УДК 004.056.53

М.М. Маркевич
В.С. Катаєв

РОЗРОБКА ЗАСТОСУНКУ ДЛЯ АНАЛІЗУ МЕТОДУ ШИФРУВАННЯ ЦЕЗАРЯ З КЛЮЧОВИМ СЛОВОМ

Вінницький національний технічний університет

Анотація

У даній роботі розроблено застосунок для аналізу методу шифрування Цезаря з ключовим словом. Проаналізовано принцип роботи даного методу та проілюстровано алгоритм роботи шифрування. Також детально описано принципи зашифрування та розшифрування повідомлень даного методу шифрування. Висвітлено переваги методу шифрування Цезаря з ключовим словом над іншими методами шифрування.

Ключові слова: шифр, захист даних, система, ключове слово, зсув.

Abstract

This work develops an application for analyzing the Caesar key cipher method. The principle of operation of the Caesar key cipher method is explained and the encryption algorithm is illustrated. The principles of message encryption and decryption of this encryption method are also described in detail. The advantages of the Caesar key cipher method over other encryption methods are highlighted..

Keywords: cipher, data protection, system, keyword, offset.

Вступ

Шифрування завжди відігравало важливу роль у захисті інформації, починаючи ще з давніх часів. У різні історичні періоди людство шукало способи зберегти свої знання, таємниці. Одним із найпростіших і водночас найвідоміших методів є шифр Цезаря — класичний спосіб заміни літер, що забезпечує базовий рівень конфіденційності та цілісності переданої інформації. У сучасному цифровому світі, де інформація є надзвичайно цінним ресурсом, шифрування залишається ключовим інструментом захисту. Особливо це актуально з огляду на стрімкий розвиток технологій, коли програмування стало невід'ємною частиною нашого повсякденного життя. Інформаційні системи активно використовуються в освіті, медицині, фінансах, розвагах та інших галузях, де надійність збереження даних має першочергове значення. Саме тому розуміння та застосування шифрування є важливою складовою сучасної кібербезпеки.

Результати дослідження

Програми для шифрування, зокрема шифрування Цезаря з ключовим словом забезпечують захист від незаконного доступу до даних [1]. Даний метод є простим у реалізації, тому його легко опанувати людям різної професії, що робить цей шифр універсальним та зручним у використанні. Програмний застосунок "Шифрування Цезаря з ключовим словом"– це додаток, який реалізовує кодування у двох режимах роботи – зашифрування та розшифрування за допомогою шифру Цезаря. Принцип роботи полягає у зміні літер алфавіту на певну кількість позицій та накладанні ключового слова на текст, що ускладнює рівень кодування та підвищує захист повідомлень користувачів. Головна мета застосунку – здійснювати кодування інформації та захищати дані від несанкціонованого доступу.

Система шифрування Цезаря із ключовим словом є одноалфавітною системою підстановки [2]. Особливістю цієї системи є використання ключового слова для зсуву й зміни порядку символів в алфавіті підстановки. Безсумнівною перевагою даного методу є те, що кількість можливих ключових слів практично невичерпна. Алгоритм даного шифрування має однаковий вигляд для функцій зашифрування/розшифрування (рис.1). Побудова схеми починається з введення даних: вхідного тексту, ключа (слово), зсуву. Далі відбувається ініціалізація введених значень. Проводиться перевірка, чи є літери в алфавіті, якщо є далі обчислюється їх індекс, якщо ж ні – залишається незмінними. Процес шифрування продовжується для всіх символів повідомлення, що залишилися.

Після цього відбувається аналіз характеру зсуву, який було застосовано до тексту. Результат шифрування включає змінені символи відповідно до заданого алгоритму разом із тими, що не підлягали зміні. У підсумку формується зашифроване повідомлення, яке зберігає структуру оригінального тексту, проте захищене від прямого прочитання.

