Автор:
Жук Артем Владиславович
студент 11 КНм групи
Науковий керівник:
Франчук Василь Михайлович,
доктор педагогічних наук, доцент
завідувач кафедри комп'ютерної та програмної інженерії

ВЕБ-ОРІЄНТОВАНИЙ ПРОГРАМНИЙ ЗАСІБ ДЛЯ ПОЛІАЛФАВІТНОГО ШИФРУВАННЯ ТЕКСТОВИХ ПОВІДОМЛЕНЬ

Анотація. Метою дослідження є розробка та створення веб-орієнтованої системи шифрування текстових повідомлення, з можливістю покроково розглядати етапи шифрування тим чи іншим методом. Завданням дослідження є створення веб-орієнтованої системи для покрокової демонстрації методів шифрування з освітньою метою. Об'єктом дослідження є веб-орієнтована система для демонстрації та вивчення методів поліалфавітного шифрування тексту, предметом дослідження є викладання навчальних матеріалів з використанням веб-орієнтованої системи для демонстрації методів шифрування. У дослідженні використано методи поліалфавітного шифрування: метод Цезаря, метод Віженера, метод Тритеміуса. Результатом дослідження є веб-орієнтована система для покрокової демонстрації методів шифрування з освітньою метою.

Ключові слова: система шифрування, метод Цезаря, метод Віженера, метод Тритеміуса.

Вступ. В умовах дистанційного навчання й регулярних відключень світла зростає попит на веб-орієнтовані програмні застосунки, за допомогою яких можна наглядно пояснити та продемонструвати певні теми кожному студенту, незалежно від того, в який час людина має змогу розпочати вивчення навчального матеріалу . Саме цю проблематику має частково спростити це дослідження. Наприклад, розглянемо таку тему, як метод поліалфавітного шифрування буквеного тексту (ширф Цезаря, шифр Віженера, шифр Тритеміуса). Процес навчання був би значно персоналізованнішим та більш мобільним, якби певна система покроково демонструвала процес шифрування (за тою чи іншою методологією) та зворотній процес – розшифрування. Шифрування використовується в усьому світі як окремими особами, так і великими організаціями для захисту важливих даних, які надсилаються від одного користувача до іншого, забезпечуючи надійне шифрування між клієнтом і сервером [1]. Методи шифрування можна розділити на симетричні та асиметричні. У шифруванні з симетричним або секретним ключем для шифрування та розшифрування даних використовується лише один ключ. В асиметричних системах використовуються два ключі; закритий і відкритий ключі. Відкритий ключ використовується для шифрування, а закритий ключ використовується для розшифрування [3, 4].

Постановка задачі. Алгоритми шифрування даних та методи шифрування вивчаються студентами ЗВО (закладів вищої освіти) в рамках курси «Основи кібербезпеки. Існує велика кількість методів шифрування, які відрізняються між собою криптостійкістю, алгоритмами, сферами використання.

Для того, щоб студенти могли більш детально розглянути різноманітні методи шифрування виникає необхідність у створенні системи, яка має продемонструвати процес шифрування та розшифрування. Методи шифрування допомогають запобіганню витоку, розкрадання, утрати, несанкціонованого знищення, перекручування, модифікації (підробки), несанкціонованого копіювання, блокування даних, тому тема шифрування є особливо актуальною для тих, хто планує працювати у сфері кібербезпеки. Кожен фахівець, який досконало буде розуміти різні типи шифрування, зможе розробити свої власні системи шифрування, щоб лише авторизовані користувачі мали доступ до даних [2].

Мета роботи. Метою дослідження є розробка та створення веб-орієнтованої системи шифрування текстових повідомлення, з можливістю покроково розглядати етапи шифрування тим чи іншим методом.

Основна частина. Для створення веб-орієнтованої системи шифрування текстових повідомлення з методів оптимізації були обрані наступні методи поліалфавітного шифрування: метод Цезаря, метод Віженера, метод Тритеміуса. Метод Цезаря – один із найпростіших методів для використання в криптографії і може забезпечити мінімальний захист даних. Метод Віженера – цей метод є простою формою багатоалфавітної заміни. Метод Тритеміуса – являє собою вдосконалений шифр Цезаря, тобто шифр підстановки.

Платформою для реалізації цієї ідеї було обрано веборієнтовану клієнт-серверну технологію, оскільки це дозволить зробити поточний освітній застосунок більш уніфікованим та доступним на будь-яких пристроях (Android, IOS, Windows, Mac OS, Android TV, webOS тощо). Це дозволить надавати відомості, щодо теми шифрування студентам з будь-яких пристроїв майже з будь-яким запасом потужності. Для написання програми було обрану мову програмування JavaScript, стандартизовану мову розмітки документів для перегляду веб-сторінок у браузері – HTML і спеціальну мову стилю сторінок CSS.

Висновки. Веб-орієнтованої система створюється з метою використання у навчальному процесі ЗВО для фахівців із кібербезпеки, інформаційних технологій. У перспективі планується вдосконалена розробка програми із використанням різноманітних методів шифрування, що надасть можливість використовувати її для вирішення завдань криптографії.

Список використаних джерел

1. Data Encryption: Types, Algorithms, Methods, and Techniques [Electronic resource] / eXpertise2Go.com. – 2012. – Mode of access : https://www.knowledgehut.com/blog/security/data-encryption
2. Types of Encryption: 5 Encryption Algorithms & How to Choose the Right One [Electronic resource] / thesslstore.com. – Mode of access : https://www.thesslstore.com/blog/types-of-encryption-encryption-algorithms-how-to-choose-the-right-one/
3. A Study of Encryption Algorithms AES, DES and RSA forSecurity [Electronic resource] / academia.edu. – 2013. – Mode of access : https://www.academia.edu/36827103/A_Study_of_Encryption_Algorithms.
4. Франчук В.М. Захист інформаційних ресурсів. Київ: Редакції газет природничо-математичного циклу, 2012. 112 с. (Бібліотека "Шкільного світу").