МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ПОЛІТЕХНІЧНИЙ УНІВЕРСИТЕТ

ІНСТИТУТ КОМП'ЮТЕРНИХ СИСТЕМ

МАТЕРІАЛИ ДЕВ'ЯТОЇ МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ СТУДЕНТІВ ТА МОЛОДИХ ВЧЕНИХ

присвячена 55-річчю
ІНСТИТУТУ КОМП'ЮТЕРНИХ СИСТЕМ

" Сучасні інформаційні технології 2019 "

" Modern Information Technology 2019 "

23-24 травня

Одеса
«Екологія»
2019

УДК 004.056.55

АНАЛІЗ РОБОТИ АЛГОРИТМІВ ШИФРУВАННЯ СТИСНУТИХ ДАНИХ

Жизнєв Д.І., к.т.н., доц. Шибаєва Н.О.
Одеський національний політехнічний університет, УКРАЇНА

АНОТАЦІЯ. В статті описаний варіант вирішення проблеми вибору алгоритму шифрування стиснутих даних шляхом розробки відповідного програмного модулю. Запропоновано спосіб розробки прикладної програми та коротко описані перспективи її розвитку.

Вступ. Шифрування даних – один із методів надійного захисту інформації від зловмисників. На сьогоднішній день була розроблена велика кількість алгоритмів шифрування, тому для вирішення конкретної задачі можуть бути використані одразу декілька з них. Логічно було б знайти такий алгоритм або їх набір, який продемонструє найкращий результат за декількома показниками та який міг би стискати текстові дані. Вирішенням цієї проблеми може стати невелика прикладна програма, яка порівнює роботу обраних алгоритмів.

Мета роботи. Метою є створення програмного модулю для аналізу та порівняння роботи (за декількома показниками) алгоритмів шифрування стиснутих даних.

Основна частина роботи. Застосування криптографії допомагає ефективно вирішити проблему захисту інформації під час користування інтернетом, діловому листуванні, фінансових операцій. Найбільш поширеними криптографічними засобами, що надають такий захист, є шифрування, цифровий підпис та аутентифікація користувача на основі паролю.

З плином часу електрона комерція, ділова активність і сфера дистанційних послуг ускладнюються, пред'являючи до систем захисту даних все більш високі вимоги: підвищена швидкодія роботи алгоритму та передачі даних, мінімальна затрата ресурсів пам'яті, високий опір до атак і т.п [1].

Для реалізації програмного модулю необхідно враховувати можливість його використання на різних операційних системах, так як алгоритми стискання працюють в різних файлових системах по різному, та роботу з різним об'ємом даних. Для вирішення першої проблеми була обрана мова високого рівня C++ та кросплатформений фреймворк QT версії 5.10.

Даний фреймворк дозволяє розробляти програмне забезпечення будь-якого рівня складності для UNIX-подібних систем та Windows. Також перевагою QT є можливість автоматичної очистки виділеної пам'яті вбудованими засобами розробки. Для вирішення другої проблеми кодування символів буде здійснюватися за допомогою UTF-16, що буде розбивати блоки вхідних слів не на 64 біти, а на 128.

У зв'язку з різною внутрішньою реалізацією, для порівняння потрібно обрати симетричний та асиметричний алгоритм шифрування, а проводити аналіз за швидкодією, кількістю використаної пам'яті та вихідною інформацією.

Алгоритм DES – найбільш використовуваний алгоритм симетричного шифрування даних, що був розроблений компанією IBM у 1977 році та має розмір блоку довжиною 64 біти для 8-бітного кодування ASCII. Таким чином, вихідне повідомлення розбивається на 8 блоків по 8 символів в кожному, але у зв'язку з тим, що зараз використовується 16-бітне кодування Юнікоду (UTF-16) для збереження довжини блоку в 8 символів потрібно збільшити розмір блоку до 128 біт.

Алгоритм працює в режимі електронної цифрової книги *(electronic code book),* що реалізується простою заміною та з використанням Сітки Фейстеля в прямому (для шифрування) і в зворотньому (для дешифрування) перетворенні даних.

