Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Кафедра прикладної математики

**КУРСОВА РОБОТА**

з дисципліни «Програмування»

на тему:

Шифрування та дешифрування тексту

Виконав:

студент І курсу групи КМ-03,

спеціальність 113

Прикладна математика

ПЕРЕДЕРЕЙ БОГДАН.

Керівник:

ЛЮБАШЕНКО Н.Д.

Оцінка: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кількість балів: \_\_\_\_

Київ - 2021

ЗМІСТ

**Элементы оглавления не найдены.**

ВСТУП

# ПОСТАНОВКА ЗАДАЧІ

У даній курсовій роботі необхідно розробити програму для шифрування та дешифрування тексту за допомогою симетричного алгоритму блочного шифрування AES(Advanced Encryption Standar) з розміром ключа шифрування 128 біт.

Програма, повинна відповідати наступним критеріям:

* Програмний код написаний на мові програмування С із дотриманням стандарту форматування коду CS50.
* Ввід тексту для шифрування та дешифрування повинен відбуватися за допомогою текстових файлів
* Програма повинна заносити послідовність своїх операцій у журнал (log-файл). Кожен запис у журналі повинен містити час, рівень логування (FATAL, ERROR, WARN, INFO, DEBUG) та довільний текст операції. Рівень глибини логування повинен задаватись із конфігураційного \*.ini файлу програми.
* Програма повинна вміти поводитись із нестандартними ситуаціями (відсутній файл із вхідними даними, некоректні команди користувача, тощо).
* Програмний код програми повинен бути зрозумілим. Необхідно забезпечити легкість підтримки програмного коду в майбутньому.
* Для забезпечення стабільності поведінки програми у майбутньому — необхідно реалізувати покриття програмного коду Unit-тестами мінімум на 60%.
* Для забезпечення стабільності програми під навантаженням — повинне бути проведене навантажувальне тестування основного алгоритму.

Додатково у програмі повинне бути реалізоване наступне:

* Програма повинна мати можливість бути запущеною із командного рядка з метою вводу самого ключа, також повинна бути можливість перегляду документації про саму систему шифрування та про параметри, які може обирати користувач. Перегляд цієї інформації здійснюється за допомогою команди /help.
* Основний алгоритм програми повинен бути реалізований у проміжній динамічній бібліотеці, яку можна використовувати у мові програмування Python.