Министерство образования Республики Беларусь

Учреждение образования

БелорусскиЙ государственный университет

информатики и радиоэлектроники

Факультет Компьютерных Систем и Сетей

Кафедра Программного Обеспечения Информационных Технологий

Отчёт по лабораторной работе №3 на тему:

КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

Выполнил

Студент гр.351001 А.Д. Шевченко

Проверил C.В. Болтак

Минск, 2025

**Условие:**

**Вариант 2**

Реализовать шифратор и дешифратор *алгоритма* ***Эль-Гамаля*** файла c произвольным содержимым, используя алгоритм быстрого возведения в степень, а также реализовать вычисление открытого ключа ***g*** при данном значении ***p***, используя алгоритм нахождения первообразного корня по модулю. Значения параметров ***p*, *x*** и ***k***задаются пользователем*.* Программа должна осуществлять проверку ограничений на вводимые пользователем значения параметров алгоритма. Организовать вывод содержимого зашифрованного файла на экран в виде чисел в 10-й системе счисления. Вывести значение ***g*** на экран. Результат работы программы – зашифрованный/расшифрованный файл/ы.

Используя алгоритм из методички, искать все первообразные корни по модулю ***p.*** Все найденные корни вывести на экран и предложить для шифрования ввести на выбор любой из найденных.

При использовании длинной арифметики для определения простоты числа использовать один из вероятностных тестов: тест Ферма или тест Миллера-Рабина.

**Тест №1 Шифрование и дешифрование текстового файла.**

Исходный файл:

A screenshot of a computer

AI-generated content may be incorrect.

Заданные параметры шифрования:

P = 461. X = 10. K = 191. G = 176. Y = 102.

A screenshot of a computer

AI-generated content may be incorrect.

Файл после шифрования:

A screenshot of a computer

AI-generated content may be incorrect.

Заданные параметры дешифрования:

P = 461. X = 10.

A screenshot of a computer

AI-generated content may be incorrect.

Файл после дешифрования:

A screenshot of a computer

AI-generated content may be incorrect.

**Тест №2 Шифрование и дешифрование изображения.**

Исходный файл:

A person taking a selfie

AI-generated content may be incorrect.

Заданные параметры шифрования:

P = 557. X = 52. K = 383. G = 30. Y = 236.

A screenshot of a computer

AI-generated content may be incorrect.

Файл после шифрования:

A screenshot of a computer

AI-generated content may be incorrect.

Заданные параметры дешифрования:

P = 557. X = 52.

A screenshot of a computer

AI-generated content may be incorrect.

Файл после дешифрования:

A person with his hand on his face

AI-generated content may be incorrect.