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

Авторська довідка

(кваліфікаційної роботи бакалавра)

Назва кваліфікаційної роботи бакалавра *Дослідження та порівняння атак на криптосистему RSA*
назви записувати нижнім регістром (як у реченні)

Назва (англ.): *Research and comparison of attacks on the RSA cryptosystem*
переклад англійською

Освітній ступінь : бакалавр

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

Екзаменаційна комісія: Екзаменаційна комісія № 40
напр.: Екзаменаційна комісія №1

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

Дата захисту: 21 червня 2023 року **Місто:** Тернопіль

Сторінки:
Кількість сторінок роботи: 52

УДК: 004.056

Автор роботи
Прізвище, ім'я, по батькові (укр.): Ремінник Микола Михайлович
розкривати ініціали

Прізвище, ім'я (англ.): Reminnyk Mykola
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.): Загородна Наталія Володимирівна
повністю

Прізвище, ім'я (англ.): Zagorodna Natalia
використовувати паспортну транслітерацію (КМУ 2010)

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

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

Рецензент
Прізвище, ім'я, по батькові (укр.): Луцків Андрій Мирославович
повністю

Прізвище, ім'я (англ.): Lutskiv Andrii
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 систем та мереж, м.Тернопіль, Україна

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

Ключові слова
українською факторизація, частотний аналіз, квадратичне решето, атака, вразливість, rsa

до 10 слів

англійською factorization, frequency analysis, quadratic grid, attack, vulnerability, rsa

до 10 слів

Анотація

українською:

Кваліфікаційна робота присвячена перевірці вимог до криптосистеми RSA, для свідчення доцільності використання шифрування блоками застосовано частотний аналіз, а для вимог до генерації напівпростих чисел - квадратичне решето.

Проаналізовано алгоритм RSA, сфери його використання. Докладно розглянуто особливості частотного криптоаналізу, факторизації (квадратичного решета). Досліджено атаки Хастада та Вінера. Для програмної реалізації дослідження створено додаток на основі мови C# із використанням зовнішніх бібліотек. Наведено опис основних його класів та файлів, які формуються під час його роботи. Для реалізації атак обрана мова Python.

Були отримані експериментальні результати і для згенерованого тексту, і для тексту, створеного реальною особою.

Досліджено, що при порушенні сучасних вимог та постійному адаптуванні під них, з'являється ризик зменшення надійності способу шифрування..

англійською:

Thesis deals with checking the requirements for the RSA cryptosystem, frequency analysis is used to demonstrate the expediency of using block encryption, and the quadratic sieve is used for the requirements for the generation of semiprime numbers.

The RSA algorithm and the areas of its use are analyzed. Features of frequency cryptanalysis, factorization (quadratic lattice) are considered in detail. Hustad and Wiener attacks are investigated. For the software implementation of the research, an application based on the C# language was created using external libraries. A description of its main classes and files, which are formed during its operation, is given. The Python language is chosen for the implementation of attacks.

Experimental results were obtained for both generated text and text created by a real person.

It has been studied that in violation of modern requirements and constant adaptation to them, there is a risk of reducing the reliability of the encryption method.

Бібліографічний опис:

Ремінник М. М. Дослідження та порівняння атак на криптосистему RSA: кваліфікаційна робота бакалавра за спеціальністю 125 — Кібербезпека / Ремінник Микола Михайлович. – Тернопіль : ТНТУ, 2023. – 51 с.

Reminnyk M. Research and comparison of attacks on the RSA cryptosystem: Bachelor thesis 125 — Cybersecurity / Reminnyk Mykola - Ternopil, TNTU, 2023 – 52 p.