" name="crypt" value="encrypt" checked />

                <label for="encrypt">Зашифровать</label>

                <input type="radio" id="decrypt" name="crypt" value="decrypt" />

                <label for="decrypt">Расшифровать</label>

                <div>

                    <input type="number" name="" id="shift" placeholder="Сдвиг" />

                    <button id="caesarBtn">OK</button>

                </div>

                <h3 id="caes">Результат</h3>

            </div>

        </form>

        <br />

        <form>

            <h2>Шифр Виженера</h2>

            <div>

                <input

                    type="text"

                    id="CodeStringV"

                    placeholder="Строка для шифрования/дешифровки"

                />

            </div>

            <div>

                <input

                    type="radio"

                    id="encrypt"

                    name="cryptV"

                    value="encrypt"

                    checked

                />

                <label for="encrypt">Зашифровать</label>

                <input type="radio" id="decrypt" name="cryptV" value="decrypt" />

                <label for="decrypt">Расшифровать</label>

                <div>

                    <input

                        type="text"

                        name=""

                        id="keyWord"

                        placeholder="Ключевое слово"

                    />

                    <button id="vizhBtn">OK</button>

                </div>

                <h3 id="vig">Результат</h3>

            </div>

        </form>

        <script src="./lab1.js"></script>

    </body>

</html>

Index.js

let shift=1;

let keyword;

const caesarBtn=document.querySelector("button#caesarBtn");

const vizhBtn=document.querySelector("button#vizhBtn");

const inputString=document.querySelector("#CodeString");

const inputStringV=document.querySelector("#CodeStringV");

const inputShift=document.querySelector("#shift");

const inputKeyWord=document.querySelector("#keyWord");

const inputRadios=document.getElementsByName("crypt");

const inputRadiosV=document.getElementsByName("cryptV");

let radioValue;

let keys=new Array();

let string="вова";

let arrString="";

let result;

let letters=['а','б','в','г','д','е',/\*'ё',\*/'ж','з','и','й','к','л','м','н','о','п','р',

'с','т','у','ф','х','ц','ч','ш','щ','ь','ы','ъ','э','ю','я'];

caesarBtn.addEventListener('click', e=> {

    arrString="";

    inputRadios.forEach(e=>{

        if(e.checked) {

            radioValue=e.value;

        }

    });

    e.preventDefault();

    string=inputString.value;

    shift=parseInt(inputShift.value,10);

    Caesar();

});

vizhBtn.addEventListener('click', e=> {

    arrString="";

    inputRadiosV.forEach(e=>{

        if(e.checked) {

            radioValue=e.value;

        }

    });

    e.preventDefault();

    string=inputStringV.value;

    keyWord=inputKeyWord.value;

    Vigenere();

});

let word=false;

function Caesar() {

    if(radioValue==="encrypt") {

        for(let i=0;i<string.length;i++) {

            word=false;

            for(let j=0;j<letters.length;j++) {

                if(string[i]===letters[j]) {

                    if(j+shift>31) {

                        arrString=arrString +(letters[(j+shift)-32]);

                        word=true;

                        break;

                    } else {

                        arrString=arrString +(letters[j+shift]);

                        word=true;

                        break;

                    }

                }

            }

            if(word===false) {

                arrString=arrString +(string[i]);

            }

        }

    } else {

        for(let i=0;i<string.length;i++) {

            word=false;

            for(let j=0;j<letters.length;j++) {

                if(string[i]===letters[j]) {

                    if(j-shift<0) {

                        arrString=arrString +(letters[(j-shift)+32]);

                        word=true;

                        break;

                    } else {

                        arrString=arrString +(letters[j-shift]);

                        word=true;

                        break;

                    }

                }

            }

            if(word===false) {

                arrString=arrString +(string[i]);

            }

        }

    }

    document.querySelector("h3#caes").innerHTML="Результат: "+arrString;

    console.log(arrString);

}

function Vigenere() {

    let keyIndex=0;

    if(radioValue==="encrypt") {

        for(let i=0;i<string.length;i++) {

            word=false;

            for(let j=0;j<letters.length;j++) {

                if(keyIndex===keyWord.length) {

                    keyIndex=0;

                }

                for(let m=0;m<letters.length;m++) {

                    if(keyWord[keyIndex]===letters[m]) {

                        shift=m;

                        break;

                    } else {

                        shift=0;

                    }

                }

                if(string[i]===letters[j]) {

                    if(j+shift>31) {

                        arrString=arrString +(letters[(j+shift)-32]);

                        word=true;

                        keyIndex++;

