Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

**Лабораторная работа №3**

По дисциплине «Криптографические методы защиты информации»

Тема: «Программная реализация ЭЦП»

**Выполнил:**

Студент 3 курса

Группы ИИ-21

Карагодин Д.Л.

**Проверил:**

Хацкевич А.С.

Брест 2023

**Цель работы:** Создать программу, которая реализует учебный вариант схем ЭЦП, используя алгоритмы с открытыми ключами.

**Ход работы:**

**Вариант 1 (**ЭЦП на базе Эль-Гамаля**)**

**Код программы:**

import random

import math

def is\_coprime(a, b):

    # Проверка на взаимную простоту двух чисел

    return math.gcd(a, b) == 1

def generate\_key(p, g):

    # Генерация секретного ключа

    private\_key = random.randint(1, p - 1)

    # Вычисление открытого ключа

    public\_key = pow(g, private\_key, p)

    return private\_key, public\_key

def sign\_message(message, p, g, private\_key):

    while True:

        # Генерация случайного числа k

        k = random.randint(1, p - 2)

        if is\_coprime(k, p - 1):

            break

    # Вычисление первой компоненты подписи (r)

    r = pow(g, k, p)

    # Вычисление второй компоненты подписи (s)

    inverse\_k = pow(k, -1, p - 1)

    hash\_message = hash(message)  # Здесь может быть использован любой хеш-алгоритм

    s = (hash\_message - private\_key \* r) \* inverse\_k % (p - 1)

    return r, s

def verify\_signature(message, signature, p, g, public\_key):

    r, s = signature

    # Вычисление левой и правой частей равенства для проверки подписи

    left\_side = pow(g, hash(message), p)

    right\_side = (pow(public\_key, r, p) \* pow(r, s, p)) % p

    # Проверка подписи

    if left\_side == right\_side:

        return True

    else:

        return False

# Пример использования алгоритма

p = 23  # Простое число

g = 5   # Генератор поля

# Генерация ключей

private\_key, public\_key = generate\_key(p, g)

# Подписание сообщения

message = "Hello, world!"

signature = sign\_message(message, p, g, private\_key)

# Проверка подписи

is\_valid = verify\_signature(message, signature, p, g, public\_key)

print("Подпись верна:", is\_valid)

**Результат программы:**

Подпись верна: True

Изменим строку «is\_valid = verify\_signature(message, signature, p, g, public\_key)» на строку «is\_valid = verify\_signature(”New message”, signature, p, g, public\_key)» .

**Результат программы:**

Подпись верна: False

**Вывод:** создал программу, которая реализует учебный вариант схем ЭЦП, используя алгоритмы с открытыми ключами.