Національна академія наук України
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова

МАКСИМЕНКО Євген Васильович

УДК 519.6

ОБЧИСЛЮВАЛЬНІ МЕТОДИ НА ОСНОВІ АЛГОРИТМУ ФЕРМА ПРИ КРИПТОАНАЛІЗІ RSA АЛГОРИТМУ АПАРАТНО-ПРОГРАМНИМИ ЗАСОБАМИ

01.05.02 – математичне моделювання та обчислювальні методи

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2017

Дисертацією є рукопис.

Робота виконана в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ.

Науковий керівник: доктор технічних наук,
старший науковий співробітник
ВИННИЧУК Степан Дмитрович,
Інститут проблем моделювання
в енергетиці ім. Г.Є. Пухова НАН України,
завідувач відділом №8, м. Київ.

Офіційні опоненти: доктор технічних наук,
старший науковий співробітник
КАЛІНОВСЬКИЙ Яків Олександрович,
Інститут проблем реєстрації інформації НАН України,
старший науковий співробітник відділу
спеціалізованих засобів моделювання, м. Київ.

доктор технічних наук,
старший науковий співробітник
ГРИЩУК Руслан Валентинович,
Житомирський військовий інститут імені С.П. Корольова, Міністерство оборони України,
начальник науково-дослідного відділу
інформаційної та кібернетичної безпеки наукового центру, м. Житомир.

Захист відбудеться «14» вересня 2017 р. о 14 годині на засіданні спеціалізованої вченої ради Д 26.185.01 Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

З дисертацією можна ознайомитись у бібліотеці Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

Автореферат розісланий «10» 08 2017 р.

Вчений секретар
спеціалізованої вченої ради Д 26.185.01 В.В. Душеба

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасний етап розвитку суспільства пов'язаний із суттєвим зростанням обсягу інформації, значна частина якої представлена в електронному вигляді. Завдання забезпечення безпеки інформації при її обробці в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (ІТС) на даний час є одним з найбільш пріоритетних в багатьох країнах світу і, в тому числі, в Україні. Одним з способів вирішення завдань захисту державних інформаційних ресурсів та інформації з обмеженим доступом (ІзОД) при її обробці та передачі в ІТС є криптографічний захист інформації (КЗІ).

КЗІ здійснюється шляхом застосування криптографічних алгоритмів (КА). Для допуску до експлуатації засобів та комплексів КЗІ, що реалізують вказані КА, здійснюється комплекс організаційно-технічних заходів щодо проведення їх тематичних досліджень, невід'ємною складовою яких є криптографічні дослідження. Обов'язковим етапом проведення цих досліджень є оцінка стійкості алгоритмів (протоколів), що використовуються в об'єктах досліджень, до всіх відомих на даний час методів криптоаналізу. Підвищення ефективності таких досліджень є актуальною технічною проблемою, вирішення якої передбачає удосконалення обчислювальних алгоритмів, технічних і програмних засобів.

Одним із сучасних різновидів КА є асиметричні КА (АКА), основною перевагою яких є можливість здійснення обміну ключовою інформацією (її формування) незахищеними каналами. Серед значної кількості сучасних АКА стандартом для багатьох криптографічних систем де-факто вважається RSA. Результати досліджень щодо методів його криптоаналізу представлені в роботах авторів Song Y. Yan, P. Kocker, A. Shamir, D. Genkin, B. Weger, G. Sounak, P. Goutam, D. Brown, С.М. Авдошин, І.Д. Горбенко та багато інших. Аналіз публікацій показує, що більшість відомих прикладів компрометації АКА RSA відносяться до певних їх практичних реалізацій, проте в загальному випадку не є ефективнішими за вирішення задачі факторизації його криптомодуля, що представляє собою багаторозрядне число.

Сучасні методи факторизації багаторозрядних чисел, такі як метод квадратичного решета (QS – Quadratic Sieve) і решета числового поля (GNFS – General Number Field Sieve), базуються на фундаментальних ідеях алгоритму Ферма. Тому задачі розробки або удосконалення алгоритму факторизації Ферма є актуальними в загальній проблематиці підвищення швидкодії апаратно-програмних засобів, що використовуються при оцінці криптостійкості КА.

Задача зменшення обчислювальної складності методу Ферма вирішувалася багатьма дослідниками. Результати цих досліджень представлені в роботах авторів D. Knuth, D. Brown, J. McKee, D. Lehmer, R. Lukes, C. Patterson, H. Williams та багатьох інших. Серед останніх результатів можна виділити праці Н.А. Каленикова, В.А. Мінаєва, І.Г. Велічко. Аналіз цих робіт показує, що сучасним підходом до зменшення обчислювальної складності алгоритму Ферма є удосконалення механізмів проріджування пробних X, які обумовлюють основні часові затрати методу. Однак у всіх цих роботах реалізується проріджування з деяким малим постійним кроком. Питання ж збільшення кроку проріджування, в тому числі використання нерівномірного кроку просіювання, залишаються на даний час не вирішеними. Крім

того, при реалізації відомих методів удосконалення алгоритму Ферма виконуються арифметичні операції з багаторозрядними числами, що суттєво підвищує обчислювальну складність при вирішенні задачі факторизації на одно та багатопроцесорних комп'ютерних системах, а також ускладнює використання сучасних засобів високопродуктивних розподілених систем обчислень, наприклад, графічних карт, де суттєвим є обмеження на типи даних.

Таким чином, в дисертації вирішується актуальна **наукова задача**, що має важливу наукову та практичну спрямованість при удосконаленні існуючих і створенні перспективних апаратно-програмних засобів здійснення криптоаналізу АКА RSA – розробка обчислювальних методів факторизації на основі алгоритму Ферма, що дозволяють підвищити швидкодію апаратно-програмних засобів, які використовуються при криптоаналізі RSA алгоритму завдяки створення більш ефективних методів проріджування і зменшення обчислювальної складності операцій з багаторозрядними числами.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження проводились в рамках НДР «Загроза», що виконувалась в Інституті спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" (ІСЗЗІ КПІ ім. Ігоря Сікорського) (д/р № 0110U000016д), НДР «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики», (д/р 0114U002361), що виконувалась в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, а також НДР «Інфраструктура» (д/р №0114U000038д), що виконувалась в Державному науково-дослідному інституті спеціального зв'язку та захисту інформації Державної служби спеціального зв'язку та захисту інформації України.

Мета і задачі дослідження. Метою роботи є зменшення обчислювальної складності методів факторизації багаторозрядних чисел для підвищення швидкодії апаратно-програмних засобів при вирішенні завдань криптоаналізу АКА RSA.

Відповідно до поставленої наукової задачі в дисертаційній роботі вирішуються наступні взаємозалежні **часткові задачі дослідження**:

1. Провести аналіз математичних методів і підходів до оцінки захищеності АКА RSA при проведенні тематичних досліджень. Визначити роль і місце алгоритму факторизації Ферма при оцінці криптостійкості RSA-алгоритму.

2. Розробити метод проріджування пробних X з нерівномірним кроком для зменшення обчислювальної складності алгоритму факторизації Ферма.

3. Здійснити аналіз та оцінити можливість використання наближуючих коефіцієнтів при переході від співвідношення $N = p * q$ до $k * N = k * p * q$, для зменшення обчислювальної складності методу факторизації Ферма.

4. Розробити спосіб спільного використання наближуючих коефіцієнтів і проріджування пробних X з нерівномірним кроком для прискорення алгоритму факторизації Ферма.

5. Запропонувати метод зниження обчислювальної складності процедури проріджування на підставі врахування особливостей криптомодуля N при вирішенні завдань криптоаналізу.

6. Розробити рекомендації стосовно можливості використання запропонованих методів та алгоритмів для апаратних та апаратно-програмних засобів при оцінці криптостійкості RSA-алгоритму.