                        keys.push(keyWord[keyIndex-1]);

                        break;

                    } else {

                        arrString=arrString +(letters[j+shift]);

                        word=true;

                        keyIndex++;

                        keys.push(keyWord[keyIndex-1]);

                        break;

                    }

                }

            }

            if(word===false) {

                arrString=arrString +(string[i]);

                keys.push(" ");

            }

        }

    } else {

        for(let i=0;i<string.length;i++) {

            word=false;

            for(let j=0;j<letters.length;j++) {

                if(keyIndex===keyWord.length) {

                    keyIndex=0;

                }

                for(let m=0;m<letters.length;m++) {

                    if(keyWord[keyIndex]===letters[m]) {

                        shift=m;

                        break;

                    } else {

                        shift=0;

                    }

                }

                if(string[i]===letters[j]) {

                    if(j-shift<0) {

                        // console.log("сдвиг=",j+shift,j,shift);

                        arrString=arrString +(letters[(j-shift)+32]);

                        word=true;

                        keyIndex++;

                        keys.push(keyWord[keyIndex-1]);

                        break;

                    } else {

                        // console.log("сдвиг=",j+shift,j,shift);

                        arrString=arrString +letters[j-shift];

                        word=true;

                        keyIndex++;

                        keys.push(keyWord[keyIndex-1]);

                        break;

                    }

                }

            }

            if(word===false) {

                arrString=arrString +(string[i]);

                keys.push(" ");

            }

        }

    }

    document.querySelector("h3#vig").innerHTML="Результат: "+arrString;

    console.log(arrString);

    console.log(keys);

}

Результати роботи програми.

