УДК 004.056.5

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ У КІЛЬЦІ ЗРІЗАНИХ ПОВІДОМЛЕНЬ

Романюк Назар

RESEARCH ON CRYPTOGRAPHIC TRANSFORMATIONS IN THE RING OF CUT MESSAGES

Romaniuk Nazar

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *The study examines cryptographic transformations based on the ring of truncated messages, a mathematical structure with promising properties for information protection. The operations of addition and multiplication within this ring and their impact on encryption reliability and attack resistance are analyzed. Encryption algorithms have been developed, showing efficiency in ensuring data confidentiality and integrity under digital threat conditions.*

У даному дослідженні розглянуто криптографічні перетворення, що використовують кільце зрізаних повідомлень — важливу математичну структуру для реалізації надійних механізмів захисту інформації. Кільце зрізаних повідомлень має значний потенціал у побудові стійких криптографічних алгоритмів завдяки властивостям, зокрема обмеженню розміру елементів і періодичності операцій, що дозволяють зменшити складність атак. Основні завдання дослідження включають детальний аналіз теоретичних засад криптографічних перетворень на основі кільця зрізаних повідомлень, а також вивчення його математичних властивостей. Кільце дозволяє виконувати операції над елементами за чітко визначеними правилами, що значно спрощує побудову криптографічних методів. Особлива увага приділяється обмеженням розміру та властивостям елементів, які визначають ефективність перетворень, розглянуто особливості використання операцій додавання і множення в кільці зрізаних повідомлень для шифрування та дешифрування. У межах дослідження розроблено криптографічні алгоритми, засновані на операціях у кільці зрізаних повідомлень. Їх ефективність оцінюється з огляду на стійкість до атак різних типів: факторизаційних, перебірних та інших методів криптоаналізу. У результаті дослідження створено інноваційні алгоритми шифрування, здатні забезпечити високий рівень захисту інформації в умовах сучасних цифрових комунікацій. Алгоритми орієнтовані на ефективну реалізацію криптографічних протоколів, зокрема для безпечного обміну даними. Завдяки використанню математичних властивостей кільця зрізаних повідомлень, розроблені рішення стійкі до широкого спектру атак, що забезпечує надійний захист персональної та корпоративної інформації в умовах зростаючих кіберзагроз.

Бібліографія

1. Доронін, А. О., & Терещенко, О. О. (2020). Методи шифрування інформації та їх застосування в цифрових системах. *Вісник НТУУ «КПІ»,* 5, 45–52. https://kpi.ua/sites/default/files/2020/5_45.pdf
2. Артьомов, С. О., & Городиський, С. М. (2021). Аналіз сучасних загроз інформаційній безпеці у хмарних середовищах. *Захист інформації,* 2, 12–19. https://www.zashist.com.ua/articles/2021-02