Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования
Кафедра инженерной психологии и эргономики

КРИПТОГРАФИЧЕСКИЕ ТЕХНОЛОГИИ

Практическая работа №1
Криптоанализ классических шифров

Выполнил:
Глик А. Г.

Проверил:
Давыдович К.И.

Минск 2023

Цель работы:

Изучить виды классических криптографических шифров и методы работы с ними.

Ход работы:

Задание

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

a. Цезарь – Шифртекст 1.

Srobdoskdehwlf vxevwlwxwlrq flskhuv

b. Простой замены – Шифртекст 2.

KjgyVgkcVWZqdX nsWnqdqsqdji XdkcZmn

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.

2. Напишите программу, используя любой известный вам язык программирования:

- зашифруйте свою фамилию, имя отчество
- дешифруйте полученный текст
- сравните с исходным текстом

3. Подготовьте отчет, включая задание, код программы, скриншоты, результаты работы программы.

Вывод:

В ходе работы произошло ознакомление с методическим материалом и дополнительной информацией, связанной с предоставленной темой; было разработано приложение, полностью покрывающее задачу, изложенную в вышепредставленных требованиях задания для практического занятия. В приложениях А и Б предоставлены код программы и результат ее работы соответственно.

ПРИЛОЖЕНИЕ А

(обязательное)

Листинг кода программы

```
import readline from 'readline';

readline.emitKeypressEvents(process.stdin);

let rl = readline.createInterface({
  input: process.stdin,
  output: process.stdout,
});

let alphabet = 'abcdefghijklmnopqrstuvwxyz';
const TEXT = 'Srobdoskdehwlf vxevwlwxwlrq flskhuv';
const secondCipher = 'KjgyVgkcVWZqdX nsWnqdqsqdji XdkcZmn';
let complianceTable = {};
let shift = 0;
let output = '';

function second() {
  rl.question('Enter text: ', (userInput) => {
    const encryptedText = encryptText(userInput);
    console.log('Ciphred text: ', encryptedText);
    rl.close();
  });

  function encryptText(input) {
    const encryptedChars = input.split('').map((char) => {
      if (complianceTable[char]) {
        return complianceTable[char];
      } else { return '*'; }});
    return encryptedChars.join('');
  }}

process.stdin.on('keypress', (ch, key) => {
  if (key.name == 'left') {
    console.log(toShift(-1));
  } else if (key.name == 'right') {
```

```
    console.log(toShift(1));
  } else if (key.name === 'up') {
    output = toShift(0);
    shift = 0;
    console.log('~~~ Alphabet saved ~~~');
    complianceTable = createCipherObject(secondCipher.toLowerCase(), output);
    second();
  } else if (key && key.ctrl && key.name == 'c') {
    process.stdin.pause();
  };
});

function toShift(direction) {
  shift += direction;
  const input = TEXT.toLowerCase();
  return input.split('').map((e) => {
    if (alphabet.includes(e)) {
      return alphabet[(alphabet.indexOf(e) + shift + alphabet.length) %
alphabet.length];
    } else return e;
  }).join('');
};

function createCipherObject(secondCipher, output) {
  const cipherObject = {};
  secondCipher.split('').forEach((e, i) => {
    cipherObject[output[i]] = e;
  })
  return cipherObject;
}

process.stdin.setRawMode(true);
```

ПРИЛОЖЕНИЕ Б

(обязательное)

Результаты работы программы

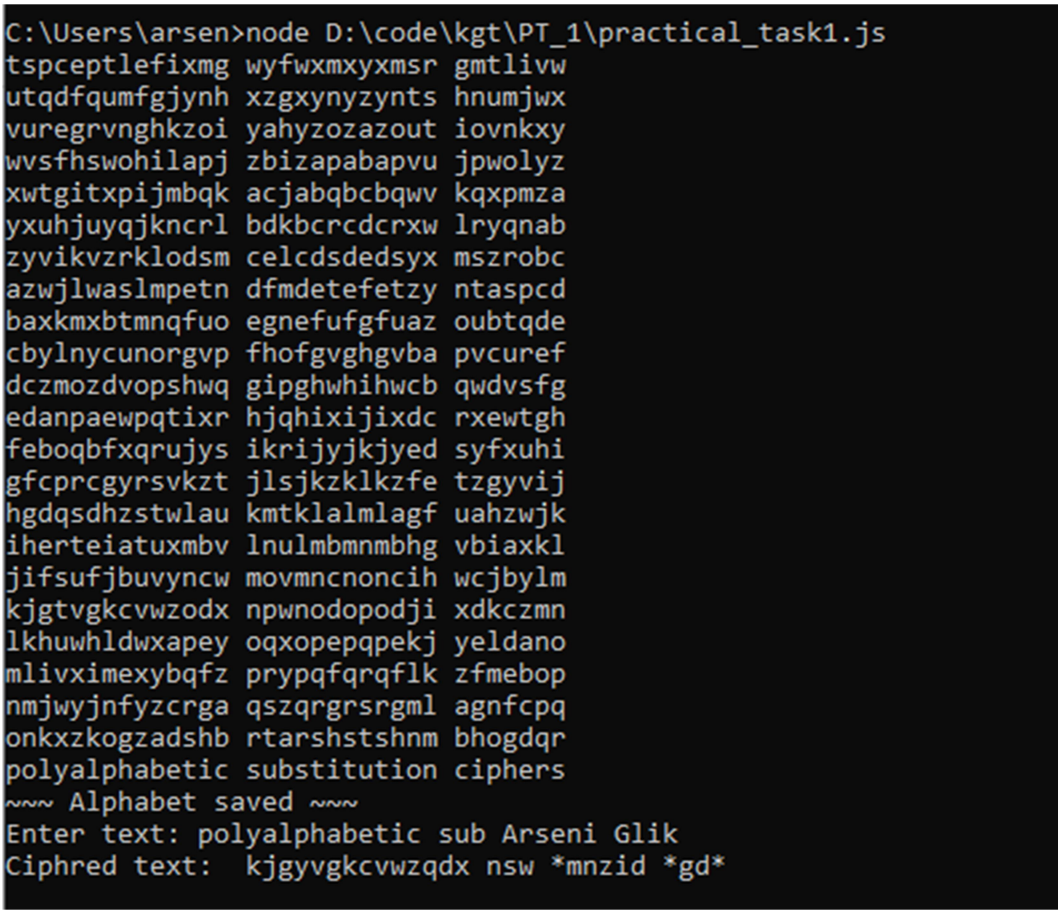

Рисунок Б – Результат работы приложение