Об'єктом дослідження є процес факторизації багаторозрядних чисел при проведенні криптоаналізу АКА RSA, а ***предметом дослідження*** – обчислювальні методи факторизації багаторозрядних чисел, що засновані на алгоритмі Ферма та використовують методи проріджування і зменшення обчислювальної складності операцій з багаторозрядними числами.

Методи дослідження. Для вирішення наукової задачі використані методи теорії чисел, теорії оптимізації, алгоритмічної теорії багаторозрядних чисел, теорії складності обчислень, чисельні методи, методи комп'ютерного моделювання.

Наукова новизна отриманих результатів визначається наступними положеннями:

1. Вперше розроблено метод проріджування пробних значень невідомої X з нерівномірним кроком, в якому запропоновано використання базової основи модуля bb, для якої одноразово визначається множина коренів модульного рівняння, за рахунок чого формуються всі допустимі для bb пробні X, оцінка допустимості яких проводиться для додаткових основ модулів. За рахунок формування списку коренів модульного рівняння для bb суттєво зменшено кількість пробних значень X, які аналізуються за допомогою додаткових модулів, а розроблений метод їх подання у вигляді приростів дозволяє уникнути виконання арифметичних операцій з багаторозрядними числами, замінивши їх операціями з числами типу *long*.

2. Вперше запропоновано метод отримання первинної основи bb з максимальним значенням мінімального прискорення при обмеженні на допустимий обсяг пам'яті ЕОМ, який ґрунтується на математичній постановці задачі нелінійного цілочисельного програмування та способі її вирішення. Показано, що її рішення можна отримати методом повного перебору показників степенів простих чисел p - множників bb, які при $p > 2$ не перевищують 2 та при $p = 2$ менші 5.

Запропонований метод дозволяє знизити обчислювальну складність алгоритму Ферма, оскільки на основі чисельних експериментів встановлено, що зменшення часу обчислень пропорційно коефіцієнту прискорення для bb.

3. Вперше запропоновано комплексний метод факторизації чисел, в якому використовується багаторазове проріджування пробних X і наближуючі коефіцієнти, що формуються за допомогою розробленого методу «покриття». З урахуванням використання ρ-методу Полларда при великих відношеннях множників числа, що факторизується, комплексний метод дозволяє розкладати числа порядка 2^{110}, що перевищує відомі межі розкладання для методів Ферма, Лемана і ρ-методу Полларда.

4. Для факторизації RSA криптомодуля N при близьких його множниках запропоновано вдосконалений метод багаторазового проріджування з нерівномірним кроком, що дозволяє враховувати особливості N. На підставі оцінки кількості елементарних операцій при обмеженні на обсяг пам'яті, необхідної для зберігання 10^7 чисел типу *long* та факторизації чисел порядку 2^{1024}, запропонований метод в середньому в 10^7 раз ефективніше за метод Ферма і не менше ніж в 300 разів ефективніше методу множинного сита.

5. Запропоновано рекомендації щодо реалізації вдосконаленого алгоритму факторизації Ферма на основі технології неспеціалізованих паралельних обчислень на графічних процесорах.

Практичне значення отриманих результатів полягає у тому, що розроблені обчислювальні методи дозволяють підвищувати швидкодію апаратно-програмних засобів, що використовуються при проведенні тематичних досліджень АКА, за рахунок використання базової основи *bb*, яка формується з урахуванням значень RSA криптомодулів, що факторизуються, а також способів заміни арифметичних операцій з багаторозрядними числами на операції з числами типу *long*. Зокрема, результати роботи дозволяють:

– проектувати більш ефективні, з точки зору швидкодії, апаратно-програмні засоби проведення криптоаналізу АКА та, як наслідок, зменшити строки виконання державних експертиз у сфері КЗІ нових КА;

– здійснювати оцінку криптостійкості АКА RSA з використанням апаратно-програмної архітектури паралельних обчислень за допомогою технології GPGPU (General-purpose Computing for Graphics Processing Units).

Отримані результати складають теоретичну, методологічну та технічну основу удосконалювання існуючих і створення нових ефективних обчислювальних методів криптоаналізу АКА.

Результати роботи реалізовані в Інституті спеціального зв’язку та захисту інформації ІСЗЗІ КПІ ім. Ігоря Сікорського, Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Державному науково-дослідному інституті спеціального зв’язку та захисту інформації Державної служби спеціального зв'язку та захисту інформації України.

Особистий внесок здобувача. Всі результати дисертаційної роботи, що винесені на захист, отримані автором самостійно. У роботах, які опубліковано у співавторстві, особисто дисертантові належать: [1] – спосіб вибору ефективного початкового наближення; [4] – метод багатократного проріджування і його програмну реалізацію; [5] – порівняльний аналіз розрядного методу обчислення квадратного кореня з відомим методами і його програмна реалізація; [7] – модифікований метод «в стовпчик» для знаходження цілочисельного квадратного кореня із залишком; [8] – залежність коефіцієнта прискорення від множників базової основи модуля та алгоритм визначення нерівномірних приростів для великих значень базового модуля; [9] – метод «покриття» вибору наближуючих коефіцієнтів.

Апробація результатів дисертації. Основні ідеї та конкретні наукові результати досліджень доповідались й обговорювались на:

1. XVI – XIX Міжнародних науково-практичних конференціях "Безпека інформації в інформаційно-телекомунікаційних системах", 2013 – 2017 рр., Київ.

2. VII науково-технічній конференції "Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення", 23 – 24 жовтня 2014 р., Київ.

3. Щорічних науково-технічних конференціях молодих вчених та спеціалістів ІПМЕ Ім. Г.Є Пухова НАН України, 2014 – 2016 рр., Київ.

4. XVII Всеукраїнській науково-практичній конференції "Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2015)", 09 –12 червня 2015 р., Миколаїв.

5. XV-XVI Міжнародних науково-практичних конференціях "Інформаційні технології та безпека (ІТБ)", 2015 – 2016 рр., Київ.

6. II науково-практичній конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем", 23 – 24 березня 2017 р., Київ.

7. Науковому семінарі НАН України "Проблеми управління інформаційною безпекою", 24 лютого 2017 р., Київ.

Публікації. Основні положення, висновки і рекомендації дисертаційного дослідження опубліковані у 15 наукових роботах, з яких 9 наукових статей – у наукових журналах та збірниках наукових праць, що входять до переліку фахових видань України, у тому числі 7 – у наукових журналах, що індексуються міжнародними наукометричними базами; 6 – публікації матеріалів конференцій.

Структура та обсяг дисертації. Робота складається зі вступу, шести розділів, висновків і практичних рекомендацій, списку використаних джерел та додатків. Загальний обсяг дисертації становить 259 сторінок: 170 сторінок основного тексту (з яких 18 сторінок повністю зайнято таблицями та ілюстраціями), список із 294 використаних джерел на 27 сторінках та 10 додатків на 62 сторінках. Робота містить 56 таблиць та 28 рисунків.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовується актуальність теми дисертації, формулюються наукова задача і мета роботи, основні напрямки її вирішення і часткові задачі дослідження, зв'язок з науковими програмами, планами і темами. Визначено наукову новизну і практичне значення отриманих результатів. Наведено відомості про апробацію результатів дослідження, публікації та реалізації основних результатів, отриманих у дисертації.

Перший розділ присвячений аналізу основних напрямків використання АКА. На підставі аналізу основних сучасних протоколів, прикладних додатків, а також міжнародних і національних стандартів показано, що на даний час серед АКА домінуючи позиції в питаннях забезпечення КЗІ і ІТС де-факто займає RSA. Досліджено питання використання RSA-алгоритмів в засобах КЗІ, які мають експертний висновок за результатами державної експертизи у галузі КЗІ.

