Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет информатики и радиоэлектроники»

Кафедра инженерной психологии и эргономики

Практическая работа №1

«Криптоанализ классических шифров»

|  |  |
| --- | --- |
| Выполнил: ст. гр. 910901 | Нехайчик И. И. |
| Проверил: | Давыдович К. И. |

Минск 2022

**Задание**

Ниже два шифртекста одного и того же сообщения, зашифрованные с помощью классических шифров:

1. Шифр Цезаря – Шифртекст: Srobdoskdehwlf vxevwlwxwlrq flskhuv.
2. Шифр простой замены – Шифртекст: KjgyVgkcVWZqdX nsWnqdqsqdji XdkcZmn.
3. Напишите программу дешифрования, используя любой известный вам язык программирования: найдите соответствующий открытый текст, вскрыв шифр Цезаря, а затем найдите ключ шифра простой замены, используя для дешифрования известный открытый текст. Обе атаки должны быть полностью описаны.
4. Напишите программу, используя любой известный вам язык программирования:

* зашифруйте свою фамилию, имя отчество;
* дешифруйте полученный текст;
* сравните с исходным текстом.

**Листинг кода**

const CEASAR\_CIPHER\_KEY = 23;

const CEASAR\_CIPHER\_STRING = 'Srobdoskdehwlf vxevwlwxwlrq flskhuv';

const SIMPLE\_REPLACEMENT\_CIPHRE\_STRING = 'KjgyVgkcVWZqdX nsWnqdqsqdji XdkcZmn';

function shiftLetters(str, key) {

  let newStr = '';

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

    if (str.charCodeAt(i) >= 65 && str.charCodeAt(i) <= 90) {

      newStr += String.fromCharCode((str.charCodeAt(i) + key - 65) % 26 + 65);

    } else if (str.charCodeAt(i) >= 97 && str.charCodeAt(i) <= 122) {

      newStr += String.fromCharCode((str.charCodeAt(i) + key - 97) % 26 + 97);

    } else {

      newStr += String.fromCharCode(str.charCodeAt(i));

    }

  }

  return newStr;

}

function CeasarCipherDecryption(str, key) {

  if (key) {

    return shiftLetters(str, key);

  }

  const arrOfStr = [];

  for (let key = 1; key <= 25; key++) {

    const newStr = shiftLetters(str, key);

    arrOfStr.push(`key: ${key}; string: ${newStr}`);

  }

  return arrOfStr;

}

function getKeyOfSimpleReplacementCipher(str) {

  let decryptedPhrase = CeasarCipherDecryption(CEASAR\_CIPHER\_STRING, CEASAR\_CIPHER\_KEY);

  let key = '';

  for (let i = 65; i <= 90; i++) {

    let decryptedArr = decryptedPhrase.toUpperCase().split('');

    let strArr = str.toUpperCase().split('');

    let index = decryptedArr.findIndex(el => el.charCodeAt() === i);

    if (index !== -1) {

      key += strArr[index];

    } else {

      key += '\*';

    }

  }

  return key;

}

console.log('Finding key of Ceasar cipher: ')

console.log(CeasarCipherDecryption(CEASAR\_CIPHER\_STRING));

console.log(`Decrypted phrase od Ceasar cipher: ${CeasarCipherDecryption(CEASAR\_CIPHER\_STRING, CEASAR\_CIPHER\_KEY)}`);

console.log(`Key of simple replacement cipher: ${getKeyOfSimpleReplacementCipher(SIMPLE\_REPLACEMENT\_CIPHRE\_STRING)}`);

**Вывод в консоли**

