УДК 004.056.53

РОГАЧЕВСЬКИЙ Дмитро
КАПЛУН Валентина

ЗАХИСТ ФАЙЛІВ З ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ЦИФРОВОГО ПІДПИСУ (ЕЦП)

Вінницький національний технічний університет

Анотація. *В даній статті досліджено можливість використання електронно-цифрового підпису для захисту інформації, яка міститься у файлах. Дані, записані у файл захищаються шифруванням та створенням цифрового підпису, з додатковою можливістю перевірки автентичності файлу за допомогою згенерованого підпису.*

Ключові слова: *електронно-цифрового підпису, автентичності файлу.*

Abstract. *This article examines the possibility of using an electronic digital signature to protect information contained in files. The data written to the file is protected by encryption and the creation of a digital signature, with the additional possibility of verifying the authenticity of the file using the generated signature.*

Keywords: *electronic digital signature, file authenticity.*

Вступ

В епоху цифрових технологій, актуальність ЕЦП набирає великих обертів, тому що його використання має широкі перспективи впровадження у всіх сферах життя сучасного суспільства, пов’язаних із передачею та обробкою інформації. Документ, поданий у режимі онлайн і підписаний цим підписом, має таку саму юридичну силу, як і паперовий, підписаний власноруч. Такий підпис надійно захищений від підробок та дійсний на всій території країни.

В даній роботі для створення ЕЦП використано роботу з криптографічним алгоритмом RSA, застосовано хеш-функцію для перевірки цілісності файлу. Електронно-цифровий підпис файлу реалізується обчисленням хеш-функції над вмістом файлу, значення хеша шифрується алгоритмом RSA, зашифрована послідовність передається адресату.

Метою даної роботи є удосконалення захисту файлів шляхом розробки застосунку, який за допомогою використання ЕЦП забезпечує захищеність автентичності вмісту файла.

Результати дослідження

Існує кілька способів захисту файлів, які можна реалізувати за допомогою використання електронно-цифрового підпису (ЕЦП). Ось декілька способів захисту файлів з використанням ЕЦП:

- цифрове підписування: ЕЦП створюється за допомогою приватного ключа, а отримувач перевіряє підпис, використовуючи публічний ключ, це підтверджує, що файл не був змінений та походить від відправника;
- електронний архів: створення електронного архіву, що містить файли та їх ЕЦП, дозволяє отримувачу перевірити підписи, щоб переконатись, що файли не були змінені та мають походження від відправника;
- ЕЦП для електронної пошти: використання ЕЦП для повідомлень електронною поштою забезпечує автентифікацію відправника та гарантує автентичність даних;
- електронний документообіг: в організаціях, де використовується електронний документообіг, ЕЦП може бути використаний для підписування всіх електронних документів, що забезпечує автентичність та цілісність всього документообігу;
- електронні контракти: при укладанні електронних контрактів ЕЦП може бути використаний для підпису та підтвердження згоди сторін, що таким чином дозволяє створювати юридично обов’язкові електронні документи, які не можуть бути відхилені через спірність підпису.

Ідея запропонованого захисту полягає у тому, що цифровий підпису реалізується наступним чином: над вмістом файлу обчислюється хеш-функція, потім значення хеша шифрується алгоритмом RSA, після чого ця зашифрована послідовність передається також адресату. Адресат, отримавши файл та шифрування виконує наступні дії: обчислює над вмістом файлі значення хеш-функції; розшифровує алгоритмом RSA отримане шифрування, отримуючи таким чином значення переданого хеша відправником; порівнює значення обчисленого ним самим хеша з одержаним значення. У такому разі, якщо значення хешів збігаються, це означає, що файл автентичний та підпис вірний, у іншому випадку файл вважається не автентичним і відрізняється від того, який передавав відправник.

Даний захист файлів шляхом використання електронно-цифрового підпису (ЕЦП) реалізовано в програмному засобі мовою програмування C#, яка відома своєю універсальністю та високою масштабованістю при розробці програмного забезпечення. Алгоритм передбачає використання математичної моделі, яка містить у собі розширений алгоритм Евкліда.