Проведено детальний аналіз нормативно-правової бази стосовно використання засобів КЗІ в Україні показав, що використання засобів КЗІ в Україні можливо тільки в разі їх допуску до експлуатації, що здійснюється на підставі тематичних досліджень, невід'ємною частиною яких є криптографічні дослідження. Оцінка криптографічних якостей АКА RSA здійснюється відомими методами криптоаналізу, які, як правило, не ефективніші за факторизацію його криптомодуля. Тому, для визначення напрямів досліджень з обраної тематики проведено аналіз сучасного стану досліджень методів факторизації АКА RSA і їх застосування при проведенні криптоаналізу.

Показано, що крім величини (числа розрядів) криптомодуля АКА RSA використання того чи іншого методу факторизації залежить від ступеня близькості

множників p і q криптомодуля N. Так, найбільш швидкими на даний час методами факторизації є QS і GNFS однак у випадку близьких множників p і q, наприклад, при помилковому формуванні RSA криптомодуля N, більш швидким може виявитись метод факторизації Ферма. При віддалених множниках N найменшою є обчислювальна складність для ρ-методу Полларда. Причому доцільно зазначити, що і QS і GNFS є різновидом так званого методу факторних баз, що є узагальненням методу факторизації Ферма. У зв'язку з цим можна стверджувати, що метод Ферма займає особливе положення серед відомих методів факторизації, а сформована наукова задача, що пов'язана з розробкою обчислювальних методів факторизації на основі алгоритму Ферма, які дозволяють підвищити швидкодію апаратно-програмних засобів при криптоаналізі АКА RSA, є актуальною.

В **другому розділі** запропоновано удосконалений метод просіювання пробних значень X з нерівномірним кроком при факторизації багаторозрядних чисел, в якому довільне зі значень X є допустимим для первинної (базової) основи модуля bb, а оцінка його допустимості проводиться тільки для додаткових основ. Запропоновано математичну постановку задачі визначення bb у вигляді нелінійного цілочисельного програмування, в якій базова основа, котра забезпечує найбільший коефіцієнт прискорення незалежно від числа N, що факторизується, шукається при обмеженнях на допустимий обсяг пам'яті. Метод удосконалює відомий метод Ферма факторизації багаторозрядних чисел, основні ідеї якого лежать в основі багатьох сучасних експоненційних і субекспоненційних методів факторизації.

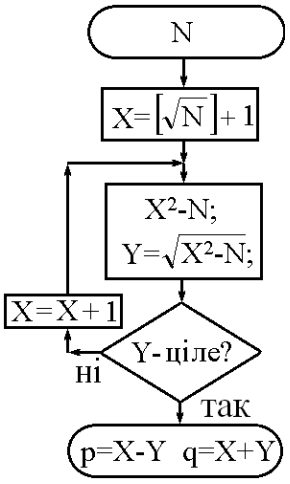

Рис. 1. Схема алгоритму методу Ферма

У методі факторизації Ферма, схема алгоритму реалізації якого представлена на рис. 1, для визначення простих множників p і q RSA криптомодуля N, шукають корінь рівняння

$$X^2 - N = Y^2, \qquad (1)$$

який при пробних X, рівних

$$X = \left(\left\lceil \sqrt{N} \right\rceil + 1\right) + x = x_0 + x, \qquad (2)$$

отримують перебором значень $x = 0, 1, 2, ...$, до тих пір, поки в (1) залишок $X^2 - N$ не виявиться квадратом цілого числа. Обчислювальна складність методу Ферма пропорційна величині x і визначається відношеннями

$$x = X - x_0 \approx (p+q)/2 - \sqrt{N} = (p+q)/2 - \sqrt{pq} = 0.5 \cdot \left(\sqrt{q} - \sqrt{p}\right)^2, \qquad (3)$$

а при $q = p \cdot (1+\alpha)^2$

$$x = X - x_0 \approx \frac{\sqrt{N}\alpha^2}{2(1+\alpha)}. \qquad (4)$$

Із аналізу (4) випливає, що зменшити обчислювальну складність методу Ферма можна за рахунок:

- виключення із аналізу частини пробних X (проріджування пробних X), для яких можна простими способами встановити, що вони не можуть бути коренями рівняння (1);
- зменшення x за рахунок α;
- спрощення процедури обчислення квадратного кореня.

В розділі 2 розглядаються способи проріджування пробних X на основі використання співвідношення

$$\left(X^2 \bmod b - N \bmod b\right) \bmod b = Y^2 \bmod b, \qquad (5)$$

де b – деяка основа модуля.

Основна ідея підходу полягає в наступному: якщо виконується (1), то для довільного b має місце рівність (5), але зворотне невірно: із виконання (5) не слідує виконання (1). Однак якщо не виконується співвідношення (5), то не буде виконуватися і (1). Тому ті пробні X, при яких не виконується (5), можна виключити з аналізу на можливість отримання кореня рівняння (1). При цьому можна значно зменшити кількість операцій обчислення квадратного кореня з $X^2 - N$ за рахунок використання множини взаємно простих модулів. Для кожного з модулів така кількість зменшується в два чи більше разів, де процедура обчислення квадратного кореня реалізується лише коли пробне значення допустиме для всіх основ модулів одночасно. Тоді основний час «витрачається» на обчислення залишків для множини основ додаткових модулів, хоча процедура аналізу пробних X здійснюється з малим постійним кроком по X, що ускладнює подальше прискорення методу Ферма.

Сутність удосконалення в розробленому методі полягає в тому, що для збільшення кроку при аналізі пробних X запропоновано виділити первинну основу *bb*, в подальшому названу базовою. Для неї формується множина *D(bb,Nmodbb)* залишків по модулю *bb* допустимих пробних X, тобто таких, що для них виконується рівняння (5), і тільки для них в подальшому здійснювати перевірку на допустимість для додаткових основ модулів. При цьому, крок між допустимими X є, як правило, нерівномірним і може бути досить великим. Середнє значення такого кроку при фіксованому *Nmodbb* в подальшому означено як коефіцієнт прискорення *z(bb, Nmodbb)*.

Для оцінки ефективності довільного з основ модуля b (включаючи і *bb*) у розділі 2 використовуються значення коефіцієнтів прискорення:

$z_{min}(b) = b/|r(b)|_{max}$, $z_{max}(b) = b/|r(b)|_{min}$, $z_{ср}(b) = b/|r(b)|_{ср}$ – мінімальне, максимальне та середнє значення, де $|r(b)|_{min}$, $|r(b)|_{max}$ та $r(b)_{ср}$ – відповідно мінімальне, максимальне та середнє значення числа елементів множини допустимих X серед всіх можливих значень $N \bmod b$, які не мають спільних дільників з b, включаючи $N \bmod b = 1$.

При оцінках обчислювальної складності алгоритмів виходять з максимально складного варіанта, який для випадку методу факторизації Ферма буде при $z(b, N \bmod b) = z_{min}(b)$. Тому при виборі основи модуля *bb*, придатної для використання для довільного *Nmodbb* важливо мати оцінку для $z_{min}(bb)$ та $z_{min}(b)$ для довільної іншої основи модуля b.

На основі використання результатів чисельних експериментів було встановлено, що в усіх проаналізованих випадках має місце співвідношення

$$z_{min}(b) = \prod_{k=1}^{n(b)} z_{min}(p_k^{m_k}), \quad (6)$$

де $p_1 = 4$, p_k $(k > 1)$ – прості числа, $m_k (k \geq 1)$ – показники степеня чисел р. При цьому для основ b, які є степенями простих чисел $p < 24$ (а також числа 4) мінімальне значення $z_{min}(b)$ при показниках p, що перевищують 2, співпадає із $z_{min}(p^2)$. Враховуючи те, що при реалізації алгоритму проріджування необхідно зберігати значення допустимих *Xmodbb*, число яких $|r(b)|_{max} = b / z_{min}(b)$, то для основ b, які є степенями простих чисел та числа 4 недоцільно використовувати показники степеня вище 2. Це дозволило сформулювати математичну постановку задачі побудови *bb*, що забезпечує найбільше серед мінімальних значень коефіцієнта прискорення, незалежно від числа *N*, яке факторизується, при обмеженні на обсяг пам'яті ЕОМ.

