УДК 004.9

ДОСЛІДЖЕННЯ МЕТОДІВ ШИФРУВАННЯ ДАНИХ ТА РОЗРОБКА ПРОГРАМНИХ РІШЕНЬ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРИКЛАДІ ДОДАТКУ CRYPTSETUP

Р.М. Валентій*[1]*, *О.М. Нікуліна*[2]

[1] *магістрант кафедри інформаційних систем та технологій, НТУ «ХПІ», Харків, Україна*

majorik901@gmail.com

[2] *завідувачка кафедри інформаційних систем та технологій, д-р. техн. наук, НТУ «ХПІ», Харків, Україна*

Olena.Nikulina@khpi.edu.ua

У сучасному світі, де обробка і зберігання даних набувають все більшого значення, дослідження методів шифрування є важливим елементом забезпечення безпеки інформації. Використання ефективних алгоритмів шифрування допомагає захистити конфіденційні дані від несанкціонованого доступу та кіберзагроз. Недостатній захист інформації може призвести до значних ризиків через її втрату та небажані наслідки в разі використання цієї інформації противниками [1 – 3].

Основною метою цієї роботи був аналіз існуючих методів шифрування даних та розробка програмних рішень, що забезпечують їх ефективну реалізацію. Дослідження охоплює порівняння різних алгоритмів за критеріями безпеки, швидкості обробки та ресурсозатратності.

Актуальність даного проекту полягає в необхідності адаптації методів шифрування до нових викликів кібербезпеки. Розробка програмних рішень, які інтегрують перевірені методи шифрування, є критично важливою для захисту чутливої інформації в умовах сучасного інформаційного суспільства.

Важливим аспектом дослідження була розробка бекенд-додатку, який дозволяє ефективно тестувати різні функції шифрування. Це забезпечує можливість оцінювання їх продуктивності та надійності без необхідності створення інтерфейсу для користувача.

Розробка бекенд додатка, що тестує методи шифрування, є важливим етапом у дослідженні та впровадженні нових алгоритмів. Додаток надає можливості для:

1. Тестування алгоритмів шифрування – здатність оцінювати різні алгоритми (AES, RSA, Blowfish тощо) на основі їх продуктивності та безпеки.
2. Порівняння методів – визначення, який алгоритм є найбільш ефективним для конкретних умов (швидкість, обсяг даних, безпека).
3. Аналіз вразливостей – проведення тестів на вразливість.

У рамках проекту використовувались такі сучасні технології, такі як Node.js платформа для бекенду обумовлений його асинхронною природою, що дозволяє ефективно обробляти запити та зменшує затримки. Express.js популярний веб-фреймворк для Node.js, який забезпечує просту маршрутизацію та обробку запитів. Crypto модуль вбудований модуль Node.js, що надає алгоритми для шифрування, хешування та підпису даних. Програмне забезпечення дозволяє проводити тестування різних методів шифрування та оцінювати їхню ефективність у реальному часі.

Діаграма архітектури бекенд-додатку для тестування шифрування описана наступним чином:

1. Запит від користувача – користувач надсилає HTTP-запит до серверної частини додатку.

2. Back-end (Node.js/Express.js): сервер на Node.js з використанням Express.js отримує запит.

В залежності від маршруту (/test або /results), запит обробляється відповідним контролером.

3. Маршрути:

– /test: цей маршрут відповідає за тестування алгоритмів шифрування. Запит передається до логіки тестування.

– /results: цей маршрут використовується для отримання результатів тестування. Він повертає результати, збережені після виконання шифрувальних операцій.

4. Crypto модуль: ввикористовується для виконання шифрувальних операцій. Це може бути вбудований модуль Node.js або стороння бібліотека для шифрування.

5. Логіка тестування: реалізує алгоритми шифрування та їх порівняння. Вона виконує шифрувальні операції, використовуючи Crypto модуль, і зберігає результати для подальшого аналізу.

6. Результати: після обробки запиту результати шифрування повертаються користувачу у відповідь на запит.

Ця діаграма відображає потік даних від запиту користувача до отримання результатів, підкреслюючи роль кожного компонента рис. 1.

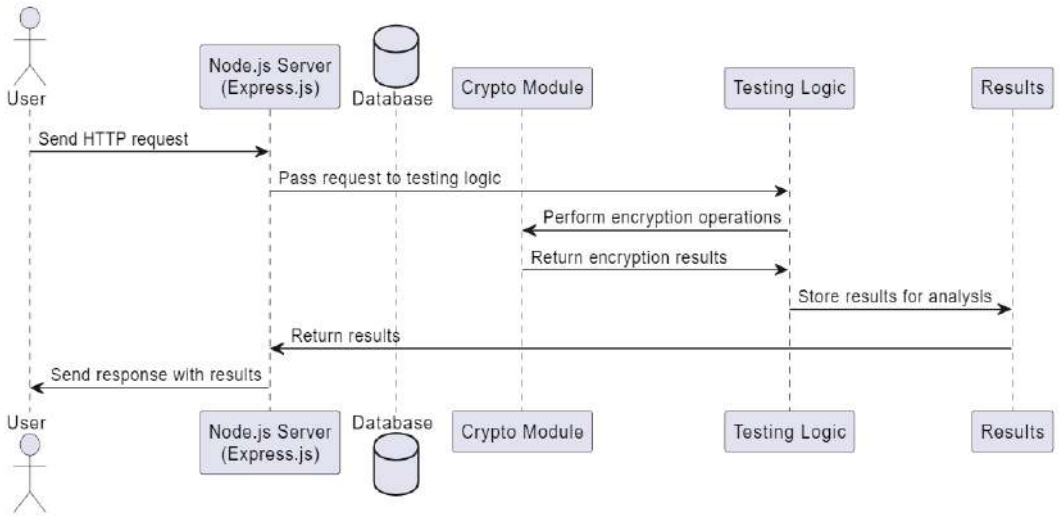

Рис.1 – Діаграма архітектури додатку

Таким чином, додаток для тестування методів шифрування є актуальним та важливим проектом, який відповідає сучасним вимогам безпеки. Він не тільки дозволяє досліджувати нові алгоритми, але й надає практичні інструменти для оцінки їх ефективності. Використання сучасного технологічного стеку гарантує гнучкість та продуктивність додатка, що робить його корисним інструментом для розробників і дослідників у сфері кібербезпеки.

Список літератури:

1. *Nieles, M. An* Introduction to Information Security. /*M. Nieles, K. Dempsey, V. Y. Pillitteri* // National Institute of Standards and Technology Special. – 2017. – 101 p.

2. Stallings, W. Computer Security : Principles and Practice. /*W. Stallings, L. Brown* // New Jork: Prentice Hall. – 2008. – 817 p.

3. *Нікуліна, О. М.* Дворівнева концепція для моделювання єдиної завадостійкої передачі цифрових даних /*О. М. Нікуліна, В.О. Шаров* // Харків: НТУ «ХПІ», 2024. – № 1 (11). – С. 70–75.