Додаток 1

Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра *Аналіз властивостей алгоритму UMAC-32 для забезпечення автентичності і цілісності даних*

назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Analysis of algorithm UMAC-32 vulnerabilities to provide data authenticity and completeness* ~~*completeness*~~

переклад англійською

Освітній ступінь : бакалавр

Шифр та назва спеціальності: 125 «Кібербезпека»

напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія № 46

напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя

напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 24 червня 2022 року **Місто:** Тернопіль

Сторінки:

Кількість сторінок роботи: 57

УДК: 004.056

Автор роботи

Прізвище, ім'я, по батькові (укр.): Мельник Степан Андрійович

розкривати ініціали

Прізвище, ім'я (англ.): Melnyk Stepan

використовувати паспортну транслітерацію (КМУ 2010)

Місце навчання (установа, факультет, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра кібербезпеки, м.Тернопіль, Україна

Керівник

Прізвище, ім'я, по батькові (укр.): Карташов Віталій Вікторович

повністю

Прізвище, ім'я (англ.): Kartashov Vitalii

використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Україна

Вчене звання, науковий ступінь, посада: к.т.н., доцент КТ

Рецензент

Прізвище, ім'я, по батькові (укр.): Приймак Микола Володимирович

повністю

Прізвище, ім'я (англ.): Pryimak Mykola

використовувати паспортну транслітерацію (КМУ 2010)

Місце праці (установа, підрозділ, місто, країна): ТНТУ ім. І. Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, Кафедра комп'ютерних наук, м.Тернопіль, Україна

Вчене звання, науковий ступінь, посада: доктор технічних наук, професор кафедри КН

Ключові слова

українською геш-функція, umac, гешування, цілісність, автентичність

до 10 слів

англійською hesh function, umac, gashing, integrity, authenticity
до 10 слів

Анотація

українською:

Об’єктом дослідження є процес забезпечення цілісності і автентичності інформації в інформаційних системах за допомогою алгоритму гешування UMAC-32.

Мета роботи полягає у розробці універсального алгоритму гешування UMAC-32, а також в аналізі механізмів забезпечення автентичності і цілісності інформації при використанні алгоритмів цифрового підпису і гешування, в оцінці їх основних ймовірно-часових характеристик.

Предметом дослідження є методи ключового гешування для забезпечення цілісності й автентичності інформації за допомогою алгоритму UMAC-32.

В результаті виконання роботи отримані наступні результати:

Проведено аналіз сучасних механізмів та протоколів забезпечення цілісності та автентичності даних на основі використання цифрових підписів та альтернативних їм варіантам геш-кодів на основі безключових та ключових геш-функцій.

Проведено аналіз методів побудови ключових геш-функцій (MAC-кодів), які при рівних умовах з MDC-кодами дозоляють інтегровано вирішувати завдання забезпечення цілісності та автентичності повідомлень без додаткового використання алгоритмів шифрування.

Алгоритм UMAC-32 може бути використаний в інформаційних системах масового призначення, які потребують швидкого обміну інформацією та якісного рівня забезпечення цілісності та автентичності переданої інформації.

англійською:

The object of research is the process of ensuring the integrity and authenticity of information in information systems using the hashing algorithm UMAC-32.

The purpose of the work is to develop a universal hashing algorithm UMAC-32, as well as to analyze the mechanisms for ensuring the authenticity and integrity of information using digital signature and hashing algorithms, in assessing their main probabilistic and temporal characteristics.

The subject of the research is the methods of key hashing to ensure the integrity and authenticity of information using the UMAC-32 algorithm.

As a result of performance of work the following results are received:

The analysis of modern mechanisms and protocols for ensuring the integrity and authenticity of data based on the use of digital signatures and alternative variants of hash codes based on keyless and key hash functions.

An analysis of methods for constructing key hash functions (MAC codes), which under equal conditions with MDC codes allow to solve the problem of ensuring the integrity and authenticity of messages without the additional use of encryption algorithms.

The UMAC-32 algorithm can be used in mass information systems that require rapid information exchange and a high level of integrity and authenticity of transmitted information.

Мельник С. А. Аналіз властивостей алгоритму UMAC-32 для забезпечення автентичності і цілісності даних: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / Мельник Степан Андрійович. – Тернопіль : ТНТУ, 2022. – 57 с.

Melnyk S. Analysis of algorithm UMAC-32 vulnerabilities to provide data authenticity and completeness: Bachelor thesis 125 — Cybersecurity / Melnyk Stepan - Ternopil, TNTU, 2022 – 57 p.