Дипломна робота на тему

«Розробка програмного забезпечення для захисту текстових файлів»

Виконав: студент групи КІ-14сп Зіменко Є.Ф.
Керівник: к.т.н., доцент кафедри ОТ Гороховський О.І.

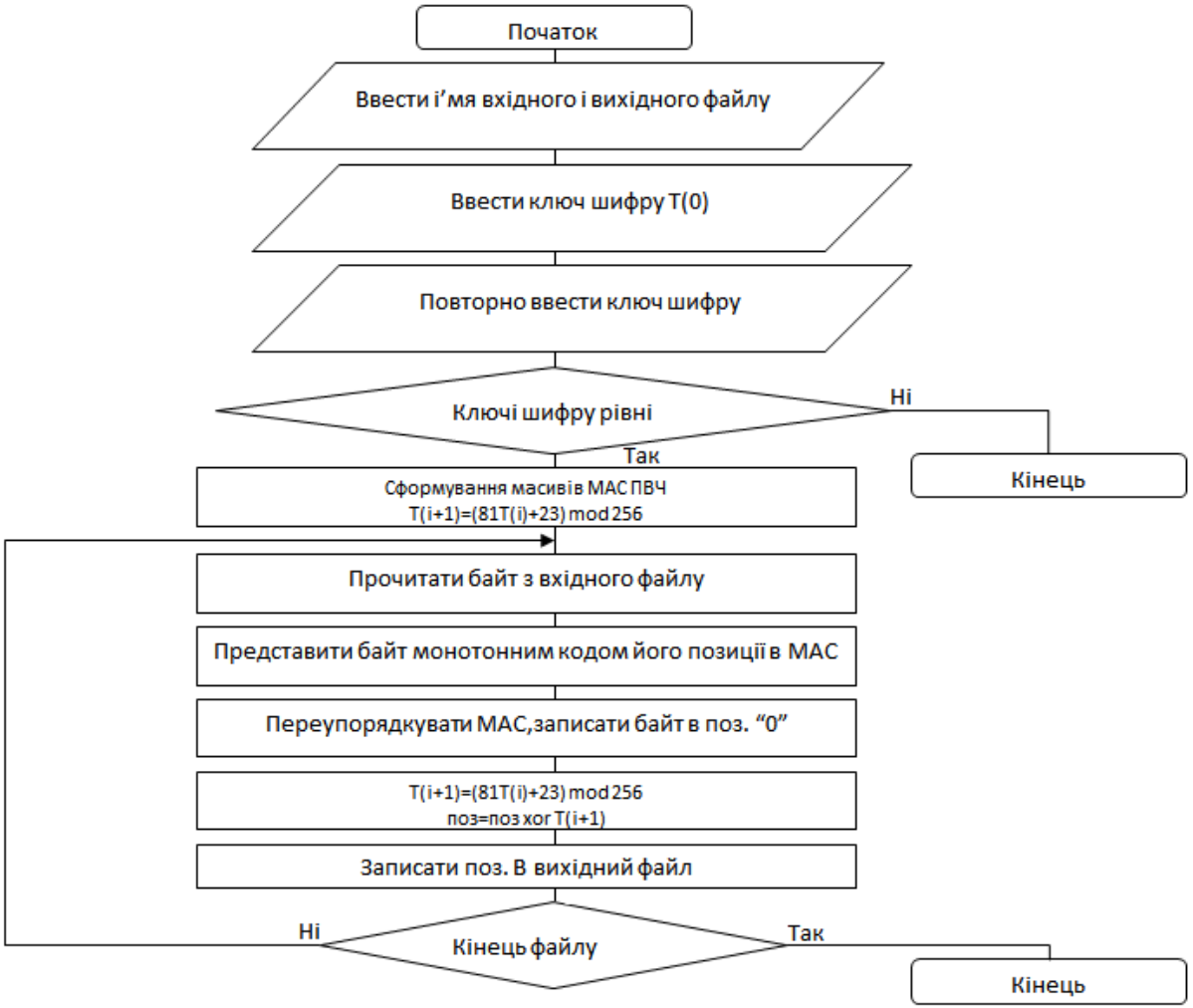
Завдання досліджень

- Проаналізувати основні алгоритми шифрування даних.
- Розробити алгоритми криптографічного шифрування даних.
- Обґрунтувати вибір мови програмування для реалізації розроблених алгоритмів і інтерфейсу.
- Розробити програмні модулі, які реалізують процеси шифрування і дешифрування різноманітних файлів.
- Проаналізувати криптостійкість розроблених алгоритмів.