Сутність розробленого захисту файлів шляхом використання ЕЦП полягає в наступному: забезпечити цілісність та автентичність даних, шляхом використання двох операцій: підписання файлу та перевірка підпису. При підписанні файлу, дані спочатку піддають хешуванню за допомогою хеш-функції, що створює унікальний хеш-код. Потім хеш-код шифрується за допомогою приватного ключа, створеного під час генерації ключів. Отриманий підпис приєднується до вихідних даних і зберігається. При перевірці підпису, отриманий підпис розшифровується за допомогою публічного ключа, який також був створений під час генерації ключів. З отриманого розшифрованого підпису витягується хеш-код, а потім самі дані також піддаються хешуванню. Отриманий хеш-код з вихідних даних порівнюється з розшифрованим хеш-кодом з підпису. Якщо вони збігаються, підпис вважається валідним.

Алгоритм роботи застосунку виглядає наступним чином (рис. 1). При запуску захищуваної програми користувача зустрічає головне вікно з елементами керування (рис. 2). Далі користувачеві необхідно вибрати шлях до файлу, який буде захищатись та шлях до файлу, у якому міститься ЕЦП. Після цього користувачеві необхідно ввести прості числа p та q у відповідні поля, натиснути кнопку "Підписати". У програмі також присутня можливість перевірки справжньості підпису. Для цього користувач вибирає відповідні шляхи до файлу та ЕЦП, вводить секретний ключ, який він отримав під час підпису. Якщо усе гаразд, програма виводить відповідну інформацію (рис. 3,а). В іншому випадку, якщо файл не відповідає первинному значенню, програма виводить діалогове вікно з відповідною помилкою (рис. 3,б).

