Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет   
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Методы защиты информации

ОТЧЁТ

к лабораторной работе №4

на тему

**АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ. АЛГОРИТМ МАК-ЭЛИСА**

Выполнил: студент гр.253505 Ющук И.А.

Проверил: ассистент кафедры информатики Герчик А.В.

Минск 2025

**СОДЕРЖАНИЕ**

[Введение 3](#_Toc207721845)

[1 Ход работы 4](#_Toc207721846)

[Заключение 4](#_Toc207721847)

[Приложение А (обязательное) Листинг программного кода 6](#_Toc207721848)

# ВВЕДЕНИЕ

Современный этап развития информационных технологий характеризуется повсеместным использованием цифровых коммуникаций и необходимостью обеспечения конфиденциальности, целостности и аутентичности передаваемых данных. Криптография, как наука о методах защиты информации, играет ключевую роль в решении этих задач. В отличие от симметричных криптосистем, где для шифрования и дешифрования используется один и тот же секретный ключ, асимметричная криптография основана на использовании двух различных, но математически связанных ключей: открытого (*public key*) и закрытого (*private key*). Это фундаментальное различие устраняет одну из главных проблем симметричного шифрования — безопасную передачу секретного ключа.

Открытый ключ предназначен для шифрования данных и может свободно распространяться, в то время как закрытый ключ, используемый для дешифрования, хранится в секрете. Такая архитектура обеспечивает основу для решения критически важных задач информационной безопасности, таких как конфиденциальная передача сообщений, цифровая подпись и аутентификация. Наиболее известными и широко применяемыми алгоритмами асимметричной криптографии являются *RSA*, *ElGamal* и *ECC* (*Elliptic Curve Cryptography*). Однако существуют и альтернативные подходы, основанные на иных сложных математических проблемах.

Одним из таких перспективных направлений является криптография на основе кодов, или кодовая криптография. Её основное преимущество заключается в том, что она опирается на проблему декодирования произвольного линейного кода, которая является *NP*-трудной. Это означает, что даже с появлением квантовых компьютеров, которые угрожают взломать алгоритмы, основанные на факторизации больших чисел (*RSA*) или дискретном логарифмировании (*ElGamal, ECC*), алгоритмы на основе кодов останутся стойкими. Это делает их кандидатами в криптосистемы так называемого «постквантового» периода.

Целью данной лабораторной работы является теоретическое и практическое изучение одного из основополагающих алгоритмов в этой области — алгоритма Мак-Элиса. Данный алгоритм, разработанный Робертом Мак-Элисом в 1978 году, стал первой криптосистемой с открытым ключом, использующей теорию кодирования для обеспечения стойкости. Его безопасность базируется на сложности исправления ошибок в произвольных линейных кодах, а не на традиционных проблемах теории чисел.

# **1 ХОД РАБОТЫ**

В рамках выполнения лабораторной работы был реализован алгоритм асимметричного шифрования Мак-Элиса на языке *Python*. На первом этапе проведено изучение математических основ алгоритма, включая теоретические аспекты работы с линейными кодами, исправляющими ошибки. Особое внимание уделено структуре кода Гоппы, который составляет основу криптостойкости системы.

После освоения теоретического материала приступили к практической реализации. С использованием библиотеки *numpy* организована работа с бинарными матрицами и векторами над полем *GF(2)*. Реализована генерация ключевой пары: сначала создан закрытый ключ, состоящий из случайной перестановочной матрицы *P*, невырожденной матрицы *S* и матрицы проверки четности *H* для кода Гоппы. Открытый ключ вычислен как композиция этих матриц по формуле

Далее реализован процесс шифрования сообщения. Исходный текст преобразован в бинарный вектор, который умножается на матрицу открытого ключа. В полученный вектор добавлен ошибочный вектор малого веса, что является критически важным элементом алгоритма. Для дешифрования выполнена обратная перестановка шифротекста с последующим синдромным декодированием с использованием свойств кода Гоппы.

Начальные данные представлены на рисунке 1.1.



Рисунок 1.1 – Входные данные

Программа была запущена с случайно сгенерированным массивом ошибок и в результате появился зашифрованный текст, а после дешифрования был восстановлен исходный текст. Процесс работы программы представлен на рисунке 1.2.

