Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет пищевых и химических технологий»

Кафедра автоматизации технологических процессов и производств

**Криптографические методы защиты информации**

**Отчёт по практической работе №2**

Вариант 3

по дисциплине «Основы защиты информации»

Специальность 1 – 40 05 01 Информационные системы и технологии

Направление специальности 1 – 40 05 01 – 11 Информационные системы и технологии (в пищевой промышленности)

|  |  |
| --- | --- |
| Проверил  Старший преподаватель  О.Б.Ганак  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_2023 г. | Выполнил  студент группы ИСИТ-191  О.А.Васечко  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

Могилев 2023

**Цель работы:** Написать программу с помощью любого языка программирования с использованием шифра Вернама (XOR-шифр) (латинский алфавит, ключ: BEGIN).

**Ход выполнения работы:**

Шифрование — это такое преобразование исходного сообщения, которое не позволит всяким нехорошим людям прочитать данные, если они это сообщение перехватят. Делается это преобразование по специальным математическим и логическим алгоритмам.

Исходное сообщение — это, собственно, то, что мы хотим зашифровать. Классический пример — текст.

Шифрованное сообщение — это сообщение, прошедшее процесс шифрования.

Шифр — это сам алгоритм, по которому мы преобразовываем сообщение.

Ключ — это компонент, на основе которого можно произвести шифрование или дешифрование.

Алфавит — это перечень всех возможных символов в исходном и зашифрованном сообщении. Включая цифры, знаки препинания, пробелы, отдельно строчные и заглавные буквы и т.д.

Для разработки программы шифрования был выбран язык программирования JavaScript, а также для визуальной части были использованы язык разметки HTML и таблица стилей CSS.

На листинге 1 представлена программа шифрования и дешифровки сообщения по заданному ключу.

function shifr(message, key) {

    const k = document.getElementById('key');

    const m = document.getElementById('mes');

    const x = document.getElementById('xor');

    const ch = document.getElementById('ch');

    let binKey = [];

    let binMess = [];

    let binXor = [];

    let chXor = [];

    let one = '';

    if (key.length === message.length) {

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

            binKey.push(key[i].toUpperCase().charCodeAt(0).toString(2));

        }

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

            binMess.push(message[j].toUpperCase().charCodeAt(0).toString(2));

        }

        for (let k = 0; k < binKey.length; k++) {

            for (let l = 0; l < binKey[k].length; l++) {

                one += binKey[k][l] ^ binMess[k][l];

            }

            binXor.push(one);

            chXor.push(parseInt(one, 2));

            one = '';

        }

        k.innerHTML = binKey;

        m.innerHTML = binMess;

        x.innerHTML = binXor;

        ch.innerHTML = chXor;

        rashifrovka(key, chXor);

    } else {

        alert('ключ и сообщение должны быть одной длины');

    }

}

function rashifrovka(key, numbers) {

    const ans = document.getElementById('rash');

    let binMess = [];

    let binKey = [];

    let binXor = [];

    let one = '';

    let res = '';

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

        binKey.push(key[i].toUpperCase().charCodeAt(0).toString(2));

    }

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

        binMess.push(addZeros(numbers[j].toString(2)));

    }

    for (let k = 0; k < binKey.length; k++) {

        for (let m = 0; m < binKey[k].length; m++) {

            one += binKey[k][m] ^ binMess[k][m];

        }

        res += String.fromCharCode(parseInt(one, 2));

        binXor.push(one);

        one = '';

    }

    ans.innerHTML = res;

}

function addZeros(x) {

    let res = x;

    let howMuch = 7 - x.length;

    let zeros = '';

    for (let i = 0; i < howMuch; i++) {

        zeros += '0';

    }

    return zeros + x

}

Листинг 1 – код программы шифрования

На рисунке 1 представлен результат работы программы шифрования методом Вернама (XOR - шифра).

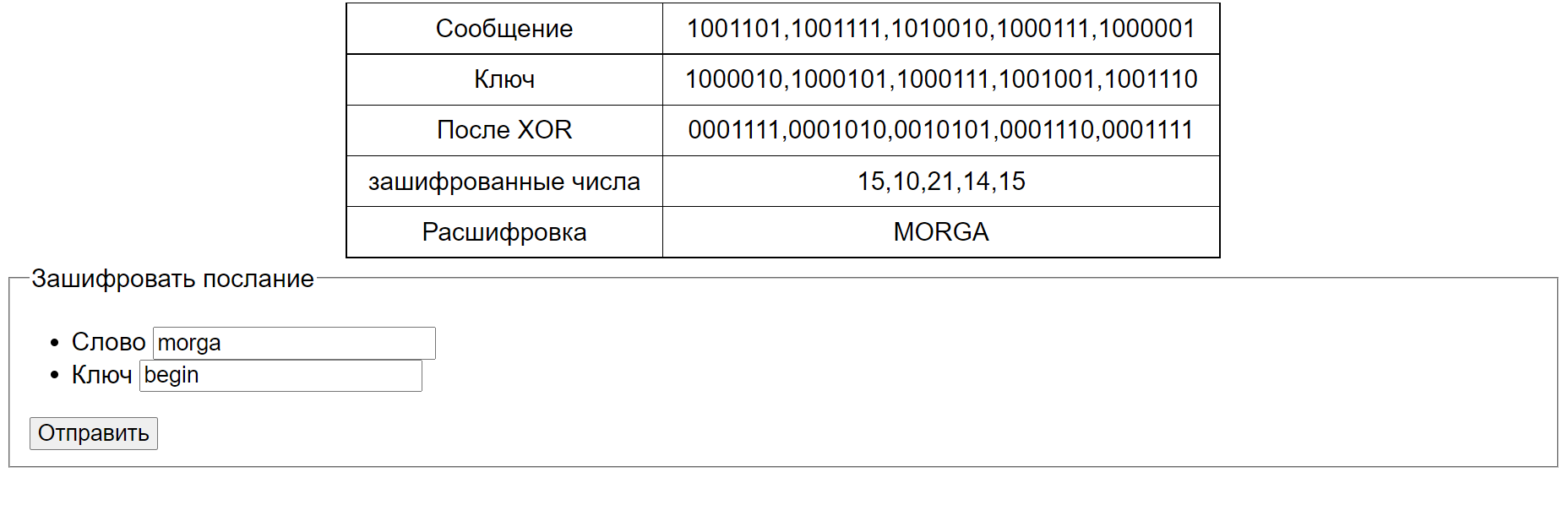


Рисунок 1 – Результат работы программы шифрования

**Вывод:** В ходе выполнения практической работы были изучены криптографические методы защиты информации, а также разработана программа зашифровки/дешифровки сообщения с помощью языка программирования JavaScript.