Математична постановка задачі вибору ефективного *bb*. Основу модуля вважатимемо ефективною, якщо вона забезпечує максимальне значення мінімального прискорення при заданому обмеженні на обсяг пам'яті ЕОМ, необхідної для зберігання інформації про допустимі значення *X* при довільних *Nmodb*, вважаючи виконаною рівність у співвідношенні (6). Тоді з урахуванням (6) задача нелінійного програмування визначається умовами:

$$\prod_{k=1}^{n(b)} z_{min}(p_k^{m_k}) \to max, \quad (7)$$

$$bb / \prod_{k=1}^{n(b)} z_{min}(p_k^{m_k}) \leq S, \quad (8)$$

де S - деяке задане значення наявного обсягу пам'яті, $p_1 = 4$, p_k $(k > 1)$ – прості числа, $m_k (k > 1)$ – показники ступеня, що не перевищують 2.

Рішення задачі (7) – (8) можливе методом повного перебору варіантів значень показників степенів чисел p, що не перевищують 2.

Удосконалений метод проріджування пробних значень через прирости. У процесі проведення досліджень було помічено, що при пошуку кореня рівняння (1) можна отримати ті ж результати, якщо використовувати не самі пробні *X*, а величину приросту між двома послідовними їх значеннями. Тоді значення остачі від ділення багаторозрядного числа *X* на деяку основу модуля b можна визначити за допомогою величини остачі від ділення приросту на b. Алгоритм зазначеного методу просіювання через прирости реалізується в наступній послідовності:

0. Попередня підготовка.

0.1. Визначення невід'ємних залишків $N \bmod bb$ і $\{N \bmod b_i\}_{i=1}^{m}$.

0.2. Для базової основи *bb* визначення $|r|_{max}(bb)$.

0.3. Визначення квадратичних залишків для *bb* (масив Mbb[bb]), та допустимих $X \bmod bb$ – множина *D(bb, Nmodbb)*. Всі такі $X \bmod bb$ визначені в діапазоні [0, *bb–1*], а їх число не перевищує значення $bb / z_{min}(bb) = |r|_{max}(bb)$. Допустимі

$X \bmod bb$ з множини *D(bb, Nmodbb)* зберігаються в масиві $Xbb[(|r|_{max}+1)]$. Оскільки при різних $N \bmod bb$ в діапазоні [0, *bb-1*] число допустимих $X \bmod bb$ різне, в клітинці *Xbb* [0] вказується фактичне значення їх числа, а самі значення записуються в порядку збільшення в клітинках від 1 до $|r|_{max}(bb)$. За їх значеннями формується послідовність приростів між допустимим $X \bmod bb$ в масиві $Xbb[\,Xbb[0]\,]$ за правилами:

$$\begin{cases} a = Xbb[1]; \\ Mbb[k] = Xbb[k+1] - Xbb[k]; (k = 1 \div (Xbb[0] - 1)); \\ Mbb[\,Xbb[0]\,] = a - Xbb[\,Xbb[0]\,] + bb. \end{cases} \quad (9)$$

0.4. Визначення допустимих $X \bmod b_i$ для основ $\{b_i\}_{i=1}^{m}$. Для кожної з них формується інформація про квадратичні залишки по модулю b_i та бінарний масив *Rb[i][t]*, в якому *Rb[i][t]* відповідає значення 1, якщо $(t^2 - N) \bmod b_i$ – квадратичний залишок по модулю b_i, а інакше 0, тобто

$$Rb[i][t\ ] = \begin{cases} 1, (t^2 - N) \bmod b_i \in M2(b_i) \\ 0, (t^2 - N) \bmod b_i \notin M2(b_i) \end{cases} (i = 1 \div m, t = 0 \div b_i - 1). \quad (10)$$

0.5. Визначення $X_0 = \lceil \sqrt{N} \rceil + 1$ і стартового *X*, рівного *Xf,* що є найближчим більшим або рівним X_0 числом, для якого $(Xf^2 - N) \bmod bb$ буде квадратичним залишком по модулю *bb*. Визначення номеру комірки i_{Xf} в масиві $Xbb[\,Xbb[0]\,]$, яка відповідає $Xf \bmod bb$.

0.6. Сумарний приріст *X* від стартового значення, число *kx*, приймається рівним 0. Значення *kx* буде обмежуватися зверху значення *kxmax*. Кожен раз, коли *kx* перевищить *kxmax*, стартове *X* буде збільшуватися на *kxmax*, а *kx* стане рівним нулю. Поточний приріст *X*, число *dx*, приймається рівним 0. Присвоїмо $X = Xf,\ i = i_{Xf}$, де *i* – поточне значення індексу для масиву *Xbb*.

1. Визначити залишки $Xf \bmod b_k$ і зберегти їх в масиві *Xb[(m+1)]*. Присвоїти *кх = 0*. Якщо всі числа $(Xf^2 - N) \bmod b_k\ (k = 1 \div m)$ є квадратичними залишками за відповідним модулем, перейти до кроку 6, а інакше до кроку 2.

2. *i=i+1*. Якщо *i=Mbb[0]*, то присвоїти *i* = 1.

3. $dx = Mbb[i]$.

4. *kx = kx + dx*.

5. У циклі по *k* від 1 до *m* перевірити виконання умови

$$Rb[k][(Xb[k] + kx) \bmod b_k\ ] = 1. \quad (11)$$

Якщо при деякому *k* виявиться, що умова (11) не виконується, тобто *X* не є квадратичним залишком по модулю b_k, перейти до кроку 7.

6. Значення $X = Xf + kx$ утворює квадратичні залишки $(X^2 - N) \bmod b\ (b = bb, b = b_k(k = 1 \div m))$ для всіх додаткових основ модулів і може бути рішенням рівняння (1). Перевірка: чи є різниця $X^2 - N$ квадратом цілого числа *Y*. Якщо так, то отримано рішення рівняння (1):*p=Xf – Y, q=Xf + Y* і робота

алгоритму завершена, а інакше визначити залишки $Xf \bmod b_k$, зберегти їх в масиві *Xb[(m+1)]*, присвоїти *kx = 0* і перейти до кроку 2.

7. Якщо $kx \geq kxmax$ перейти до кроку 1, присвоївши $Xf = Xf + кx$, а інакше перейти до кроку 2.

Схема алгоритму представлена на рис. 2.

