



# НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
# ПОЛТАВСЬКА ПОЛІТЕХНІКА
# ІМЕНІ ЮРІЯ КОНДРАТЮКА

## ЗБІРНИК МАТЕРІАЛІВ

### 76-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

### ТОМ 1

**14 травня – 23 травня 2024 р.**

**УДК 368.016**

*Рассоха І.В., к.ф.-м. н., доцент*
*Барановський П.М.., студент групи 101-ТН,*
*Юхно О.В., студент групи 101-ТН,*
*Національний університет*
*«Полтавська політехніка імені Юрія Кондратюка»*

# МАТЕМАТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ ДЕЯКИХ ВИДІВ АТАК НА КРИПТОСИСТЕМУ RSA

З'ясуємо різницю між криптографією та криптоаналізом. Криптографія займається проектуванням шифрів, тоді як криптоаналіз спрямований на їх розшифрування. Перший створює методи шифрування, другий намагається їх розібрати. Математичною базою в даному випадку є одностороння функція або одностороння функція із секретом. Під односторонньою функцією розуміють функцію, якщо існує ефективний алгоритм її обчислення при всіх допустимих значеннях аргументу і не існує такого алгоритму для обчислення оберненої функції. В даній роботі ми розглядаємо RSA шифрування та математичні основи основних видів атак на вказану криптосистему. Шифрування RSA ґрунтується на терії подільності, зокрема, на добутку двох великих простих чисел. Цей принцип обумовлює більшість атак на неї. Різноманітні атаки загрожують цілісності RSA шифрування. Від нападів на факторизацію цілих чисел до використання математичних функцій. Розуміння цих вразливостей є ключовим для підвищення криптографічної безпеки.

Однією з таких атак є атака на факторинг цілих чисел. Факторизація цілих чисел (розкладання числа на прості множники) – давня проблема теорії чисел, становить значний виклик для безпеки RSA [1]. Сучасній математиці відомо досить багато методів факторизації: метод Евкліда, решето Ератосфена, лінійне решето, квадратичне решето тощо. Спеціалізовані та універсальні алгоритми факторизації намагаються розкрити прості множники модулю RSA. Ефективність цих алгоритмів варіюється, що впливає на безпеку криптографічних систем.

Атака Вінера використовує вразливості при генерації ключів RSA. Зловмисники можуть розшифрувати криптотексти ефективно, використовуючи невеликий приватний ключ. Розуміння таких атак підкреслює важливість надійних практик генерації ключів [2].

Вразливості з малою публічною експонентою обумовлена тим, що вибір малої публічної експоненти в RSA шифруванні приводить до вразливості. Атаки використовують гомоморфні властивості RSA, особливо коли використовуються малі експоненти. Проти таких ризиків використовуються контрзаходи, такі як використання більших експонент або введення випадковості. Гомоморфна структура RSA шифрування дозволяє деякі атаки, наприклад, обрані атаки на криптотексти. Розуміння

того, як гомоморфні властивості можуть бути використані, є важливим для зміцнення криптографічних захистів [3].

Атаки на криптосистему – складна форма криптоаналізу, для розуміння якої необхідне широке використання таких математични понять, як модульна арифметика, гомеоморфні властивості тощо, а впровадження контрзаходів, які часто грунтуються на математичних принципах, є ключовим забезпечення цілісності криптографічних систем.

*Література:*


1. *Король, Ю. В. QS- алгоритм факторизації цілих чисел, його модифікації = QS-method of factorization of integers, its modifications : дипломна робота спеціаліста / Ю. В. Король ; наук. кер. О. В. Савастру ; ОНУ ім. І.І. Мечникова, ІМЕМ, Каф. комп'ютерної алгебри та дискретної математики . – Одеса, 2017 . – 91 с.*
2. *Boneh, D., 1999. Twenty years of attacks on the RSA Cryptosystem. Notices of the AMS, 46: 2003-2013.*
3. *Hastad J., 1986. On using RSA with Low Exponent in a Public-Key Network. Advances in Cryptology, 218: 404-408.*



**УДК 81'25:004.4]-043.86**



*А.В. Бережний, аспірант*
*Національний університет*
*«Полтавська політехніка імені Юрія Кондратюка»*


# СИСТЕМИ АВТОМАТИЗАЦІЇ ПЕРЕКЛАДУ: ЕВОЛЮЦІЯ ПІДХОДІВ

Стрімкі темпи розвитку перекладацьких технологій, володіння якими (особливо CAT-інструментами) є однією з найважливіших умов для забезпечення конкурентоспроможності майбутнього перекладача, зумовлюють увагу до них в контексті підготовки відповідного фахівця. Значною мірою це пов’язано з тим, що ринок перекладацьких послуг із кожним роком набуває рис дійсної індустрії, свідченнями чому є наявність своїх галузевих стандартів. Саме це стає безумовною підставою для обов’язкового належного опанування цими технологіями саме фахівців-перекладачів, якщо вони прагнуть бути затребуваними на сучасному ринку праці.

Крім того, аналіз провідних стандартів перекладацької галузі доводить, що всі вони містять згадки про технічний інструментарій перекладача, прописують вимоги до його володіння, і навіть вказують, які саме програми має опанувати професійний перекладач, що дозволяє нам зробити висновок про виключне місце технологій у структурі сучасної перекладацької діяльності, зокрема CAT-інструментів. Отже, модерні перекладацькі технології мають бути неодмінним складником їхньої