

**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

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 підрбок, 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 перевірених 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.

Овчинников О.П., ЧПБ ім. Героїв Чорнобиля НУЦЗУ Аспекти попередження ураження електричним струмом під час гасіння пожеж та ліквідації надзвичайних ситуацій.....	240
Кривошеєва К.А., НУЦЗУ Можливості використання 3D моделювання при підготовці фахівців ДСНС.....	241
Лазарак Р.В., ЛДУБЖД Обґрунтування параметрів надійності функціонування автоматичних систем водяного пожежогасіння з частотнокерованим автономним джерелом електроенергії.....	242
Лисенко О.С., НУЦЗУ Застосування програмного продукту ABAQUS.....	243
Малярова Д.М., НУЦЗУ Підтвердження автентичності електронних документів за допомогою алгоритму хешування SHA-1.....	244
Мирошниченко А.О., НУЦЗУ Дослідження методів та моделей захисту піротехників в зоні надзвичайної ситуації внаслідок вибуху на об'єктах критичної інфраструктури.....	245
Оленич М.О., НУЦЗУ Математичний опис оцінки межі автоколивань автоматичної системи протипожежного захисту.....	246
Павлюк Д.І., НУЦЗУ Технічне обслуговування та регламентні роботи телекомунікаційних систем та інформаційних технологій.....	247
Перебийніс К.С., ЧПБ ім. Героїв Чорнобиля НУЦЗУ Аналіз систем автоматизованого проектування (CAD) для виконання функцій проектування в інформаційних технологіях.....	248
Пономарьов К.А., НУЦЗУ Розробка засобів для автоматизації роботи інженера-проектувальника у галузі забезпечення пожежної безпеки об'єктів.....	249
Радул А.Ю., НУЦЗУ Застосування ємкісного методу для викриття аерозольних продуктів горіння.....	250
Славгородська О.С., НУЦЗУ Аналіз стану й тенденцій розвитку пожежної автоматизації України.....	251
Соловійов І.І., ГУ ДСНС України у Херсонській області Розробка математичної моделі підриву вибухонебезпечного предмету в процесі підводного гуманітарного розмінування.....	252
Стовпець О.С., НУЦЗУ Дослідження особливостей конструкції ємкісного чутливого елемента димового пожежного сповіщувача.....	253
Твердохлебов С.В., НУЦЗУ Використання ROIP-каналів для підвищення надійності системи моніторингу району надзвичайної ситуації.....	254
Тимков Н.О., ЛДУБЖД Забезпечення функціонування автоматичних систем водяного пожежогасіння при відсутності основного електроживлення.....	255
Федоренко Є.Р., Шинкаренко А.С., НУЦЗУ Рішення задачі розпізнання джерел забруднення при надзвичайних ситуаціях.....	256
Філіппова В.В., ЛДУБЖД Застосування безпілотних літальних апаратів при створенні інфрачервоних знімків земної поверхні.....	257
Шинкаренко А.С., Федоренко Є.Р., НУЦЗУ Сучасні базові концепції технології формування корпоративних сховищ даних.....	258
Шуміло В.Ю., НУЦЗУ Щодо напрямів забезпечення інформаційної безпеки в умовах надзвичайних ситуацій.....	259
Щербак О.С., НУЦЗУ Дослідження термічних уражень конструкцій в зоні надзвичайної ситуації внаслідок пожежі на об'єктах критичної інфраструктури.....	260
Kulitsa O., CIFS after Heroes of Chernoby NUCDU Video stream intensity control technology based on the selection of compression process parameters and block encoding.....	261