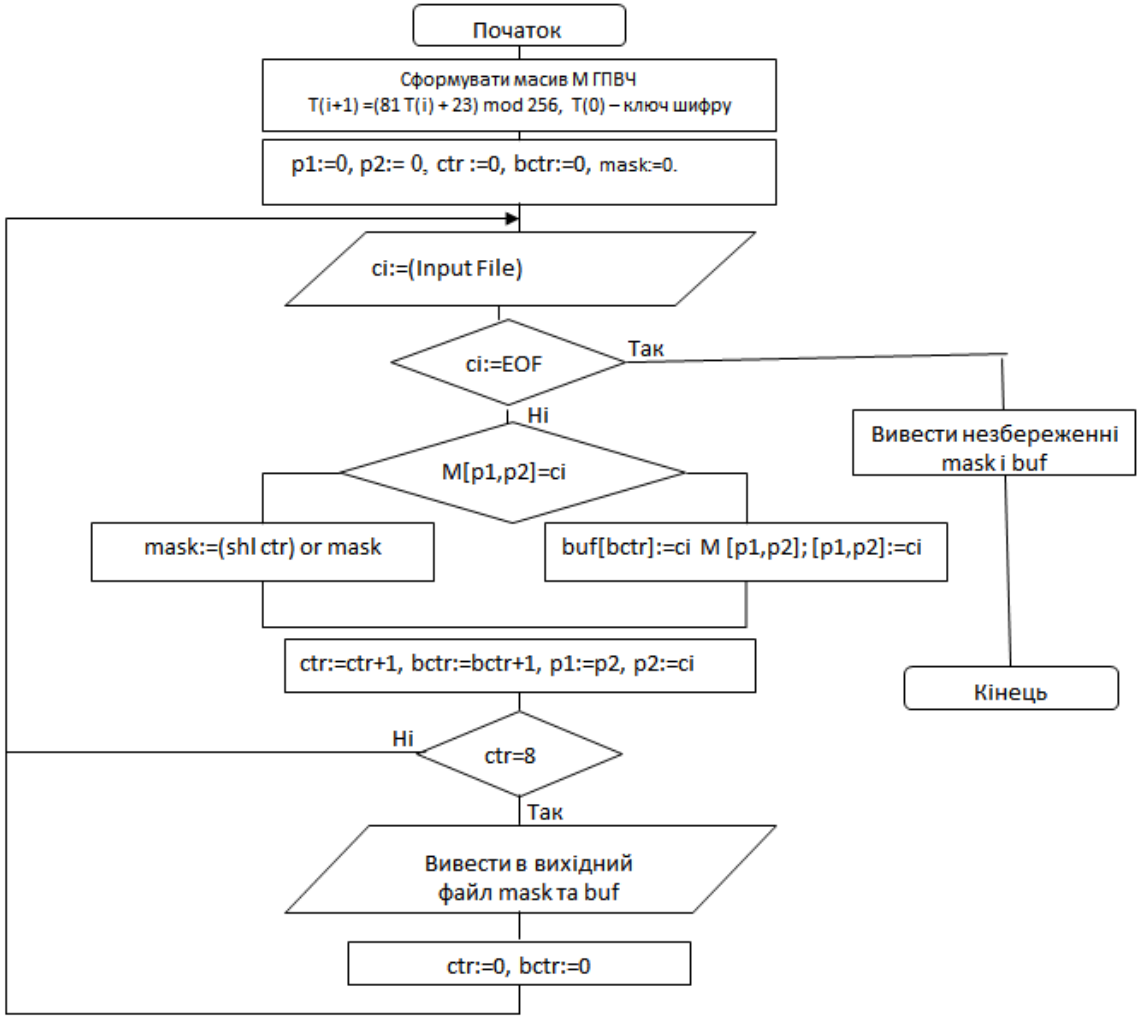
Характеристики методів шифрування

Метод	Коефіцієнт ущільнення	Обчислювальні затрати	Адаптивний	Додаткові Обчислювальні затрати для шифрування
Словниковий	Близький до оптимального для великих масивів	Середні	Так	Так
Хаффмана	Оптимальний	Середні	Ні	Так
MTF	Близький до оптимального	Середні	Так	Ні
Імовірнісний	Близький до оптимального	Малі	Так	Ні
Арифметич-ний	Найбільший	Великі	Так	Так

