ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

МАТЕРІАЛИ

міжнародної науково-практичної конференції молодих учених

«Проблеми та перспективи забезпечення цивільного захисту»

Харків – 2023

УДК 004.312.26

ПІДТВЕРДЖЕННЯ АВТЕНТИЧНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ЗА ДОПОМОГОЮ АЛГОРИТМУ ХЕШУВАННЯ SHA-1

Малярова Д.М., НУЦЗУ
НК – Маляров М.В., к.т.н, доц., НУЦЗУ

Через широке застосування комп'ютерних технологій, легкість доступу та збільшення обсягу інформації зростає інтерес і до криптографічних методів захисту інформації. Програмні засоби захисту інформації стають все більш розповсюдженими та використовуються у системах контролю і управління доступом, антивірусних програмах, шифрувальних програмних застосунках тощо [1].

Окрему нішу у криптографічних методах захисту інформації займають, так звані, хеш-функції [1], які використовуються для автентифікації, перевірки цілісності даних, захисту файлів тощо. Якщо основним завданням шифрування є захист інформації від сторонніх осіб, то у хеш-функцій інша задача. Вона, направлена на захист файлів та інформації від змін і підробок, запевняючи користувача, що інформація якою він користується ніде не зазнала змін (є автентичною) [2]. Існують різні алгоритми хешування даних, які відрізняються різною розрядністю, обчислювальною складністю та криптостійкістю. Більшість сучасних алгоритмів хешування базуються на основі вже перевірений старих, тому для більшого розуміння самої суті хешування використовують старі, більш спрощені алгоритми, наприклад, алгоритм хешування SHA-1 [2].

У роботі розглянуто алгоритм та програмну реалізацію криптографічного хешування SHA-1, що реалізує хеш-функцію, побудовану на ідеї функції стиснення. SHA-1 є найбільш широко використовуваним з існуючих хеш-функцій SHA, виробляє 160-бітний дайджест повідомлень і використовується в декількох широко розповсюджених програмах безпеки та протоколах.

Проведені дослідження підтвердили присутність лавинного ефекту, котрий проявляється у повній зміні вихідного повідомлення при, навіть, незначних змінах (додатковий пробіл або прописна буква замість строкової) у вхідному повідомленні. Також, було визначено, що будь-яке повідомлення (навіть порожній рядок) має свій дайджест. Практична реалізація алгоритму підтвердила слабку залежність часу формування хеш дайджесту від довжини повідомлення. При коливаннях розміру вхідного повідомлення до 56 символів, час формування хеш дайджесту коливається у межах 1-2 мс.

Зрозуміло, методи та сфери застосування хешування не обмежуються перерахованими. Також як і алгоритми хешування не обмежуються тільки алгоритмом SHA-1. Але наведена реалізація дає змогу зрозуміти саму основу знаходження хеш-функцій та використовувати її як базу при подальших дослідженнях та програмних розробках.

ЛІТЕРАТУРА

1. Швачич Г.Г., Толстой В.В., Петречук Л.М., Іващенко Ю.С., Гуляєва О.А., Соболенко О.В. Сучасні інформаційно-комунікаційні технології: Навчальний посібник. Дніпро. 2017. 230 с.
2. Глинчук Л.Я. Криптологія: навч.-метод. посіб. Луцьк. 2014. 164 с.