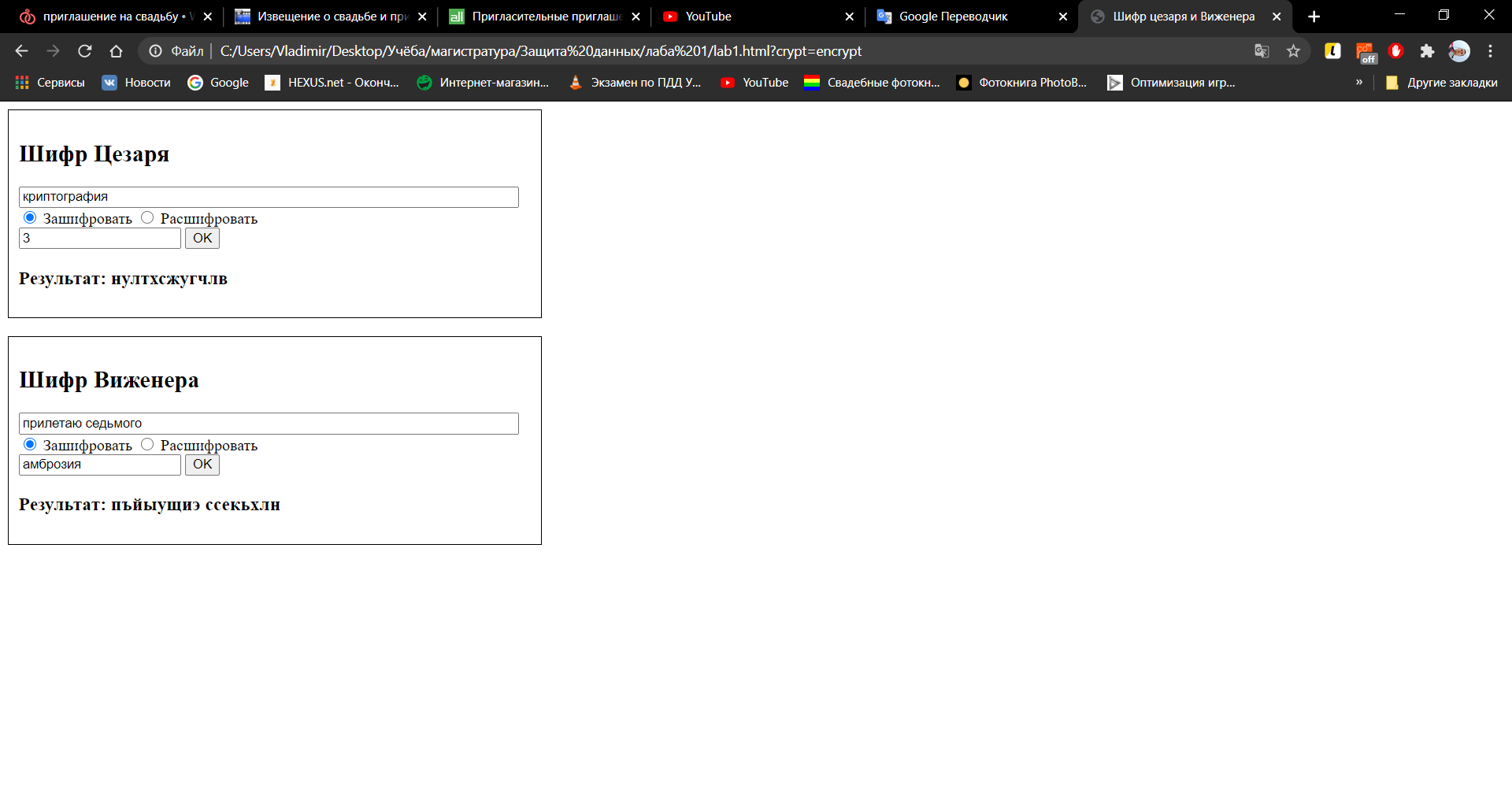


Рисунок 1 – перевірка роботи шифрів на основі прикладів з методички (шифрування)

Шифр Цезаря в розробленому варіанті відрізняється на одну букву від прикладу з методички, так як використовується російський алфавіт без букви «ё».

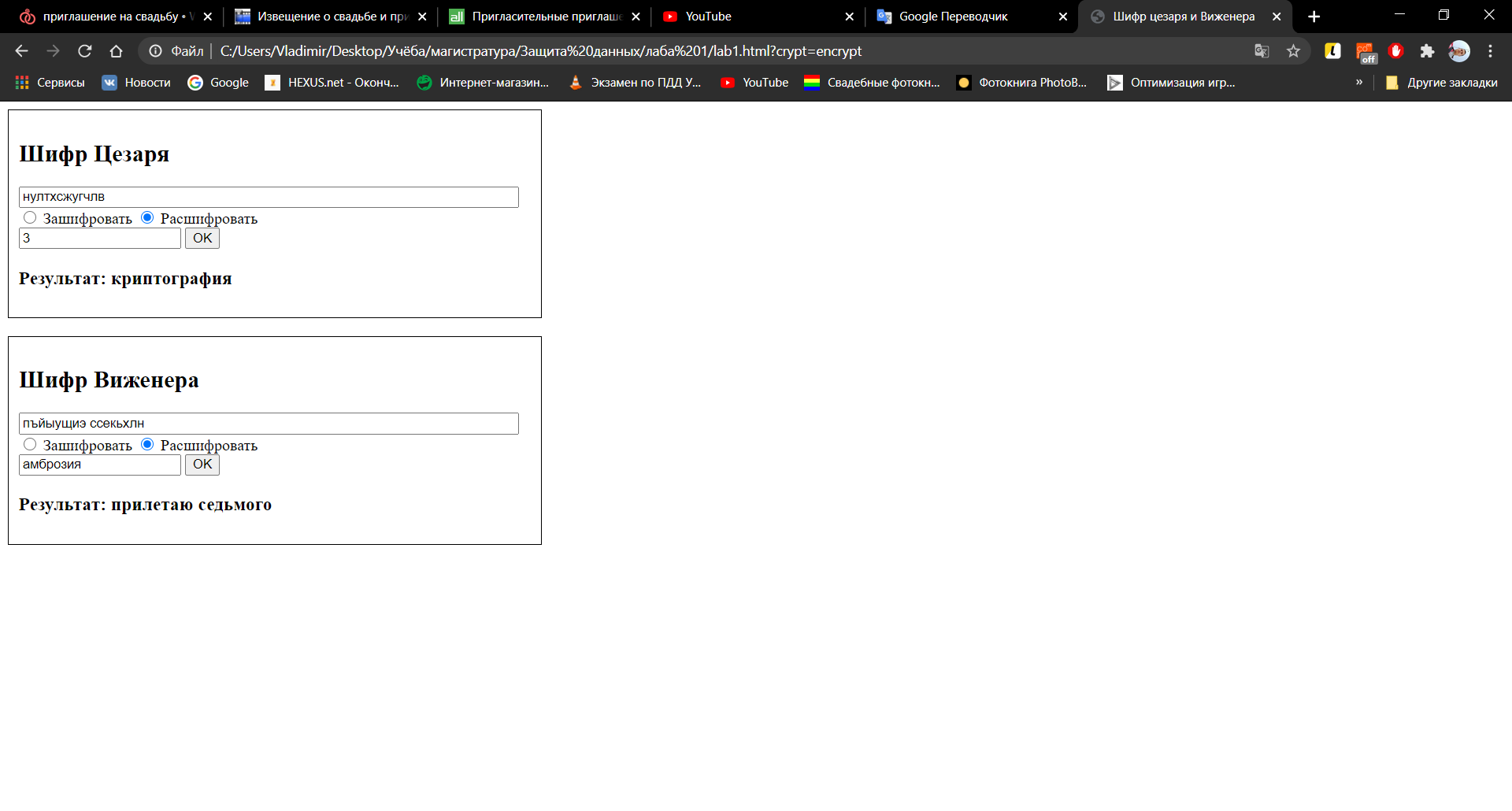


Рисунок 2 – Дешифрування прикладів з рисунка 1.