Алгоритм шифрування на основі методу MTF



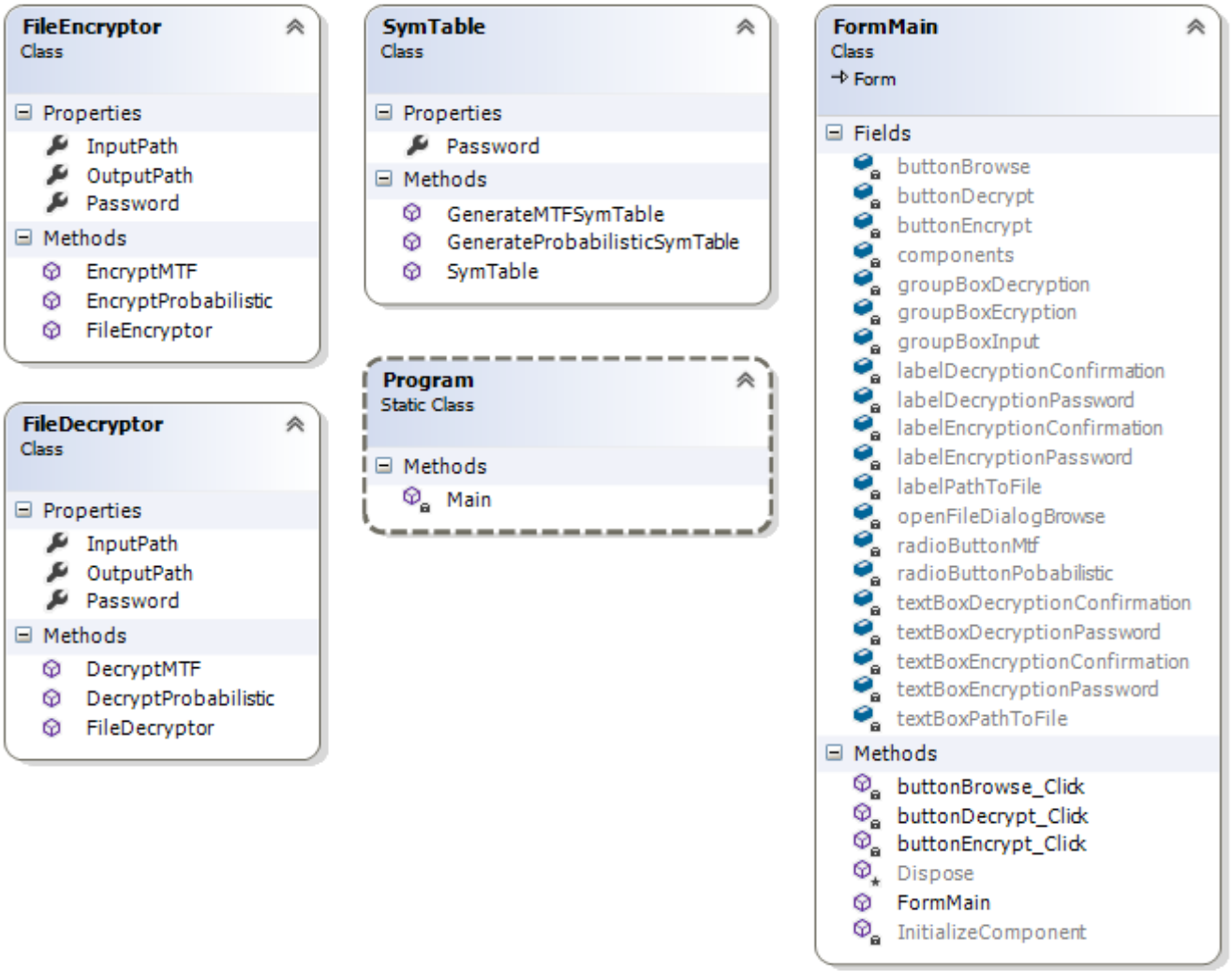
Алгоритм шифрування на основі імовірнісного методу



