Державний заклад
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ імені К. Д. УШИНСЬКОГО»

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І. І. МЕЧНИКОВА

ДВАДЦЯТЬ ДРУГА ВСЕУКРАЇНСЬКА КОНФЕРЕНЦІЯ СТУДЕНТІВ І МОЛОДИХ НАУКОВЦІВ

ІНФОРМАТИКА, ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

25 квітня 2025 р.

Одеса – 2025

Інформатика, інформаційні системи та технології: тези доповідей двадцять другої всеукраїнської конференції студентів і молодих науковців. Одеса, 25 квітня 2025 р. - Одеса, 2025. – 315 с.

Друкується за рішенням Вченої Ради
Університету Ушинського
(протокол № 16 від 29.05.2025 р.)

Організатори конференції продовжують традицію обміну досвідом у сфері освіти та використання інформаційних технологій. У конференції приймають участь студенти, аспіранти та молоді науковці вищих навчальних закладів України.

Тематика конференції охоплює наступне коло питань: сучасні інформаційні технології; інтелектуальні системи; методика викладання інформатики; інформаційні технології в освіті; психолого-педагогічне забезпечення інформатизації навчальної діяльності; дистанційна освіта і глобальні телекомунікаційні мережі; математичне моделювання й інформаційні технології; інформатизація системи керування освітою; інформаційні технології в менеджменті.

Наукові керівники:

завідувачка кафедри прикладної математики та інформатики
фізико-математичного факультету Університету Ушинського, д. т. н., проф. Т. Л. Мазурок,
завідувач кафедри математичного забезпечення комп'ютерних систем факультету математики, фізики та інформаційних технологій ОНУ імені І. І. Мечникова, д. т. н., проф. Є. В. Малахов

Оргкомітет:

Голова:

Ректор Університету Ушинського,
д. і. наук, доц. А. В. Красножон

Заступники голови:

Проректор з наукової роботи Університету Ушинського, д. політ. н., проф. Г.В. Музиченко
Декан факультету математики, фізики та інформаційних технологій ОНУ імені І. І. Мечникова, д. ф-м. н., проф. Ю. А. Ніцук

Члени оргкомітету:

д. т. н., проф.	Є. В. Малахов	д. т. н., проф.	Т. Л. Мазурок
д. т. н., проф.	Ю. О. Гунченко	к. п. н., доц.	А. О. Яновський
ст. викладач	І. М. Лісіцина	викладач	О. Я. Рубанська
ст. викладач	Н. Ф. Трубіна	к. ф.-м. н.	О. П. Бойко
ст. викладач	В. А. Корабльов	PhD, associated prof. (Poland)	A. Rychlik

другої – 0,9938, 0,0305 та 1,0000, що свідчить про прийнятну якість двох побудованих лінійних регресійних моделей.

Висновки Удосконалено дві трифакторні лінійні регресійні моделі для оцінювання кількості рядків коду вебзастосунків, що створюються з використанням фреймворку Codeigniter, в залежності від кількості класів, середньої кількості методів на клас та метрики DIT на рівні застосунку на основі розбиття набору даних на два кластери. Ці моделі в порівнянні з існуючими регресійними моделями дозволяють описувати всі дані, за якими вони були побудовані. В подальшому планується створення регресійних моделей для оцінювання кількості рядків коду вебзастосунків, що розробляються з використанням інших фреймворків, які дозволяли би описувати всі дані, за якими вони будуть побудовані.

Література

1. Prykhodko S.B., Shutko I.S., Prykhodko A.S. Early size estimation of web apps created using Codeigniter framework by nonlinear regression models. Radioelectronic and computer systems. 2022. Vol. 3 (103). P. 84-94. DOI: 10.32620/reks.2022.3.06
2. Prykhodko S., Prykhodko N. Building nonlinear regression models for estimating the number of clusters and their initial centroids. Proceedings of the 2023 IEEE 18th International Conference on Computer Sciences and Information Technologies (CSIT), 2023. P. 1-4. DOI: 10.1109/CSIT61576.2023.10324095

МОДИФІКАЦІЯ АЛГОРИТМУ ФАКТОРИЗАЦІЇ ВЕЛИКИХ ЧИСЕЛ ДЛЯ ВІДКРИТОЇ КРИПТОГРАФІЇ

Алєксєєва С. А., Тимошенко Л. М.
Національний університет «Одеська політехніка»

Ключові слова: криптографія, факторизація, криптоаналіз, метод Ферма.

У сучасному цифровому світі та великій війні сьогодення інформаційна безпека набуває критичного значення. Асиметричні криптографічні алгоритми, зокрема RSA, що ґрунтуються на складності факторизації великих цілих чисел, є фундаментальною основою для забезпечення конфіденційності та автентичності даних. Однак розвиток обчислювальних потужностей та нові методи криптоаналізу ставлять під загрозу стійкість криптосистем[1]. Тому актуальним є дослідження та модифікація методів факторизації з метою оцінки їх ефективності та виявлення потенційних загроз для відкритої криптографії.

Крипостійкість системи RSA заснована на тому, що приховане повідомлення не може бути розкрите без знання множників p і q, а їх знаходження з n вважають складно вирішуваним завданням [2].

Мета роботи – зменшення обчислювальної складності алгоритму факторизації великих чисел як оцінки криптостійкості RSA-подібних систем шляхом удосконалення методу Ферма. Для її реалізації проаналізовано сучасні методи рішення криптоаналітичних задач та розглянуто основні алгоритми факторизації; обґрунтувано використання системи залишкових класів; модифіковано метод факторизації Ферма та оцінено його обчислювальну складність; виконано порівняльний аналіз ефективностей запропонованого і класичного методів факторизації Ферма.

У залежності від складності алгоритми факторизації поділяють на групи – експонентні, складність їх експонентно залежить від довжини числа в бінарному представленні, та субекспонентні, які працюють довше поліноміального часу, але швидше експонентного[3].

При дослідженні роботи алгоритмів виявлено, що при наявності близьких множників p та q найбільш ефективним є класичний метод Ферма. З простоти алгоритмічної реалізації розкладу натурального числа у добуток простих множників за допомогою цього алгоритму виникла ідея спроби модифікації методу Ферма для його можливої реалізації на звичайному комп'ютері з довгими числами. Для удосконалення методу Ферма обґрунтовано використано систему залишкових класів та символи Якобі[4]. СЗК зменшить обчислювальну складність за рахунок зменшення довжини чисел. Символи Якобі дозволять однозначно визначити обчислюваність квадратного кореня за модулем у методі Ферма.

Блок-схема запропонованого алгоритму зображена на рисунку 1.

