Додаток 1
Форма відомостей про авторів матеріалу та описова інформація для видань ТНТУ

Авторська довідка

(реферату дипломної роботи магістра)

Назва дипломної роботи магістра: Використання оптимізованих алгоритмів асиметричної криптографії (CL-PKE) для пристроїв обмеженими ресурсами
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Use of optimized algorithms of asymmetric cryptography (CL-PKE) for resource constrained devices*
переклад англійською

Освітній ступінь : магістр

Шифр та назва спеціальності: 125 «Кіберберпека»

Екзаменаційна комісія: Екзаменаційна комісія №
напр.: Екзаменаційна комісія №1

Установа захисту: Тернопільський національний технічний університет імені Івана Пулюя
напр.: Тернопільський національний технічний університет імені Івана Пулюя

Дата захисту: 22 грудня 2021 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок дипломної роботи: 51 Кількість сторінок реферату:

УДК: УДК 004.056.55

Автор дипломної роботи
Прізвище, ім'я, по батькові (укр.): Ганайчук Олександр Володимрович
розкривати ініціали

Прізвище, ім'я (англ.): Hanaichuk Oleksandr
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.): Alexander Marek Boguslaw
використовувати паспортну транслітерацію (КМУ 2010)

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

Вчене звання, науковий ступінь, посада: кандидат технічних наук, професор кафедри кібербезпеки

Рецензент
Прізвище, ім'я, по батькові (укр.): Дуда Олексій Михайлович
повністю

Прізвище, ім'я (англ.): Duda Oleksii
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'ютених наук, м.Тернопіль, Україна

Вчене звання, науковий ступінь, посада: кандидат технічних наук, доцент кафедри комп'ютених наук

Ключові слова

українською: Криптографія з еліптичною кривою; криптосистема відкритого ключа буз сертифікатів; Шифрування відкритого ключа без сертифікатів; підпис відкритого ключа без сертифікатів

до 10 слів

англійською: Cryptography with an elliptical curve; public key cryptosystem of certificates; Public key encryption without certificates; public key signature without certificates

до 10 слів

Анотація

українською:

В роботі проведено огляд літературних джерел в області дослідження. Проведено аналіз існуючих оптимізованих алгоритмів CL-PKE. Запропоновано оптимізований алгоритм асиметричної криптографії для пристроїв з обмеженим доступом. У першій главі проведений огляд існуючих алгоритмів. У другій главі проведено аналіз еліптичної кривої та способи її використання у криптографії та проведений аналіз криптографії з відкритим ключем без сертифікатів. У третій главі проведена розробка оптимізованого алгоритму та проведено аналіз безпеки даного алгоритму. У підрозділі "Охорона праці" розглянуто правила охорони праці під час експлуатації електронно-обчислювальних машин У підрозділі "Безпека в надзвичайних ситуаціях " описано способи підвищення стійкості роботи об'єктів господарської діяльності у воєнний час.

англійською:

The paper reviews the literature in the field of research. The analysis of the existing optimized CL-PKE algorithms is carried out. An optimized asymmetric cryptography algorithm for devices with limited access is proposed. The first chapter reviews the existing algorithms. The second chapter analyzes the elliptic curve and ways to use it in cryptography and analyzes public key cryptography without certificates. In the third chapter the development of the optimized algorithm is carried out and the security analysis of this algorithm is carried out. The subsection "Occupational Safety" discusses the rules of occupational safety during the operation of electronic computers. The subsection "Safety in Emergencies" describes ways to increase the sustainability of economic activities in wartime.

Бібліографічний опис:

1. Ганайчук О. Використання оптимізованих алгоритмів асиметричної криптографії (CL-PKE) для пристроїв із обмеженими ресурсами [Текст] / Ганайчук О. Збірник тез IX науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» – Тернопіль (8 – 9 грудня 2021 р.), ТНТУ, 2021. – с.61