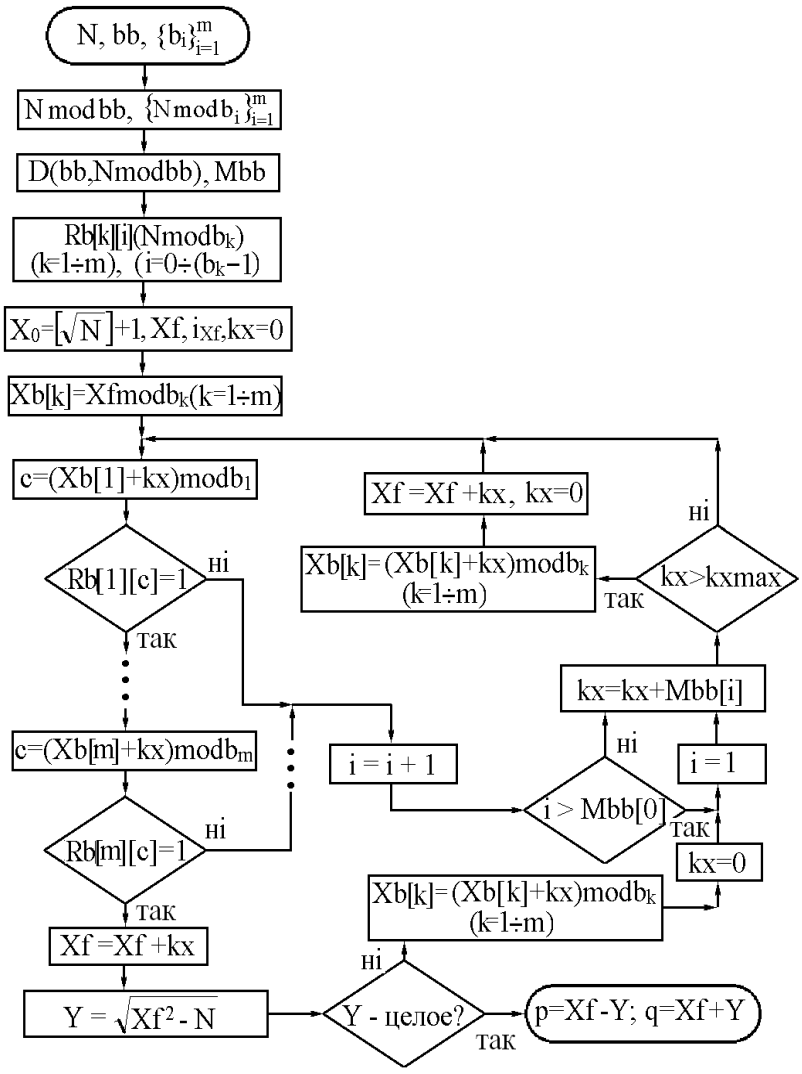

Рис. 2. Схема алгоритму модифікованого методу проріджування

У **третьому розділі** оцінено можливість використання наближуючих коефіцієнтів для прискорення методу факторизації Ферма, а також запропоновано метод вибору їх значень.

Обчислювальна складність методу Ферма визначається кількістю операцій перевірки пробних значень *X*. Їх число для методу Ферма, згідно (4), буде тим меншим, чим менше виявиться значення коефіцієнта α, чого можна домогтися, якщо замість рівняння (1) шукати корінь рівняння

$$X^2 - KN = X^2 - abN = Y^2, \quad (12)$$

де $K = a * b$ – наближуючий коефіцієнт, причому $\alpha_1 = \left|\sqrt{ap/(bq)} - 1\right|$ ближче до нуля ніж $\alpha = \left|\sqrt{q/p} - 1\right|$. Якщо такі *a* і *b*, знайдені то для $N' = ap*bq$ близькими будуть *ap* і *bq*, які можна визначити за допомогою методу Ферма.

Проведені дослідження щодо використання наближуючих коефіцієнтів для зменшення обчислювальної складності методу Ферма показали наступне:

1) При $Kmod4=2$ методом Ферма неможливо знайти цілочисельний корінь рівняння (12), а при близьких *p* і *q* RSA-криптомодуля *N* використання коефіцієнтів $K=a * b$ призводить до збільшення обчислювальної складності.

2) Використання наближуючих коефіцієнтів $K=a * b$ прискорює процес розкладання на множники при великих значеннях відношень p/q і може бути використано для удосконалення класичного методу Ферма.

Метод пошуку послідовності наближуючих коефіцієнтів $K=a * b$ реалізується запропонованим методом «покриття» в наступній послідовності:

1. При $K = 1$ знайти перше пробне *X*, при якому $q/p > 3$, після чого встановити значення $K = 3$.

2. Для фіксованого K при вирішенні рівняння $X^2 - KN = Y^2$ визначити $x_0 = \left[\sqrt{KN}\right] + 1$ и знайти x таке, що

$$\frac{q_K}{p_K} * K = \frac{x_0 + x + \sqrt{(x_0 + x)^2 - KN}}{x_0 + x - \sqrt{(x_0 + x)^2 - KN}} * K > K + m_K , \qquad (13)$$

де m_K – деяке ціле парне число;

3. Непарне значення K збільшувати на величину не меншу ніж m_K до тих пір, поки не знайдено корінь рівняння (1).

Доведено, що процес збільшення цілочисельних непарних значень K гарантує отримання рішення рівняння (1).

В четвертому розділі вирішується ряд завдань, пов'язаних з чисельною реалізацією методу багатократного проріджування МП, методу «покриття», їх спільного використання та чисельним експериментам. Вирішується також задача формування комплексного методу факторизації, в якому крім методів МП та «покриття» при великих значеннях співвідношень q / p $(q > p)$ використовується ρ-метод Полларда та розроблений модифікований метод обчислення цілочисельного значення кореня з остачею «в стовпчик».

Чисельна реалізація методу МП. При чисельній реалізації методу використовувалось подання великих чисел N послідовністю розрядів розкладання N за деякою основою числення b_0. Якщо

$$N = \sum_{i=0}^{m(N)} c_i b_0^i , \qquad (14)$$

то інформація про число N задається масивом, в нульовій клітинці якого вказано кількість елементів масиву, що дорівнює $m(N)+1$, які описують число N, а в клітинках і (i=1÷$m(N)$+1) – числа c_{i-1}. Так у випадку числа N = 235691 та основи системи числення b_0 = 60 $N = 11 + 28 \cdot 60 + 5 \cdot 60^2 + 1 \cdot 60^3 = c_0 + c_1 \cdot b_0^1 + c_2 \cdot b_0^2 + c_3 \cdot b_0^3$, $m(N)$=3, а елементами масиву *Mas* будуть числа: *Mas*[0]=4; *Mas*[1]=11; *Mas*[2]=29; *Mas*[3]=5; *Mas*[4]=1.

В загальному виді масив типу Mas формується за правилами:

$$Mas[i] = \begin{cases} i = 0: \quad Mas[0] = m(N) + 1, \\ i = 1 \div m(N) + 1: \quad Mas[i] = c_{m(N)+1-i} , \end{cases} \qquad (15)$$

а арифметичні операції над числами зводяться до арифметичних операцій над елементами масивів типу *Mas* з урахуванням переносу розрядів.

При проведенні чисельних експериментів формувалась множина значень чисел, для яких близькими до $2^{1/4}$ є відношення наступного до попереднього. На їх основі будувались N такі, що при bb = 277200 число допустимих пробних X – елементів множини *Xbb* – дорівнює максимально можливому значенню $|r(bb)|_{max}$ = 2880 для, а коефіцієнт прискорення $z(bb,Nmodbb) = z_{min}(bb)$ = 96.25. Число додаткових основ m =14. Їх значення наведено в таблиці 1.

Таблиця 1.

Додаткові основи b_k ($k = 1 \div m$) і їх прості множники

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14
b_k	4199	2461	2987	3131	3589	3649	3569	3713	3869	4189	4087	109	113	127
Множники b_k	13 17 19	23 107	29 103	31 101	37 97	41 89	43 83	47 79	53 73	59 71	61 67	109	113	127

На першому етапі ставилась задача визначення найменших значень $N=p*q$ таких, що $q \le 4p$, а час розкладання t на множники числа N перевищував 1000 секунд для ПК з характеристиками: тактова частота 2.4 GHz, ОЗП 6 ГБ, 32-розрядна операційна система. Результати для $q \le 2p$ представлено в табл. 2.

Таблиця 2.

Мінімальні N при різних значеннях q / p для яких $t > 1000$

q/p	N	x	l_{sqrt}	t, c
$2^{0.25}$	21901077424364047404871524279 83	5 558 342 544 918	732	1103
$2^{0.5}$	11510335725869974368123931928 3	5 106 595 343 108	750	1039
$2^{0.75}$	24197500008691435623032029847	5 284 605 435 652	996	1180
2	71939597119470617183335226 87	5 145 026 742 943	777	1057

В табл. 2 величина x – це фактичне значення числа пробних X для методу Ферма, l_{sqrt} – кількість «перевірочних» обчислень кореня.

На основі даних про час розкладання на множники таких чисел встановлено, що час обчислень пропорційний $x = (p+q)/2 - \left\lceil \sqrt{N} \right\rceil$ незалежно від співвідношення q/p. В подальшому було оцінено ефективність запропонованих методів в залежності від обраних базової та додаткових основ при реалізації процедури просіювання.