SHA-1 яскравий приклад криптографічного алгоритму хешування даних, що на виході генерує 160-бітне хеш-значення. Використовує хеш-функцію, яка побудована на принципах функції стиснення. Функція приймає на вхід блок повідомлення в 512 біт та вихід (результат) з попереднього блоку. Хеш блоку M_i виглядає так:

$$h_i = f(M_i, h_{i-1}) \quad (1)$$

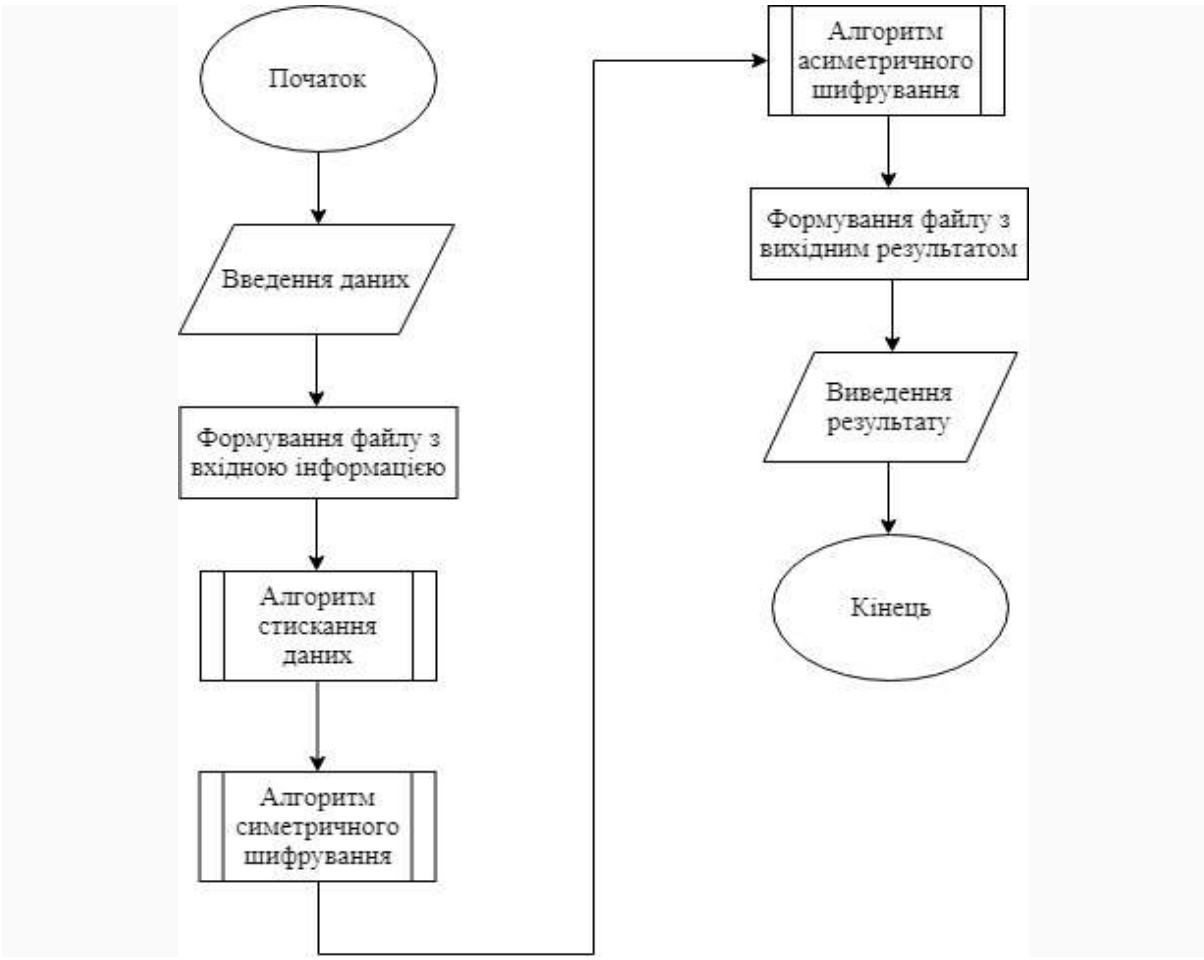

Рис. 1 – Блок-схема алгоритму роботи програмного модулю

З рисунку видно, що модуль має невеликий функціонал, що дає йому можливість бути впровадженим в якості додаткової функції в будь-якій системі для тесту швидкодії та ресурсів. При розширені потенціалу та функціоналу додатку, він може існувати в якості самостійного програмного забезпечення.

Висновки. Була освітлена проблема аналізу алгоритмів шифрування даних та запропоноване її вирішення – розробка відповідного програмного модулю. Програма дозволить наочно продемонструвати переваги та недоліки різних алгоритмів шифрування текстових даних для їх подальшого порівняння.

Великі за об’ємом дані повинні бути попередньо стиснуті для меншого використання ресурсів комп’ютера.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мао Венбо. Сучасна криптографія: Теорія та практика [Текст]: для професіоналів / Венбо Мао – Москва, СПб., Київ : Вільямс. 2005. – 27 с.