Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра *Розробка методів ключового хешування з використанням арифметики еліптич-них кривих*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Development of key hashing methods using elliptic curves theory*
переклад англійською

Освітній ступінь : бакалавр

Шифр та назва спеціальності: 125 «Кібербезпека»
напр.:151 Автоматизація та комп'ютерно-інтегровані технології

Екзаменаційна комісія: Екзаменаційна комісія № 37
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 2021 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 90

УДК: 004.056

Автор роботи
Прізвище, ім'я, по батькові (укр.): Кушнір Володимир Петрович
розкривати ініціали

Прізвище, ім'я (англ.): Kushnir Volodymyr Petrovych
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.): Александер Марек Богуслав
повністю

Прізвище, ім'я (англ.): Aleksander Marek Bohuslav
використовувати паспортну транслітерацію (КМУ 2010)

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

Вчене звання, науковий ступінь, посада: доктор технічних наук, доцент кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Липак Галина Ігорівна
повністю

Прізвище, ім'я (англ.): Lypak Halyna Ihorivna
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: кандидат наук із соціальних комунікацій, доцент кафедри КН

Ключові слова:
українською: інтернет-платіжна система, цілісність інформації, автентифікація повідомлення, електронний цифровий підпис, хеш-функція
до 10 слів

англійською: internet payment system, integrity of information, authentication messages, digital signature, hash function
до 10 слів

Анотація

українською:

Кваліфікаційна робота присвячена ключового хешування для забезпечення цілісності та автентичності інформації в Інтернет-платіжних системах. У резуль-таті в роботі проведено аналіз існуючих механізмів забезпечення цілісності та автентичності інформації в Інтернет-платіжних системах. проведена оцінка стій-кості сучасних алгоритмів ключового та без ключового хешування за допомо-гою методики тестування NIST STS національного інституту стандартів та тех-нологій США. Проведений аналіз побудови хеш-функцій MASH-1 та MASH-2 та визначені їх часові характеристики. З використанням положень теорії еліпти-чних кривих розроблені методи вдосконалення алгоритмів ключового хешуван-ня MASH-1 та MASH-2. Обгрунтовані рекомендації, щодо їх використання для забезпечення цілісності та автентичності транзакцій в Інтернет-платіжних систе-мах. Створений програмний продукт імітаційної моделі ключевого алгоритму хешування з використанням арифметики в групі точок еліптичної кривої.

англійською:

The qualification thesis is devoted to modeling of hash key to ensure the integrity and authenticity of information in the payment systems of Internet. The result of work is the analysis of existent mechanisms which provides integrity and authentication of information in the payment systems of Internet. Conducted estimation of firmness of modern algorithms key and without the key randomising by the method of testing NIST STS national institute of standards and technologies of the USA. Conducted analysis of construction of hash function MASH-1 and MASH-2 and certain them sentinel descriptions. With the use of positions of theory of elliptic curves the developed methods The software product of simulation model of keyed hashing algorithm is created with the use of arithmetic in the group of points of elliptic curve.