При дослідженнях впливу значення базової основи bb на час розкладання виявилось, що при використанні $bb = 25200$ (25200 = 277200/11) час обчислень збільшувався в середньому в 1.77 рази, а при $bb = 3600$ (3600 = 277200/11/7) – в середньому в 3.11 рази. Для коректності порівняння результатів сумарне число простих чисел в bb та додаткових основах модулів залишалося незмінним. Для цього при bb=25200 додаткова основа b_{12}=109 була замінена на $b'_{12} = 1199 = 109 * 11$, а при $bb=3600$ змінювались основи $b_{12}=109$ на $b'_{12} = 1199 = 109 * 11$ та $b_{13}=113$ на $b'_{13} = 791 = 113 * 7$. Отримані результати дозволили зробити висновок про те, що домінуючу роль у зниженні обчислювальної складності модифікованого методу Ферма відіграє $z_{min}(bb)$, яка пропорційно зменшується при збільшенні $z_{min}(bb)$.

При оцінці впливу додаткових основ встановлено, що на час факторизації впливає не саме число основ, а кількість простих множників, які формують ці основи. При зменшенні числа простих множників у додаткових основах збільшується час обчислень за рахунок збільшення кількості обчислень квадратного кореня в середньому в 2^c раз, де c – число простих множників.

Особливості спільного використання методів проріджування та наближуючих коефіцієнтів. Проведені чисельні експерименти з визначення коефіцієнтів прискорення для *bb*, що містять прості множники, наявні в наближуючому коефіцієнті *K*, показали, що довільна їх степінь в *bb* не змінює *z(bb,Nmodbb)*, а тільки збільшує число пробних *X,* допустимих для *bb*. Тому при розробці методу факторизації, що враховує алгоритми методів МП та «покриття» доцільно при кожній зміні наближуючого коефіцієнта *K* перевіряти наявність спільних дільників у *K* та *bb*. За їх наявності доцільно змінити базову основу *bb* та додаткові основи і використовувати їх для діапазону *xx* пробних *X* навіть для випадків, коли виконується умова (13). При кожній зміні наближуючого коефіцієнта *K* необхідно отримувати значення початкового наближення для методу Ферма відповідно до (2), що потребує обчислення квадратного кореня з остачею для числа *KN*. Тому в роботі розглядалася задача розробки ефективного способу обчислення квадратного кореня з багаторозрядного числа.

Модифікований метод «в стовпчик» обчислення квадратного кореня з багаторозрядних чисел. В методі «в стовпчик» здійснюється послідовне обчислення значень розрядів числа, що є цілочисельним значенням квадратного кореня, при якому значення розряду визначається в результаті операції ділення. Суть запропонованого модифікованого методу «в стовпчик» полягає в тому, що при визначенні значення розряду операція ділення багаторозрядних чисел замінюється на операцію ділення малих чисел (типу *double*). Проведені чисельні експерименти для отримання порівняльних характеристик модифікованого методу «в стовпчик» із іншими методами показали, що для чисел до 2^{140} запропонований метод характеризується значно меншою обчислювальною складністю в порівняння з іншими проаналізованими методами, у якому всі операції виконуються з числами типу *long* та *double*, що дозволяє використовувати його на довільному комп'ютері без додаткових бібліотек для роботи з великими числами.

Комплексний метод факторизації на основі методів МП, «покриття» та ρ-методу Полларда. Для оцінки граничних значень чисел N, які можна розкласти на множники на звичайному комп'ютері за допомогою комплексного методу факторизації, що включає методи МП, «покриття» при $q/p < N^{1/5}$ і ρ-метод Полларда для відношеннях $q/p \geq N^{1/5}$. Отримано верхню та нижню оцінки для сумарного числа блоків довжиною *xx*, необхідних для розкладання на множники числа *N*. Довжина блоку вибиралась такою, що з урахуванням проріджування пробних значень час роботи комп'ютера для аналізу пробних *X* одного блоку дорівнював 1 секунді при коефіцієнті прискорення $z_{min}(bb)$=337.639. На основі цих даних зроблено висновок про те, що за допомогою даного комплексного методу можливо розкласти на множники число порядку 2^{110}, що перевищує відомі границі використання методів Ферма, Лемана та ρ-метод Полларда.

Для ρ-методу Полларда, при аналізі близько $2*10^6$ варіантів чисел *N*, менших за 10^9, було виявлено, що для забезпечення його збіжності може знадобитися багаторазова заміна відображення $f : Z/(N) \rightarrow Z/(N)$ виду $f(x)= x^2 - c$, а за рахунок вибору початкового наближення обчислювальна складність методу може зменшуватись більш ніж на третину.

П'ятий розділ присвячений удосконаленню алгоритму МП на основі вибору базової основи модуля *bb*, максимальної для *Nmodbb* при заданих обмеженнях на обсяг доступної пам'яті ЕОМ. В розділі розглядаються питання оцінки впливу *Nmodbb* на величину прискорення *z(bb, Nmodbb)*, вибору показників степеня простих чисел – множників bb в залежності від росту *z(bb, Nmodbb)* при збільшенні показників степеня на одиницю показника та порівняння обчислювальної складності алгоритму удосконаленого методу МП з алгоритмами методів Ферма, Лемана та сита.

Оцінка впливу *Nmodbb* на величину прискорення *z(bb, Nmodbb)*. На основі чисельних експериментів виявлено такі закономірності у значеннях *z(bb,Nmodbb)* при зміні показників степеня простих *p* – множників *bb*:

1. величина *z(bb,Nmodbb)* визначається значеннями показників степенів *t* простих чисел *p* – множників *bb* для кожного з простих p незалежно;

2. значення $z(p^k,Nmodp)$ при $p > 2$ визначаються всього двома підмножинами величин Nmodp: для першої з них, що містить значення $Nmodp = 1$, коефіцієнт прискорення $z(p,Nmodp) = z_{min}(p)$ та значення $z(p^k,Nmodp)$ ростуть з ростом *k*; для другої відносяться ті *Nmodp*, для яких $z(p,Nmodp) = z_{max}(p)$ залишаються незмінними для довільних *k*;

3. значення $z(2^k,Nmod8)$ при $k > 2$ визначаються всього трьома підмножинами величин *Nmod8*, для першої з яких $z(2^k,Nmod8) = 4$ при $k > 2$ та $Nmod8 = 3$ чи $Nmod8 = 7$; для другої $z(2^k,5) = 8$ при $Nmod8 = 5$ та $k > 4$; для третьої при $Nmod8 = 1$ значення $z(2^k,1)$ змінюються з ростом *k*.

Визначено значення *Nmodp*, що відповідають підмножинам п.2.

Вибір показників степенів простих чисел – множників bb в залежності від росту z(bb, Nmodbb) при збільшенні показників степеня на одиницю. В залежності від *Nmodp* з ростом показника степеня *t* може змінюватися $z(p^t,1)$. Для таких випадків необхідно визначити діапазон значень *t*. Для цього запропоновано використовувати характеристичну функцію відносного приросту коефіцієнта прискорення

$$s(p,t) = (z(p^{t+1},1) / z(p^t,1) - 1) / p, \qquad (16)$$

де при близьких до нуля значеннях $s(p,t)$ збільшення *bb* в p раз забезпечує незначний ріст коефіцієнта прискорення, проте суттєво зростає обсяг необхідної пам'яті ЕОМ, що використовується для зберігання приростів для допустимих *X*. Тому на основі сортування значень $s(p,t)$ в порядку спадання можна визначити значення максимальних величин показників степенів множників p для шуканої базової основи *bb*.