Шифрування/дешифрування фрази: «как много ещё нужно сделать».

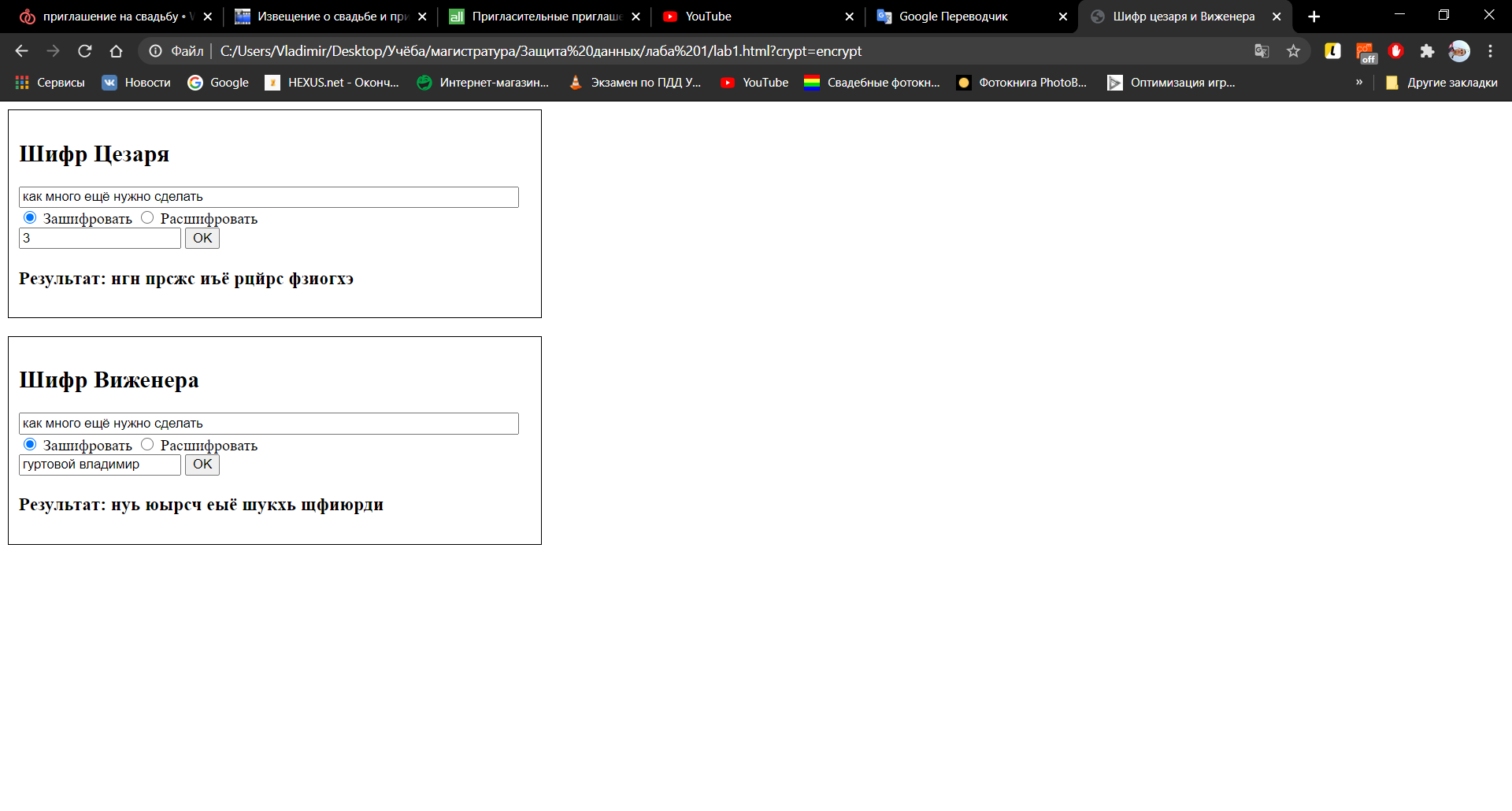


Рисунок 3 – Шифрування фрази «как много ещё нужно сделать»