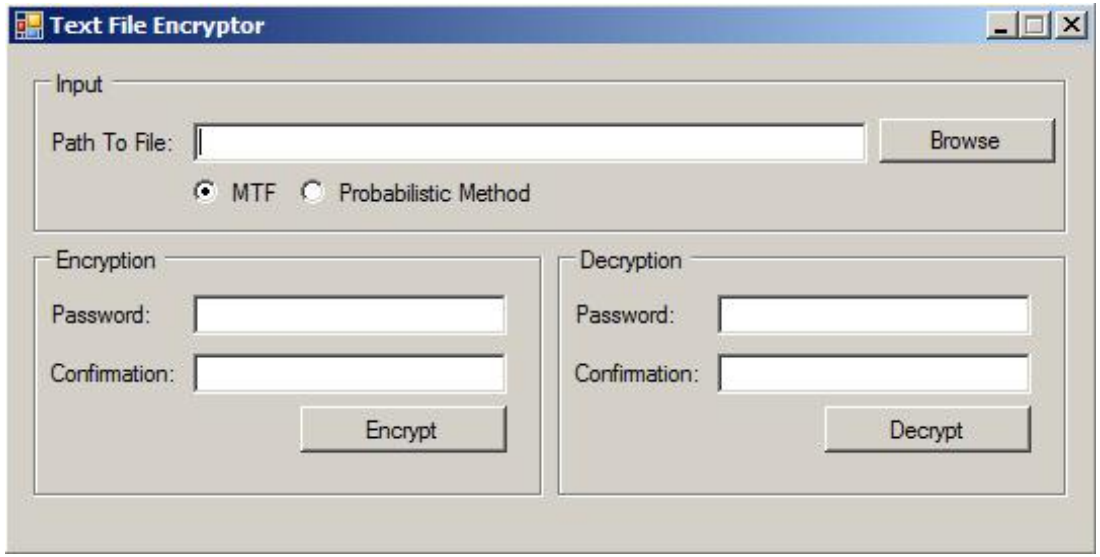
Критерії вибору мови програмування

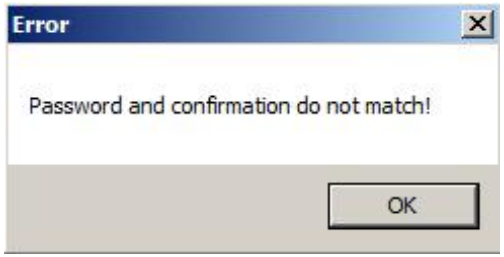
- Можливість автоматизованої розробки інтерфейсу користувача.
- Простота програмної реалізації складних обчислень.
- Наявність вбудованої бібліотеки класів/функцій.
- Дружнє середовище розробки програмного забезпечення.

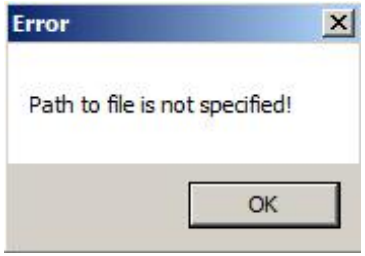
Класова діаграма



Інтерфейс програми







Аналіз криптостійкості шифрування

Оцінимо нижню оцінку складності дешифрування повідомлення для ідеального алгоритму:

$$D = \frac{c}{v}$$

де c - кількість ключів;

v - швидкодія комп'ютера.

Тактова частота потужного комп'ютера перевищує уже 2 ГГц, а кількість ключів для розглянутого алгоритму складає 2160, отже нижня оцінка складності дешифрування дорівнює:

$$D = \frac{2^{160}}{2 \cdot 10^{9}} = 0{,}73 \cdot 10^{39} (c^{-1}).$$

Щоб обчислити приблизний час, за який відбудеться дешифрування алгоритму методом простого перебору, необхідно найти відношення нижньої оцінки складності дешифрування до кількості секунд в році, тобто 315360000 секунд:

$$t_{СЕР} = \frac{D}{315360000} = \frac{0{,}73 \cdot 10^{39}}{315360000} = 23 \cdot 10^{30} \text{ років}$$

ДЯКУЮ ЗА УВАГУ