З урахуванням такої інформації формулюється математична постановка задачі пошуку *bb*, для якого максимальним буде коефіцієнт прискорення $z(bb,Nmodbb)$ при обмеженнях на обсяг доступної пам'яті ЕОМ. Для цього використовується інформація про структуру *bb* ($bb = \prod_{i=1}^{h} p_i^{k_i}$), властивості коефіцієнтів прискорення

$((z(bb,N)=\prod_{i=1}^{h} z(p_i^{k_i},N))$ та число елементів множини $D(bb,Nmodbb)$ $(r(bb,N)=bb/z(bb,N)=\prod_{i=1}^{h} p_i^{k_i}/z(p_i^{k_i},N))$.

Задачу цілочисельного нелінійного програмування пошуку bb, для якого забезпечується максимальне значення $z(bb,N\,mod\,bb)$ при обмеженні на обсяг наявної пам'яті ЕОМ

$$\prod_{k=1}^{n(b)} z(p_k^{m_k}) \to max, \tag{17}$$

$$bb/\prod_{k=1}^{n(b)} z(p_k^{m_k}) \le RAM, \tag{18}$$

пропонується вирішувати методом повного перебору показників степенів простих p – можливих множників bb, множина яких визначена на основі їх вибору, при якому $s(p,t)$ перевищує деяку мінімальну величину.

Для практичного вирішення задачі (17) – (18) за умов, що $p \le 23$, значення доступного обсягу пам'яті Zq_{max}, що відповідають кількості чисел типу *long*, рівні 10^3, 10^5, та 10^7 були сформовані множини показників степенів p при $s(p,t) > 0.033$. За допомогою розробленого програмного додатку були визначені всі варіанти значень bb, для яких при відомому Nmodbb забезпечується максимальне значення коефіцієнта прискорення, а серед всіх цих варіантів виділено величини $z_{min}(bb, Nmodbb)$, $z_{max}(bb, Nmodbb)$ та середнє $z(bb, Nmodbb)$. Результати обчислень наведено в табл. 3.

Таблиця 3.

Значення z_{min} , z_{max} та z_{cp} для ряду граничних значень Zq_{max}

Zq_{max}	z_{min}	$Zq(z_{min})$	$bb(z_{min})$	z_{max}	$Zq(z_{max})$	$bb(z_{max})$	z_{cp}
10^3	213.57	924	394680	1386	960	2661120	579.73
10^5	822.83	92736	152612460	9572.06	92160	1764322560	2976.53
10^7	2407.28	8814960	42440137740	42252.44	9123840	771008958720	11088.62

На основі оцінки числа елементарних операцій при обсязі доступної пам'яті 10^7 чисел типу *long* (40 МВ) та при розкладанні на множники чисел порядку 2^{1024} встановлено, що удосконалений метод многократного проріджування МП в 10^7 раз ефективніше методу Ферма та не менш ніж у 300 раз ефективніше методу множинного сита.

У **шостому розділі** проведено обґрунтування та розроблено науково-технічні рекомендації з апаратно-програмної реалізації запропонованих методів при проведенні криптоаналізу RSA-алгоритму.

Проведено аналіз сучасних прикладів використання технологій і розподілених обчислень при факторизації багаторозрядного числа. Показано, що найбільш ефективним напрямом реалізації проведення криптоаналізу АКА RSA є GPGPU – технологія неспеціалізованих паралельних обчислень на графічних процесорах, яка дозволяє розробникам ПО використовувати потокові процесори для

неграфічних даних. Встановлено, що для апаратно-програмної реалізації запропонованих методів факторизації можна ефективно використовувати архітектуру паралельних обчислень CUDA від компанії NVIDIA. Наведено аналіз використання апаратно-програмної архітектури CUDA в задачах факторизації. Запропоновано алгоритм розробленого комплексного методу факторизації багаторозрядних чисел при його апаратно-програмній реалізації на графічних процесорах NVIDIA.

У **висновках** викладені найбільш вагомі наукові і практичні результати, отримані в дисертації, їх значення для науки і практики, сформульовані вирішена наукова задача і методи, використані при її вирішенні. Обґрунтовується вірогідність отриманих результатів і дано рекомендації з їх наукового і практичного застосування.

У **додатку** містяться відповідні акти, що підтверджують практичне використання результатів дисертаційної роботи в ІСЗЗІ КПІ ім. Ігоря Сікорського, Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, а також Державному науково-дослідному інституті спеціального зв'язку та захисту інформації Державної служби спеціального зв'язку та захисту інформації України та інші додаткові матеріали.

ВИСНОВКИ

У дисертації отримано теоретичне узагальнення і нове вирішення наукової задачі, що полягає в розробці методів факторизації на основі алгоритму Ферма, що дозволяють підвищити швидкодію апаратно-програмних засобів, які використовуються при криптоаналізі АКА RSA за рахунок створення більш ефективних методів проріджування і зменшення обчислювальної складності операцій з багаторозрядними числами.

Основні наукові і практичні результати роботи полягають у наступному:

1. Вперше розроблено метод проріджування пробних значень невідомої X з нерівномірним кроком, в якому запропоновано використання базової основи модуля bb, для якої одноразово визначається множина коренів модульного рівняння, за рахунок чого формуються всі допустимі для bb пробні X, оцінка допустимості яких проводиться для додаткових основ модулів. За рахунок формування списку коренів модульного рівняння для bb суттєво зменшено кількість пробних значень X, які аналізуються за допомогою додаткових модулів, а розроблений метод їх подання у вигляді приростів дозволяє уникнути виконання арифметичних операцій з багаторозрядними числами, замінивши їх операціями з числами типу *long*.

2. Вперше сформульовано математичну постановку задачі визначення первинної (базової) основи bb з максимальним коефіцієнтом прискорення для заданого криптомодуля N, що факторизується, при обмеженні на максимально допустиму величину наявного обсягу пам'яті ЕОМ, як задачу нелінійного цілочисельного програмування. Показано, що її рішення можна отримати методом повного перебору показників степенів простих чисел – множників bb, де множина таких показників для довільного з простих множників bb визначається на основі оцінки відносної зміни коефіцієнта прискорення.

На основі чисельних експериментів встановлено, що зменшення обчислювальної складності методу Ферма пропорційно коефіцієнту прискорення для *bb*, як відношення можливих X до числа допустимих для *bb*. Тому запропонований спосіб отримання максимально можливого коефіцієнта прискорення при врахуванні обмежень на наявну пам'ять ЕОМ дозволяє знизити обчислювальну складність методу Ферма.

3. Запропоновано комплексний метод факторизації чисел, в якому використовується багаторазове проріджування пробних X і наближуючих коефіцієнтів K, що формуються на підставі розробленого методу «покриття». З урахуванням використання ρ-методу Полларда при великих відношеннях множників числа, що факторизується, запропонований метод дозволяє розкладати числа порядку 2^{110}, що перевищує відомі межі розкладання для методів Ферма, Лемана і ρ-методу Полларда.

4. Запропоновано алгоритм MPbb для забезпечення роботи з великими основами модуля *bb* при використанні чисел типу *long*.

5. Для факторизації криптомодуля N RSA-алгоритму при близьких його множниках запропоновано вдосконалений метод багаторазового проріджування з нерівномірним кроком, що дозволяє враховувати особливості N. На підставі оцінки числа елементарних операцій при обмеженні на розмір пам'яті, необхідної для зберігання 10^7 чисел типу *long* та факторизації чисел порядку 2^{1024}, запропонований метод в середньому в 10^7 раз ефективніше методу Ферма і не менше ніж в 300 разів ефективніше методу множинного сита при послідовній організації обчислень.

6. Запропоновано рекомендації щодо реалізації вдосконаленого алгоритму факторизації Ферма на базі технології неспеціалізованих паралельних обчислень на графічних процесорах.

