БУ ВО Ханты – Мансийского автономного округа – Югры

«Сургутский государственный университет»

Политехнический институт

Кафедра автоматики и компьютерный систем

**ЛАБОРАТОРНАЯ РАБОТА №2**

по дисциплине: «Основы защиты информации»

по теме: «Шифрование RSA»

Выполнила: студентка группы №609-11

Пашина Илона Руслановна

Приняла: старший преподаватель кафедры АиКС

Кривицкая Марина Александровна

Сургут

2024 г.

**Тема**: шифрование с открытым ключом.

**Задание на лабораторную работу:**

1. Программно реализовать шифрование/дешифрование RSA

**Среда реализации**: любая.

**Листинг**

package main

import (

"crypto/rand"

"fmt"

"math/big"

)

func generateRandomPrime(phi \*big.Int) \*big.Int {

for {

e, err := rand.Prime(rand.Reader, 100)

if err != nil {

panic(err)

}

if new(big.Int).GCD(nil, nil, e, phi).Cmp(big.NewInt(1)) == 0 {

return e

}

}

}

func generateKeys(bits int) (publicKey, privateKey, n \*big.Int) {

p, err := rand.Prime(rand.Reader, bits/2)

if err != nil {

panic(err)

}

q, err := rand.Prime(rand.Reader, bits/2)

if err != nil {

panic(err)

}

n = new(big.Int).Mul(p, q)

phi := new(big.Int).Mul(new(big.Int).Sub(p, big.NewInt(1)), new(big.Int).Sub(q, big.NewInt(1)))

e := generateRandomPrime(phi)

d := new(big.Int).ModInverse(e, phi)

publicKey = new(big.Int).Set(e)

privateKey = new(big.Int).Set(d)

return

}

func crypt(Key, text, n \*big.Int) \*big.Int {

return new(big.Int).Exp(text, Key, n)

}

func main() {

publicKey, privateKey, n := generateKeys(2048)

plaintext := big.NewInt(12345)

ciphertext := crypt(publicKey, plaintext, n)

decrypted := crypt(privateKey, ciphertext, n)

fmt.Println("Публичный ключ:", publicKey)

fmt.Println("Секретный ключ:", privateKey)

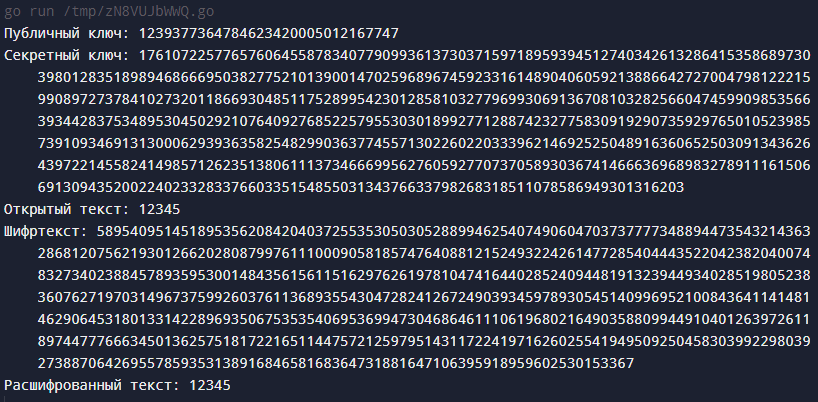
fmt.Println("Открытый текст:", plaintext)

fmt.Println("Шифртекст:", ciphertext)

fmt.Println("Расшифрованный текст:", decrypted)

}

**Пример работы программы:**



**Вывод:**

В ходе лабораторной работы был изучен и написан код шифрования/дешифрования RSA.