УДК 004.91

П. Я. Бондаренко[1]
М. М. Підгорний[1]

МОДИФІКАЦІЯ МЕТОДУ СИМЕТРИЧНОГО ШИФРУВАННЯ ДАНИХ

[1] Вінницький національний технічний університет

Анотація
Розглядається питання удосконалення симетричного методу шифрування цифрових даних.
Ключові слова: *шифрування даних, симетричний метод шифрування, криптографічний метод.*

Abstract
The issue of improving the symmetric method of digital data encryption is considered.
Keywords: data encryption, symmetric encryption method, cryptographic method.

Вступ

Швидкий розвиток технологій сучасного суспільства зумовив зростаючу потребу людей у захисті та збереженні цілісності цифрової інформації. Тому стає актуальною необхідність розробки ефективної методики шифрування даних, які можуть зберігатися на носіях або пересилатися через мережі.

Модифікація алгоритму шифрування Вермана

Для дослідження роботи механізму симетричного шифрування було створено програму на мові програмування C++ у середовищі Visual Studio 2019. У програмі використовується модель алгоритму шифрування Вернама, яка модифікована трьома механізмами:

створення ключа з двох частин – випадкової та заданої користувачем. Так, як будь-який генератор випадкових чисел працює на математичній моделі і всі числа насправді є псевдовипадковими, виникає ризик передбачення цифрового ключа. При використані частини ключа від користувача суттєво підвищується надійність та стійкість ключа. Випадкова частина змінюється кожен раз після використання ключа;

додаткова генерація ключа для ключа – тобто генерація ключа завдяки якому кодується основний ключ, який передається. Шифрування можливе будь-яким методом;

створення «шкідливої» інформації, яка потрібна для збільшення обсягу інформації. Якщо дешифратор не знає метод видалення «шкідливого» сміття, то дешифрувати інформацію неможливо. Доцільно використовувати цей механізм, якщо дискретність та безпека важливіша, ніж швидкість передачі інформації або обсяг збереження на носії.

На рисунку 1 зображено шифрування з ключем, який складається з двох частин.

На рисунку 2 зображено шифрування з ключем, який складається з двох частин та з механізмом вставки «шкідливої» інформації.

На рисунку 3 зображено шифрування з ключем, який складається з двох частин, з механізмом вставки «шкідливої» інформації та з механізмом подвійного ключа.

