Секція 1

ПОРІВНЯЛЬНИЙ АНАЛІЗ ДВОХ АЛГОРИТМІВ ФАКТОРИЗАЦІЇ

Труш М. С.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Алгоритм RSA залишається одним із найпоширеніших методів асиметричного шифрування, забезпечуючи захист передачі даних в Інтернеті та в інших мережах. Існує достатньо комерційних та відкритих платформ, які використовують криптосистему RSA, в тому числі поширені операційні системи, такі як Windows, MacOS, UNIX-подібні операційні системи [1]. Актуальність RSA підкріплюється його стійкістю проти класичних методів криптоаналізу, які базуються на факторизації великих чисел. Для стимулювання розвитку більш ефективних алгоритмів факторизації компанія RSA Laboratories заснувала RSA Factoring Challenge, який тривав до 2007 року. Незважаючи на завершення виклику, останні досягнення, такі як факторизація числа RSA-250 у 2020 році, демонструють, що дослідження в цій галузі тривають і мають значний вплив на безпеку RSA [2]. Окрім традиційних методів криптоаналізу, сьогоднішні дослідження фокусуються на розробці нових підходів до факторизації великих чисел для криптосистеми RSA, що дозволяє не лише оцінювати ефективність алгоритмів, але й створює потенційну загрозу для систем безпеки, якщо такі методи стануть обчислювально доступними [3]. Порівняльний аналіз алгоритмів факторизації дає можливість дослідникам оптимізувати стратегії захисту на основі сучасних криптоаналітичних досягнень, передбачаючи потенційні слабкі місця і рекомендувати більш захищені варіанти ключів або алгоритмів, щоб забезпечити довготривалу безпеку даних в умовах стрімкого розвитку обчислювальних технологій.

Мета роботи. Аналіз двох алгоритмів факторизації з проведенням експерименту для визначення найбільш ефективного алгоритму.

Основні положення. В роботі детально розглянуто алгоритм факторизації, в якому використовуються змінні P і Q, що коригуються на кожному кроці для поступового досягнення нульової різниці (дельти) між факторизованим числом N та добутком змінних P і Q. До переваг алгоритму належить значна швидкодія завдяки використанню простих операцій додавання та віднімання замість множення, що мінімізує обчислювальні витрати, особливо для великих чисел. В роботі показано, що на певному етапі алгоритм досягає стабільності в кількості ітерацій, що дозволяє

прогнозувати час факторизації та забезпечує додаткове прискорення виконання завдання. Окрім основних принципів факторизації, у документі також розглядається особлива техніка контролю помилок, яка базується на спостереженні за зміною знаку різниці дельти на кожному кроці алгоритму. Якщо дельта становить від'ємною, алгоритм корегує значення P і Q, таким чином, щоб на наступному кроці результат був додатнім, і навпаки. Це чергування знаків помилки дозволяє точно налаштувати кроки алгоритму, мінімізуючи кількість обчислень і швидше наближаючись до нульового значення при якому можна вважати, що спільний дільник для числа *N* знайдено.

Висновки. Попри високу стійкість і поширеність криптосистеми RSA, зокрема у комерційних системах, розвиток нових методів криптоаналізу постійно стимулює вдосконалення технік факторизації. Факторизація RSA-250, який складається з 829 бітів, демонструє прогрес у галузі, що підвищує актуальність аналізу різних алгоритмів факторизації. Дослідження також показали, що оптимізація обчислень за рахунок використання менш ресурсомістких операцій підвищує швидкодію роботи алгоритму.

Список літератури

1. RSA authentication agent supported platforms. *Scribd*. URL – https://www.scribd.com/document/89623408/RSA-Authentication-Agent-Supported-Platforms (дата звернення: 05.11.2024).

2. Boudot F., Gaudry P., Guillevic A., Heninger N., Thomé E., Zimmermann P. Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment. The 40th Annual International Cryptology Conference (Crypto 2020). August 2020. DOI: https://doi.org/10.48550/arXiv.2006.06197.

3. Pevnev V. Pseudoprime Numbers: Basic Concepts And The Problem Of Security. International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications. 2017. Page 583-593. URL: https://ceur-ws.org/Vol-1844/10000583.pdf (дата звернення 06.11.2024).

Відомості про авторів

Труш Марина Сергіївна, студентка кафедри інженерії програмного забезпечення, НАУ «ХАІ»

Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu