Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра *Програмна реалізація криптографічного протоколу розділення секрету*

назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Software implementation of secret sharing cryptographic protocol*

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: 23 червня 2021 року **Місто:** Тернопіль

Сторінки:

Кількість сторінок роботи: 70

УДК: 004.056

Автор роботи

Прізвище, ім'я, по батькові (укр.): Кмиць Володимир Романович

розкривати ініціали

Прізвище, ім'я (англ.): Kmyts Volodymyr Romanovych

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.): Муж Валерій Вікторович

повністю

Прізвище, ім'я (англ.): Muzh Valerii Viktorovych

використовувати паспортну транслітерацію (КМУ 2010)

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

Вчене звання, науковий ступінь, посада: кандидат юридичних наук, доцент кафедри кібербезпеки

Рецензент

Прізвище, ім'я, по батькові (укр.): Никитюк Вячеслав Вячеславович

повністю

Прізвище, ім'я (англ.): Nykytiuk Viacheslav Viacheslavovych

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 технічних наук, доц. кафедри КН

Ключові слова

українською: криптографічний протокол, розділення секрету, поліном Лагранжа, китайська теорема про остачі, схема Асмута Блюма

до 10 слів

англійською: cryptographic protocol, secret sharing, Lagrange polynom, Chinese remaining theorem, Asmuth-Bloom s scheme.

до 10 слів

Анотація

українською:

Кваліфікаційна робота присвячена розробці програмного забезпечення для криптографічного протоколу розподілу секрету. В роботі обґрунтовано вибір програмного середовища розробки та вибір методів порогових схем розділення секрету. Протестовано програмне забезпечення, в якому реалізовано дві схеми розділення секрету: Шаміра та Асмута-Блюма. Показано роботу програмного забезпечення при коректному використанні параметрів схеми та можливість відновлення секрету за частками. Також показано, що при недостатній кількості часток секрету, таємна інформація не буде відновлена.

Дану розробку можна використовувати для зберігання особливо важливої інформації в державницьких органах, або ж для надійного зберігання ключа шифрування.

В першому розділі описано сутність криптографічних протоколів та алгоритми відновлення секрету. В другому розділі обґрунтовано вибір програмного середовища та описано реалізацію розробки. В третьому розділі висвітлено результати тестування програмної розробки.

англійською:

Qualification thesis is devoted to the development of software for cryptographic protocol of secret sharing. The choice of software development environment and the choice of methods of threshold schemes for sharing secrets are substantiated in the paper. The software was tested, in which two schemes of secret sharing were implemented: Shamir and Asmuth-Bloom. The work of the software with the correct use of the parameters of the scheme and the possibility of restoring the secret by shares is shown. It is also shown that if there are not enough shares of the secret, the secret information will not be restored.

This development can be used to store particularly important information in government organizations, or to securely store the encryption key.

The first section describes the essence of cryptographic protocols and algorithms for the secret sharing. The second section substantiates the choice of software environment and describes the implementation of development. The third section highlights the results of software development testing.