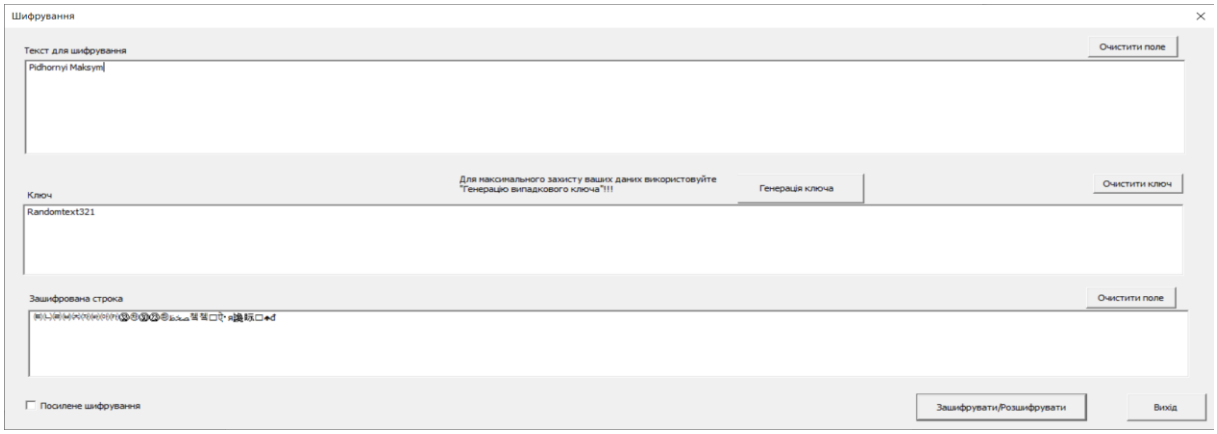

Рисунок 1 – шифрування ключем з двох частин

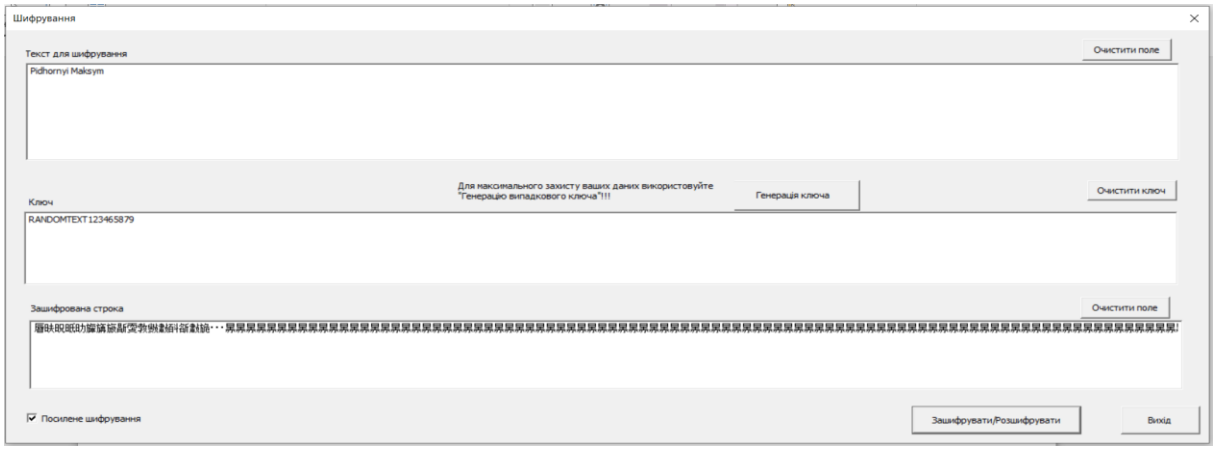

Рисунок 2 – шифрування ключем з двох частин та посиленням зайвою інформацією

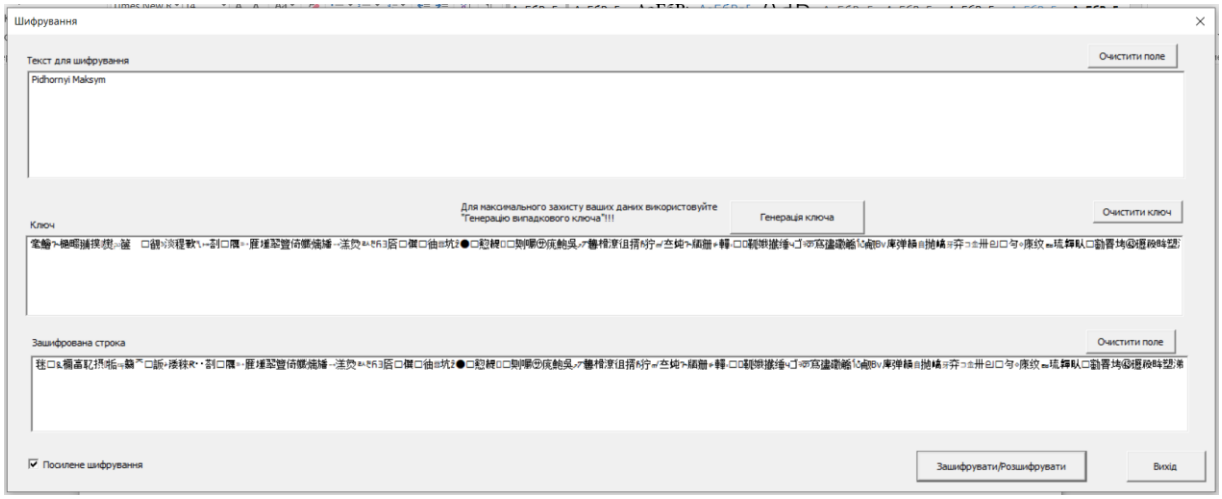

Рисунок 3 – шифрування ключем з двох частин, посиленням зайвою інформацією та подвійним ключем

Висновки

Модифікація моделі алгоритму шифрування Вермана вищеописаними механізмами у їх поєднанні дає змогу значно підвищити ступінь захисту інформації, що передається каналами зв’язку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Windows API. URL: https://uk.wikipedia.org/wiki/Windows_API.
2. URL: https://vc.ru/hr/50161-pochemu-c-krut-aktualen-i-bessmerten.
3. Вибір платформи для додатків Windows URL: https://docs.microsoft.com/ru-ru/windows/apps/desktop/choose-your-platform.
4. Литвиненко Н.А. Технологія програмування на С ++. Win32 API-додатки. - СПб .: БХВ-Петербург, 2010. - 288 с .: іл. - (Навчальний посібник).
5. Рисований О.М. Системне програмування [Текст]: підручник для студентів напрямку "Компютерна інженерія" Вищих Навчальних Закладів в 2-х томах. Том 2. – Видання четверте: виправлено та доповнено - Х .: "Слово", 2015. - 378 с.

Бондаренко Павло Якович – викладач кафедри військової підготовки, Вінницький національний технічний університет, м. Вінниця, e-mail: pavlobondarenko1970@gmail.com

Підгорний Максим Максимович, слухач кафедри військової підготовки, навчальна група 06-21, Вінницький національний технічний університет, м. Вінниця, e-mail: maksonpatiphone@gmail.com

Bondarenko Pavlo – Lecturer of the Department of Military Training, Vinnytsia National Technical University, Vinntsia, e-mail: pavlobondarenko1970@gmail.com

Pidgorniy Maksim Maksimovich, student, Department of Military Training, study group 06-21, Vinnytsia National Technical University, Vinnytsia, e-mail: maksonpatiphone@gmail.com