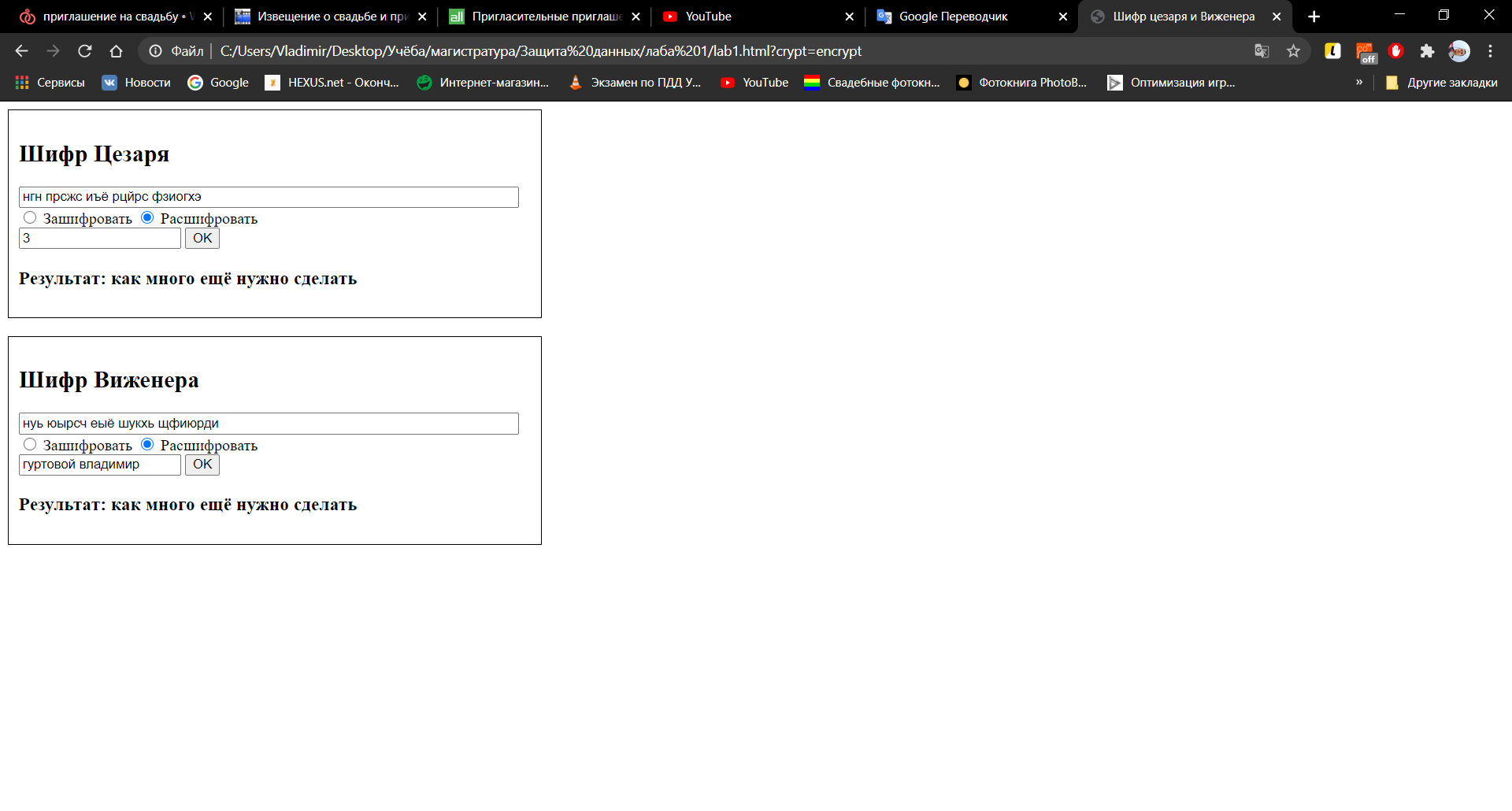


Рисунок 4 – Дешифрування фрази з рисунка 3

Криптоаналіз.

Шифр Цезаря найбільш простий шифр для злому, так як величина зрушення постійна. Покращити стійкість шифру можливо за допомогою збільшення розміру алфавіту.

Шифр Віженера – більш складний, так як величина зрушення змінюється. Для збільшення стійкості шифру потрібно збільшувати алфавіт, також має значення величина ключа та повторення символів в ключі.