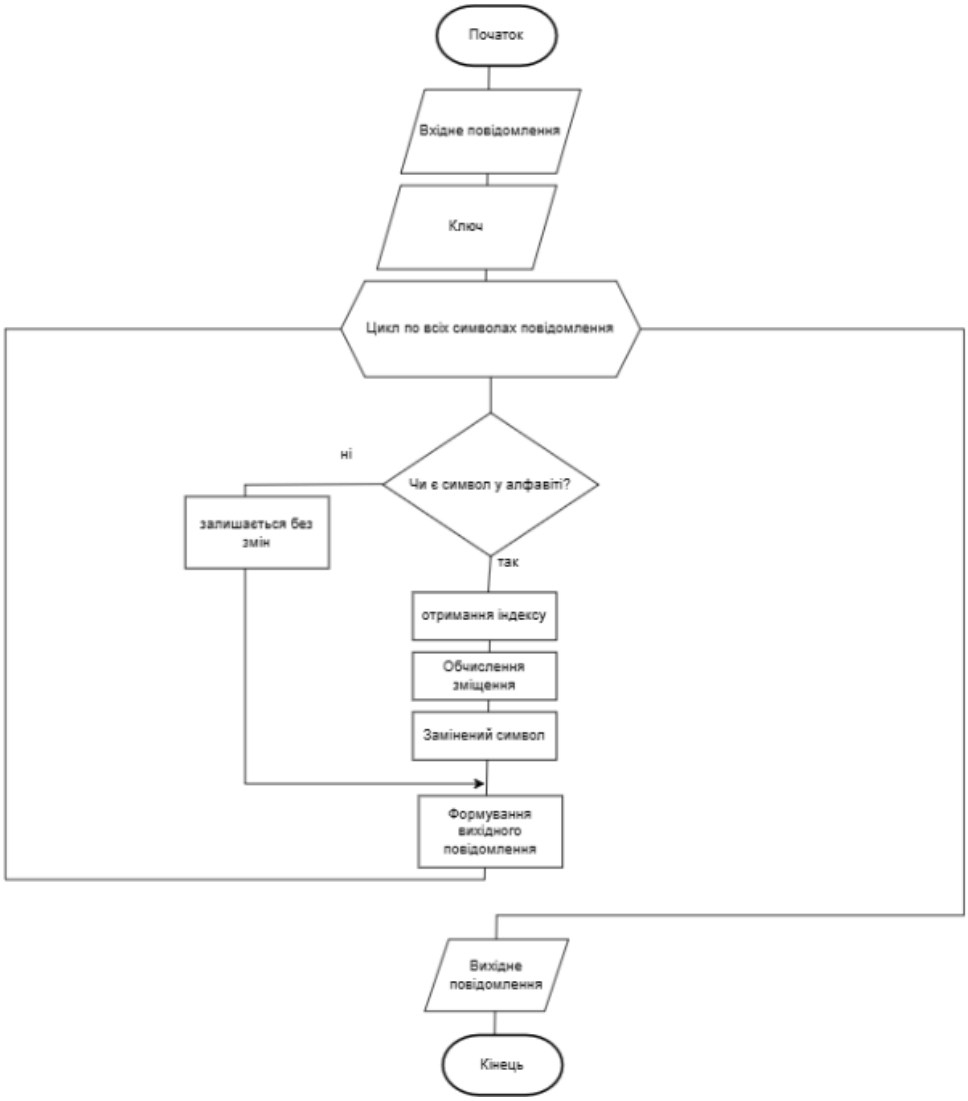

Рисунок 1 - Алгоритм роботи методу шифрування Цезаря з ключовим словом

Висновки

Отже, шифр Цезаря з використанням ключового слова належить до найпростіших методів шифрування, але дане шифрування здатне забезпечити елементарний рівень захисту інформації. Завдяки своїй доступності та зрозумілості, цей метод залишається актуальним не лише з історичної точки зору, але й як основа для вивчення більш складних криптографічних алгоритмів. Використання ключового слова підвищує стійкість шифру до дешифрування шляхом збільшення кількості можливих варіантів зсуву.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
2. Основні поняття та положення комп’ютерної криптографії. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://dspace.wunu.edu.ua/bitstream/316497/8109/1/%D0%BE%D0%BF%D0%BE%D1%80%D0%BD%D0%B8%D0%B9%20%D0%BA%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9.pdf (дата доступу 10.11.2024)

Маркевич Мар'яна Михайлівна – студентка групи 1БКС-23б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: 7mariaanaa@gmail.com

Науковий керівник: ***Катаєв Віталій Сергійович*** – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: kataev@vntu.net

Markevych Mariana Mykhailivna – student of group 1BKS-23b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: 7mariaanaa@gmail.com

Supervisor: ***Vitalii Kataiev*** – assistant of the Department of Management and Security of Information Systems; Vinnytsia National Technical University , Vinnytsia, e-mail: kataev@vntu.net