УДК 004.4

О.М. Липчей
Г.Б. Ракитянська

Аналіз дискретних структур у криптографії та безпеці інформації

Вінницький національний технічний університет

Анотація

Ця робота присвячена аналізу дискретних структур у контексті криптографії та безпеки інформації. Дискретні структури, такі як графи, групи та кільця, відіграють ключову роль у розвитку криптографічних алгоритмів та протоколів. Ця робота досліджує їхні застосування та вплив на безпеку інформації.

Ключові слова: дискретні структури, криптографія, безпека інформації, графи, групи, кільця, алгоритми шифрування, електронний підпис, ідентифікація, загрози безпеці, надійність систем.

Abstract

This work is devoted to the analysis of discrete structures in the context of cryptography and information security. Discrete structures such as graphs, groups, and rings play a key role in the development of cryptographic algorithms and protocols. This work explores their applications and impact on information security.

Keywords: discrete structures, cryptography, information security, graphs, groups, rings, encryption algorithms, electronic signature, identification, security threats, system reliability.

Вступ

Криптографія та безпека інформації стають дедалі важливішими у сучасному цифровому світі, де велика кількість конфіденційної інформації потребує захисту від несанкціонованого доступу. Із зростанням кількості цифрових транзакцій, збільшенням обсягу електронних даних і обсяг загроз для безпеки. У такому контексті дискретні структури відіграють надзвичайно важливу роль у створенні криптографічних систем.

Дискретні структури, такі як арифметика великих чисел, теорія чисел, групи та поля, становлять основу для розробки ефективних криптографічних алгоритмів. Вони використовуються для створення алгоритмів шифрування, електронного підпису, забезпечення цифрової ідентифікації та здійснення захисту конфіденційної інформації.

Результат дослідження

Результати дослідження свідчать про те, що аналіз основних дискретних структур, таких як графи, групи та кільця, має велике значення для розробки ефективних криптографічних систем. Розуміння властивостей цих структур дозволяє створювати алгоритми шифрування, електронного підпису та ідентифікації, які мають високу стійкість до криптоаналізу та недоступність для несанкціонованого доступу.

Наприклад, графи[1] використовуються для моделювання складних взаємозв'язків між об'єктами в криптографічних протоколах, що дозволяє ефективно аналізувати і підвищувати безпеку таких систем. Групи та кільця забезпечують математичну основу для реалізації алгоритмів шифрування та цифрового підпису, забезпечуючи конфіденційність та цілісність інформації.

Проте дослідження також виявило можливі загрози безпеці інформації, пов'язані з використанням дискретних структур[2] у криптографії. Наприклад, атаки з використанням квантових комп'ютерів можуть стати загрозою для алгоритмів, що базуються на складних математичних операціях, таких як факторизація великих чисел чи обчислення дискретного логарифма. Тому

важливим напрямком подальших досліджень є розробка квантовостійких криптографічних алгоритмів, які забезпечать безпеку інформації навіть у змінених умовах обчислювального середовища.

Висновки

. Дослідження дискретних структур підтверджує їхню важливу роль у сучасній криптографії та безпеці інформації. Вони є фундаментальними складовими у створенні надійних криптографічних систем, а їх розуміння та використання дозволяє розробляти більш ефективні методи захисту інформації. Аналіз дискретних структур показує, що їх використання може сприяти збільшенню безпеки в цифровому середовищі, а подальше дослідження в цій області може відкрити нові можливості для розвитку криптографічних технологій. Таким чином, розуміння та використання дискретних структур в криптографії залишається надзвичайно актуальним та перспективним напрямком досліджень.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Графи [Електронний ресурс]– Режим доступу до ресурсу: — https://uk.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D1%84_(%D0%BC%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)
2. Дискретних структур [Електронний ресурс]– Режим доступу до ресурсу: — http://elar.kpnu.edu.ua:8081/xmlui/handle/123456789/6686

Липчей Ольга Михайлівна **–** студентка групи 1ПІ-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: olha.lipchey@gmail.com.

Ракитянська Ганна Борисівна - доцент, Вінницький національний технічний університет, кафедра програмного забезпечення, rakit@vntu.edu.ua

Lipchey Olha Mykhaylivna - student of group 1PI-22b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: olha.lipchey@gmail.com.

Hanna Borisivna Rakityanska - associate professor, Vinnytsia National Technical University university, department of software, rakit@vntu.edu.ua