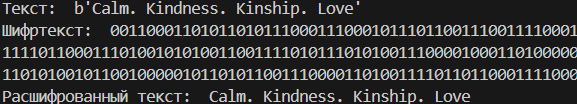


Рисунок 1.2 – Результат работы программы

# ЗАКЛЮЧЕНИЕ

В результате выполнения лабораторной работы был успешно реализован алгоритм асимметричного шифрования Мак-Элиса, основанный на теории кодов, исправляющих ошибки. Практическая реализация охватила все ключевые этапы алгоритма: генерацию пары ключей, процедуры шифрования и дешифрования сообщений, а также механизм работы с ошибками. Основным достижением работы стало создание работоспособной криптосистемы, наглядно демонстрирующей применение теории линейных кодов в криптографии.

Реализация подтвердила теоретические положения алгоритма, в частности, зависимость стойкости системы от сложности декодирования произвольного линейного кода. Особое значение имела корректная реализация механизма добавления и исправления ошибок, который является фундаментальным для безопасности схемы. Разработанный алгоритм продемонстрировал способность к восстановлению исходного сообщения даже при наличии преднамеренно внесенных искажений.

Практическая ценность работы заключается в создании инструмента для изучения перспективных направлений криптографии. Реализованная система может использоваться для демонстрации принципов работы криптографии, изучения свойств кодов Гоппы и понимания преимуществ постквантовых криптографических алгоритмов. В процессе реализации были приобретены навыки работы с бинарными матрицами, освоены методы синдромного декодирования и отработаны приемы работы в конечном поле *GF(2)*.

Перспективы развития работы включают оптимизацию алгоритмов для работы с большими параметрами системы, реализацию дополнительных режимов работы и исследование стойкости системы к различным типам криптоатак. Также представляет интерес сравнение эффективности алгоритма Мак-Элиса с другими постквантовыми криптосистемами.

Таким образом, реализованная криптосистема Мак-Элиса представляет собой законченное решение, которое демонстрирует принципы построения асимметричных алгоритмов на основе теории кодирования и служит основой для дальнейшего изучения перспективных направлений в области защиты информации.

# ПРИЛОЖЕНИЕ А (обязательное) Листинг программного кода

import random

import numpy as np

# Проверочная матрица

H = np.array([[1, 0, 1, 0, 1, 0, 1],

[0, 1, 1, 0, 0, 1, 1],

[0, 0, 0, 1, 1, 1, 1]])

# Матрица генерации

G = np.array([[1, 1, 0, 1],

[1, 0, 1, 1],

[1, 0, 0, 0],

[0, 1, 1, 1],

[0, 1, 0, 0],

[0, 0, 1, 0],

[0, 0, 0, 1]])

"""Эта матрица используется для декодирования закодированных сообщений.

Она позволяет извлечь исходные 4 бита из 7-битного закодированного сообщения."""

R = np.array([[0, 0, 1, 0, 0, 0, 0],

[0, 0, 0, 0, 1, 0, 0],

[0, 0, 0, 0, 0, 1, 0],

[0, 0, 0, 0, 0, 0, 1]])

def random\_binary\_non\_singular\_matrix(n):

a = np.random.randint(0, 2, size=(n, n))

while np.linalg.det(a) == 0:

a = np.random.randint(0, 2, size=(n, n))

return a

input\_file = "input.txt"

encrypt\_file = "encrypt.txt"

decoded\_file = "decoded.txt"

S = random\_binary\_non\_singular\_matrix(4)

S\_inv = np.linalg.inv(S).astype(int)

def generate\_permutation\_matrix(n):

i = np.eye(n)

p = np.random.permutation(i)

return p.astype(int)

P = generate\_permutation\_matrix(7)

P\_inv = np.linalg.inv(P).astype(int)

G\_hat = np.transpose(np.mod((S.dot(np.transpose(G))).dot(P), 2))

# Определяет позицию ошибки в закодированных данных.

def detect\_error(err\_enc\_bits):

err\_idx\_vec = np.mod(H.dot(err\_enc\_bits), 2)

err\_idx\_vec = err\_idx\_vec[::-1]

err\_idx = int(''.join(str(bit) for bit in err\_idx\_vec), 2)

return err\_idx - 1