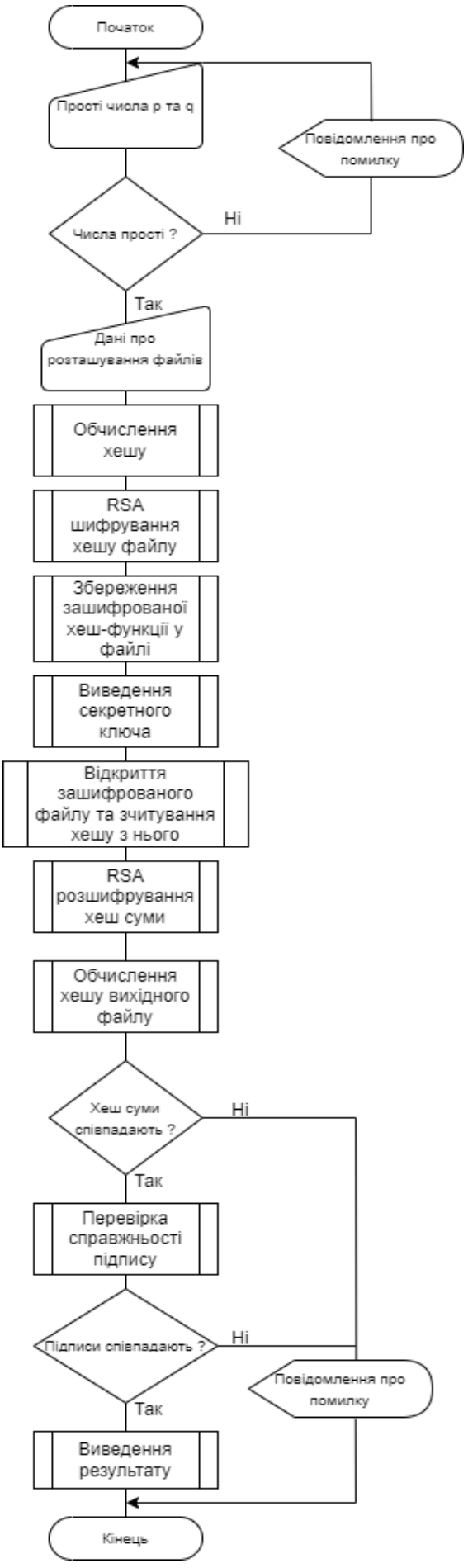


Рисунок 1 – Алгоритм захисту ПЗ

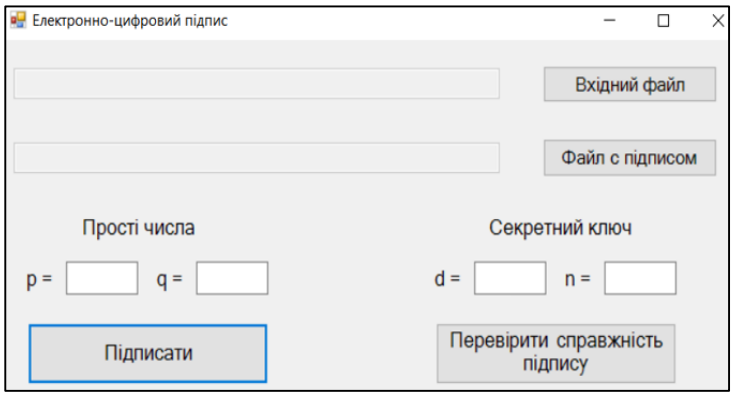
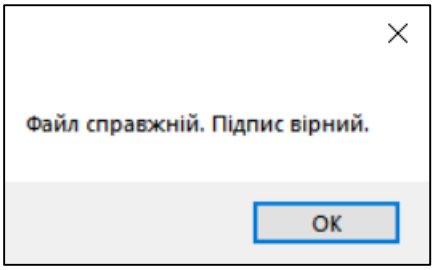


Рисунок 2 – Вигляд головного вікна програми

а)



б)

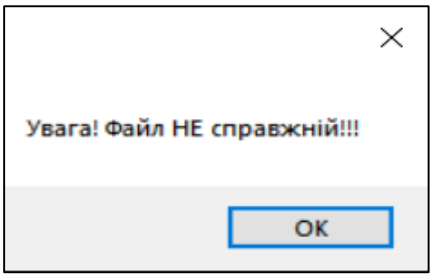


Рисунок 3 – Вигляд повідомлень при правильному (а) і неправильному (б) проходженні валідності підпису

Тестування розробки довело коректність роботи програмного застосунку і правильність роботи захисту файлів за допомогою використання електронно-цифрового підпису (ЕЦП).

Висновки

Даний підхід використовує алгоритм RSA, який є основою для розробки та використання електронно-цифрового підпису (ЕЦП). RSA використовує два ключі – приватний ключ для підписування документів та публічний ключ для перевірки підпису. Процес створення ЕЦП за допомогою RSA включає обчислення хеш-функції вхідного файлу, шифрування хешу за допомогою приватного ключа та додавання підпису до повідомлення. Перевірка ЕЦП здійснюється з використанням публічного ключа, де хеш вхідного повідомлення порівнюється з розшифрованим підписом, що дає змогу встановити автентичність та цілісність даних. RSA є одним з найбільш поширених алгоритмів для ЕЦП через свою ефективність та безпеку. Застосування алгоритму RSA для ЕЦП забезпечує надійність та довіру в цифровому середовищі, що робить його популярним в багатьох сферах, включаючи бізнес, фінанси та юриспруденцію. Ці висновки підкреслюють значимість алгоритму RSA для розробки та застосування ЕЦП з метою забезпечення безпеки та автентичності в електронному середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ЕЦП: особливості використання. : URL: https://pravokator.club/news/elektronnyj-tsyfrovyj-pidpys-osoblyvosti-vykorystannya/ (дата звернення: 31.05.2023).
2. RSA: від простих чисел до електронного підпису. : URL: https://habr.com/ru/post/534014/ (дата звернення: 31.05.2023).
3. Електронний підпис RSA. : URL: https://studfile.net/preview/7008661/page:6/ (дата звернення: 31.05.2023).
4. Алгоритм шифрування RSA. : URL: https://e-nigma.ru/stat/rsa/ (дата звернення: 31.05.2023).

РОГАЧЕВСЬКИЙ Дмитро – студент групи 1БС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: dimonrogach@gmail.com.
КАПЛУН Валентина, ст. викл. кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, valuka8379@gmail.com.

ROHACHEVSKYI D. - student of group 1BS-20b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.
KAPLUN V. – Lecturer of the Chair of Safety of Infomation and Communication Systems, VNTU, Vinnytsia.