Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра *Аналіз та реалізація криптографічних перетворень для алгоритму ECDH(Elliptic Curve Diffie-Hellman)*

назви записувати нижнім регістром (як у реченні)

Назва (англ.):*Analysis and implementation of cryptographic transformations for the ECDH algorithm (Elliptic Curve Diffie-Hellman)*

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: 78

УДК: 004.056

Автор роботи

Прізвище, ім'я, по батькові (укр.): Сава Лука Михайлович

розкривати ініціали

Прізвище, ім'я (англ.): Sava Luka Mikhailovich

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.): Карпінський Микола Петрович

повністю

Прізвище, ім'я (англ.): Karpinsky Mykola Petrovich

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: доктор технічних наук, професор кафедри кібербезпеки

Рецензент

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

повністю

Прізвище, ім'я (англ.): Nikityuk Vyacheslav Vyacheslavovich

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, доцент кафедри комп'ютерних наук

Ключові слова:
українською: RSA, AES, ECC, ECDH, ECDLP, ЕК, SSL
до 10 слів

англійською: RSA, AES, ECC, ECDH, ECDLP, EC, SSL
до 10 слів

Анотація

українською:

Кваліфікаційна робота присвячена аналізу можливостей асиметричної схеми шифрування алгоритмом Діффі Хеллмана на еліптичних кривих та створенню відповідних програмних модулів. Метою даного дипломного проекту є аналіз асиметричного алгоритму Діффі Хеллмана на основі використання еліптичних кривих та розробка програмних модулів для виконання: генерації ключів, шифрування інформації та використання гібридної схеми шифрування.

Для досягнення поставленої мети були вирішені такі завдання:

- проведено аналіз алгоритму ECC;
- виявлено недоліки та переваги алгоритму ECC;
- досліджено алгоритм ноження точки ECC на ціле число та порядок, кофактор еліптичної кривої;
- досліджено схеми генерації ключів асиметричної криптографії;
- досліджено особливості генерації ключів алгоритму ECDH та процесу шифрування;
- виконано огляд методів використання списків контролю доступу;
- розроблено і реалізовано програмні модулі для генерації ключів ECDH, шифрування та дешифрування.

англійською:

The qualification of the work is devoted to the analysis of the possibilities of an asymmetric encryption scheme by the Diff Hellman algorithm on elliptic curves and the creation of different software modules. The method of this graduation project is the analysis of the asymmetric Diff Hellman algorithm based on elliptic curves and the development of software modules for viconnancy: key generation, encryption of information, and variety of hybrid encryption schemes.

For the achievement of the delivered mark, the following tasks were fulfilled:

- analysis of the ECC algorithm was carried out;
- shortcomings and advantages of the ECC algorithm were revealed;
- the algorithm for shearing the ECC point on the integer number and order, the cofactor of the elliptic curve has been completed;
- updated key generation scheme for asymmetric cryptography;
- the special features of key generation in the ECDH algorithm and the encryption process were verified;
- review of the methods of selection of access control lists;
- software modules for ECDH key generation, encryption and decryption were developed and implemented.

Бібліографічний опис:

Сава Л. М. Аналіз та реалізація криптографічних перетворень для алгоритму ECDH(Elliptic Curve Diffie-Hellman): кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / Л. М. Сава. – Тернопіль : ТНТУ, 2022. – 78 с.