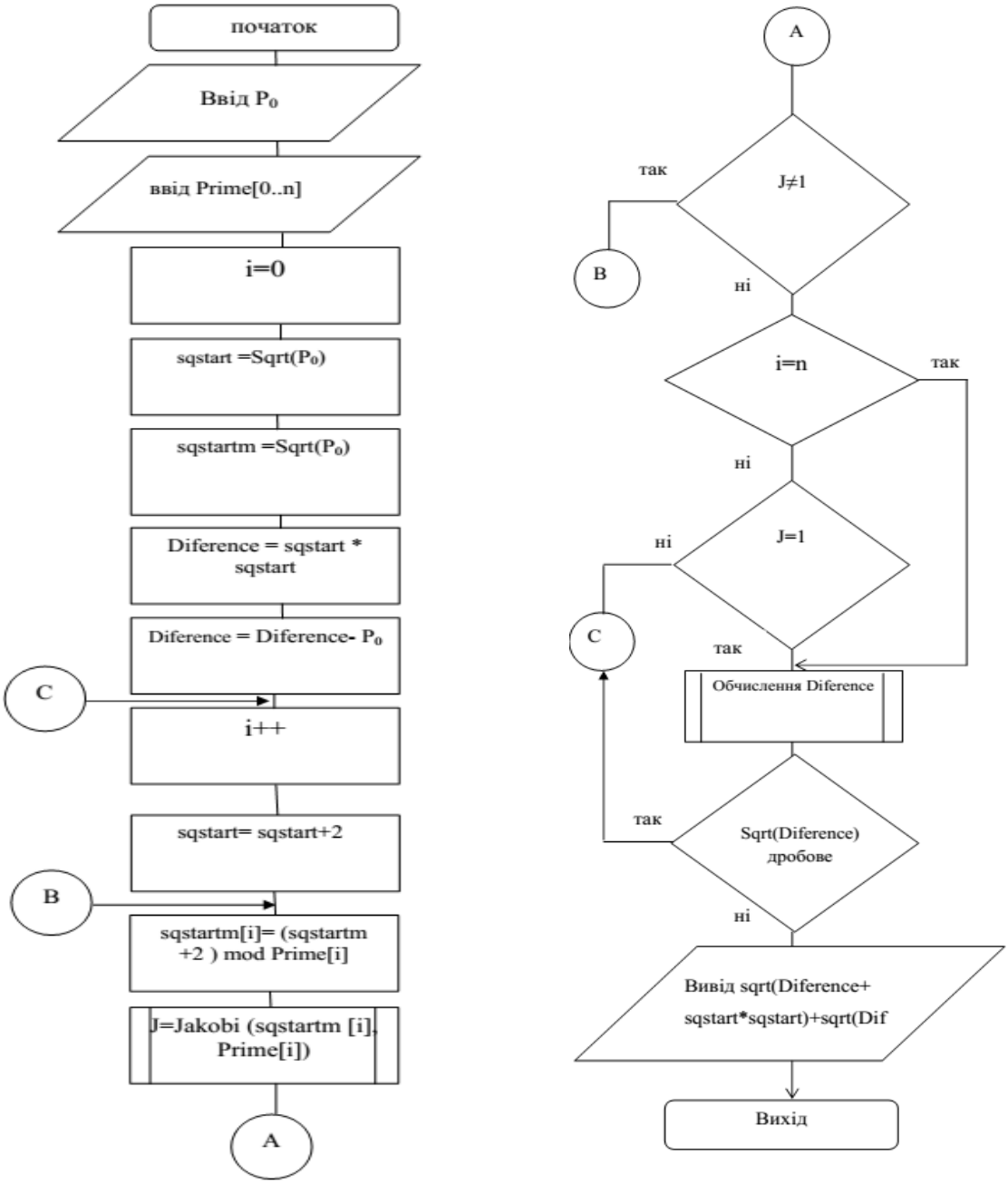

Рисунок 1 – Блок-схема модифікованого алгоритму факторизації

Реалізація і використання запропонованого алгоритму дозволить проєктувати ефективніші з точки зору швидкодії апаратно-програмні засоби криптоаналізу та підвищити якість оцінки криптостійкості системи RSA.

Література

1. Joux A. Algorithmic Cryptanalysis. Boca Raton: CRC Press, 2009. 384 p.
2. Koblitz N. A Course in Number Theory and Cryptography. 3rd ed. New York: Springer, 2012. 261 p.
3. Козюкалов М., Бойко М. Дослідження та аналіз алгоритмів факторизації чисел. *ЛОГОΣ. Мистецтво наукової думки*. 2020.(10), С.64-68.

4. Тимошенко Л.М., Вербик К.В., Івасьєв С.В.. Удосконалення алгоритму факторизації для криптографічних систем захисту інформації. *Сучасна спеціальна техніка*. № 4.2014. С. 35-40.

EXPO ЯК ІНСТРУМЕНТ ДЛЯ РОЗРОБКИ МОБІЛЬНИХ ДОДАТКІВ

Бабков А. С., Рудніченко М. Д.
Національний університет «Одеська політехніка»

Анотація: У даній роботі наведено аналіз використання Expo як інструменту для розробки мобільних додатків, його переваг та недоліків у порівнянні з альтернативними підходами.

Ключові слова: Expo, React Native, мобільна розробка, кросплатформені додатки.

Вступ. Expo є потужним інструментом для створення мобільних додатків на основі React Native, що значно спрощує процес розробки, тестування та розгортання програм. Завдяки своєму інтуїтивному підходу та вбудованому набору функцій, Expo дозволяє розробникам швидко створювати кросплатформені додатки без необхідності встановлення додаткових нативних бібліотек або SDK. Однак, незважаючи на численні переваги, використання Expo також має певні обмеження, що впливають на можливості кастомізації та продуктивність додатків. Важливим є порівняння основних підходів до мобільної розробки, визначення їх переваг та недоліків, а також оцінка ефективності Expo у цьому контексті.

Основні підходи до мобільної розробки. Сучасні методи створення мобільних додатків можна поділити на три основні категорії: використання Expo, традиційна розробка на React Native з нативними модулями та повністю нативна розробка. Кожен з цих підходів має свої особливості, які визначають їх ефективність у різних сценаріях.

Expo забезпечує зручне середовище для швидкої розробки мобільних додатків. Його головна перевага — можливість запуску додатка без налаштування нативних середовищ iOS та Android. Expo пропонує широкий спектр API, що спрощує роботу з такими функціями, як камера, push-сповіщення, геолокація та мультимедіа. Проте основним недоліком є обмежений доступ до нативних модулів, що може обмежувати можливості додатка.

Традиційна розробка на React Native дозволяє використовувати як JavaScript, так і нативний код (Swift, Kotlin, Java) для інтеграції необхідних функцій. Це забезпечує більшу гнучкість у порівнянні з Expo, але водночас ускладнює процес розробки, оскільки вимагає налаштування середовищ та встановлення додаткових бібліотек.