Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования
Кафедра инженерной психологии и эргономики

КРИПТОГРАФИЧЕСКИЕ ТЕХНОЛОГИИ

Практическая работа №4
Исследование ассиметричных алгоритмов шифрования

Выполнил:
Глик А. Г.

Проверил:
Давыдович К.И.

Минск 2023

Цель работы:

Основная часть занятия состоит в закреплении теоретического материала курса, приобретении навыков выполнения задач по основам криптографических технологий, анализа результатов, грамотного оформления отчетов, в частности: создание ключей в системе PGP, передача подписанных и защищенных сообщений.

Теоретические сведения:

PGP использует два взаимосвязанных ключа - открытый и закрытый, которые позволяют пользователям обмениваться подписанными и зашифрованными сообщениями.

Открытые ключи могут быть публикованы на сервере открытых ключей или распространены среди корреспондентов, в то время как закрытые ключи хранятся в каталоге секретных ключей. PGP также предоставляет функции генерации ключей, шифрования и расшифровки файлов, а также наложения и проверки электронной подписи.

Ход работы:

Задание

Вариант 5

1. Переведите число 3^{43} в двоичную систему счисления.
2. Пусть каждая из 16 первых букв русского алфавита имеет четырехразрядный двоичный код, соответствующий номеру от 0 до 15.
    2.1. Составьте из этих букв произвольное сообщение состоящее из 32 символов.
    2.2. Разбейте полученное сообщение на блоки длиной 64 бита.
    2.3. Значения полученных блоков запишите в десятичной системе счисления.
3. Найдите состояние 28-разрядного двоичного регистра сдвига после циклического сдвига влево на 5, числа X = 179327333 (Вариант 5), предварительно записанного в регистр.
4. Найдите сумму по модулю 2 двух чисел 224489930110 и X = 179327333 (Вариант 5).

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

```
function decimalToBinary(number,  exp) {
  return (BigInt(number) ** BigInt(exp)).toString(2);
}

console.log(`1. ${decimalToBinary(3, 43)}`);

const letterToBinary = {};
const alphabet = 'АБВГДЕЖЗИЙКЛМНОП'; // 16 букв русского алфавита
const message = "ЗИЙКЛМНОПАБВГДЕЖ";

for (let i = 0; i < alphabet.length; i++) {
  const letter = alphabet[i];
  const binaryCode = (i).toString(2).padStart(4, '0');
  letterToBinary[letter] = binaryCode;
}


function splitMessageIntoBlocks(message, blockSize) {
  let blocks = null;
  for (let i = 0; i < message.length; i += blockSize) {
    blocks = message.slice(i, i + blockSize);
  }
  return blocks;
}

// Функция для конвертации блока букв в двоичный блок
function convertLettersToBinary(block) {
  let binaryBlock = "";
  for (const letter of block) {
    binaryBlock += letterToBinary[letter];
  }
  return binaryBlock;
}

// block to bin
```

```
        function binaryToDecimal(binaryBlock) {
  return parseInt(binaryBlock, 2);
}

const blockSize = 64;
const block = splitMessageIntoBlocks(message, blockSize);

// каждый блок в двоичный и затем в десятичный формат
const decimalValues = binaryToDecimal(convertLettersToBinary(block));

console.log(`2. Значения полученных блоков в десятичной системе счисления: ${decimalValues}`);


/*------PART 3-------*/
let X = 179327333;
const bitLength = 28;
const shiftBits = 5;
X = ((X << shiftBits) | (X >> (bitLength - shiftBits))) & ((1 << bitLength) - 1);
console.log(`3. Состояние 28-разрядного регистра после циклического сдвига на 5 разрядов: ${X}`);
/*влево на 5 разрядов для числа X, а затем обрезает результат до 28 разрядов с помощью маски ((1 << bitLength) - 1). */

/*-----PART 4-----*/
const number1 = 224489930110;
const number2 = 179327333;
const sumMod2 = (number1 + number2) % 2;

console.log(`5. Сумма ${number1} и ${number2} по модулю 2: ${sumMod2}`);
```

ПРИЛОЖЕНИЕ Б

(обязательное)

Результаты работы программы

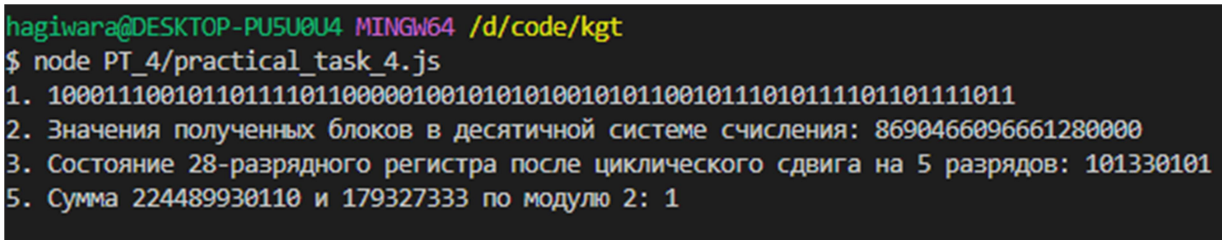

Рисунок Б – Результат работы приложение