Таким чином, розроблені обчислювальні методи та запропоновані науково-технічні рішення в сукупності дозволяють підвищити швидкодію апаратно-програмних і програмних засобів, що використовуються оцінюванні криптостійкості АКА RSA. Це має важливу наукову й практичну спрямованість при удосконаленні існуючих та створенні нових засобів для проведення тематичних досліджень для допуску до експлуатації КЗІ, що використовують АКА.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Максименко Е.В. Оценка вычислительных затрат ρ-метода Полларда в зависимости от выбора отображения и начального приближения для малых факторизуемых чисел / С.Д. Винничук, Є.В. Максименко, В.М. Мисько // Захист інформації. – 2014. – Том 16, № 4. – С. 263-268.

2. Максименко Е.В. Особенности реализации процедуры умножения больших чисел в ортогональных базисах / Е.В. Максименко // Моделювання та інформаційні технології. – 2015. – Вип. 74. – С. 49-56.

3. Максименко Е.В. Способ эффективного использования приращений при многократном прореживании пробных значений для метода факторизации Ферма // Information Technology and Security. – 2016. – Том. 4, №. 1. – С. 91-99.

4. Максименко Е.В. Многократное прореживание для ускорения метода факторизации Ферма при неравномерных шагах для неизвестной / С.Д. Винничук, Е.В. Максименко // Вісник НТУУ “КПІ”. Інформатика, управління та обчислювальна техніка: Зб. наук. пр. – К.: Век+. – 2016. – № 64. – С. 13-24.

5. Максименко Е.В. Использование разрядной модели двоичного представления квадрата числа в процедурах вычисления квадратного корня / Е.В. Максименко, В.В. Мохор // Моделювання та інформаційні технології. – 2016. – Вип. 76. – С. 134-142.

6. Максименко Є.В. Вибір ефективної базової основи модуля при багаторазовому проріджуванні пробних значень в методі факторизації Ферма з нерівномірним кроком // Інформатика та математичні методи в моделюванні. Одесса. – 2016. – Том 6. – № 3.– С. 270-279.

7. Максименко Е.В. Методы извлечения корня с остатком из многоразрядных чисел для решения задач ассиметричной криптографии / С.Д. Винничук, А.В. Корнейко, Е.В. Максименко // Захист інформації. НАУ. – 2016. – Том 18, №4. – С. 336-345.

8. Максименко Е.В. Формирование неравномерных приращений для базового основания модуля в задаче факторизации методом Ферма / С.Д. Винничук, Е.В. Максименко // Information Technology and Security. – 2016. – Том. 4, № 2. – С. 245-254.

9. Максименко Е.В. Ускорения метода факторизации Ферма на основе использования приближающих коэффициентов / С.Д. Винничук, Е.В. Максименко // Сучасний захист інформації. – 2017. – №1. – С.79-88.

10. Максименко Є.В. Дослідження особливостей застосування ρ-методу факторизації Полларда / С.Д. Винничук, І.П. Кисиленко, Є.В. Максименко // VII науково-технічна конференція “Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”. м. Київ, ВІТІ. 23-24 жовтня 2014 р. – 75 с.

11. Максименко Є.В. “Метод прямого вычисления квадратных корней” / Є.В. Максименко // Щорічна науково – технічна конференція молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України. м. Київ. 12 січня 2016 р.

12. Максименко Є.В. Уточнена оцінка часової складності методу Ферма. / С.Д. Винничук, Є.В. Максименко // XVIII міжнародна науково-практична конференція "Безпека інформації в інформаційно-телекомунікаційних системах”. м. Київ. Держспецзв’язку України, 25-26 травня 2016 р. – 70 с.

13. Максименко Е.В. Модифицированный метод факторизации Ферма и исследование его предельных свойств. / Е.В. Максименко / XVI Международная научно-практическая конференция ІТБ-2016 “Информационные технологии и безопасность”. м. Київ. ІПРІ НАН України. 1 грудня 2016 р. – 194 с.

14. Максименко Е. В. Ускорение метода факторизации Ферма на основе использования приближающих коэффициентов / С. Д. Винничук, Е. В. Максименко // ІІ Науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем”. м. Київ. Київський національний університет імені Тараса Шевченка. 23-24 березня 2017 р. – 33 с.

15. Максименко Є.В. Удосконалений метод факторизації Ферма / Є.В. Максименко // XIX міжнародна науково-практична конференція “Безпека інформації в ІТС”. м. Київ. Державна служба спеціального зв’язку та захисту інформації України. 25-26 травня 2017 р. – 115 с.

АНОТАЦІЯ

Максименко Є.В. Обчислювальні методи на основі алгоритму Ферма при криптоаналізі RSA алгоритму апаратно-програмними засобами. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.02 – математичне моделювання та обчислювальні методи. – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова, Київ, 2017.

Дисертаційна робота Максименка Є.В. присвячена удосконаленню обчислювальних методів факторизації на основі алгоритму Ферма, які використовуються при проведенні досліджень криптоалгоритмів та протоколів, що застосовуються в засобах та комплексах криптографічного захисту інформації на основі створення більш ефективних методів проріджування і зменшення обчислювальної складності операцій з багаторозрядними числами. Новими науковими результатами, отриманими в дисертаційній роботі, є модифікованих метод проріджування пробних значень X з нерівномірним кроком в процедурах факторизації багаторозрядних чисел методом Ферма, спосіб представлення яких у вигляді приростів для аналізу дозволяє уникнути виконання арифметичних операцій з багаторозрядними числами, замінивши їх операціями з числами типу *long*. Крім того, запропонований метод дозволяє враховувати особливості чисел, що факторизуються. На підставі оцінки числа елементарних операцій при обмеженні на розмір пам'яті, необхідної для зберігання 10^7 чисел типу *long* та факторизації чисел порядку 2^{1024}, запропонований метод в середньому в 10^7 раз ефективніше класичного методу Ферма і не менше ніж в 300 разів ефективніше методу множинного сита. Результати роботи дозволяють підвищити швидкодію апаратно-програмних засобів, які використовуються для проведення тематичних досліджень засобів криптографічного захисту інформації і протоколів на основі RSA-алгоритму.

Ключові слова: факторизація, багаторозрядні числа, метод Ферма, RSA, метод просіювання, модульні операції, асиметричний криптоалгоритм, криптоаналіз.

ABSTRACT

Maksymenko Yevhen. The Computational methods based on the algorithm of Fermat's factorization method during cryptanalysis of RSA algorithm by hardware and software methods. – As the manuscript.

Dissertation on competition of scientific degree of bachelor of science on speciality 01.05.02 – mathematical modeling and computing methods. – National Academy of Sciences of Ukraine, Pukhov Institute of Modeling in Energy Engineering. Kyiv, 2017.

Yevhen Maksymenko’s dissertation is devoted to the improvement of computing factorization methods based on the Fermat’s algorithm, which are used in the research of cryptographic algorithms and protocols which are used in the means and complexes of cryptographic protection of information (CPI) based on the creation of more effective

methods of thinning and reducing the computational operations of complex multi-digit numbers. New scientific results obtained in the dissertation are the modified method of screening the test values of X with an uneven step in the procedures of factorizing multi-digit numbers by the Fermat's method, the method of representation which in the form of increments for analysis avoids performing arithmetic operations with multi-digit numbers, replacing them by operations with numbers of the type '*long'*. In addition, the proposed method allows us to take into account the features of factorizing numbers. On the basis of the estimation of the number of elementary operations, limiting the memory size needed to store 10^7 numbers of the type '*long'* and factorizing the numbers of order 2^{1024}, the proposed method is on average 10^7 times more effective than the classical Fermat's method and at least 300 times more efficient than the multiple sieve method. The results of the work allow to increase the speed of hardware and software which are used for cryptographic analysis RSA AKA.

Keywords: factorization, multi-digit numbers, Fermat's method, RSA, sieve method, modular operations, asymmetric cryptographic algorithm, cryptographic analysis.

АННОТАЦИЯ

Максименко Е.В. Вычислительные методы на основе алгоритма Ферма при криптоанализе RSA алгоритма аппаратно-программными средствами. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 01.05.02 – математическое моделирование и вычислительные методы. – Институт проблем моделирования в энергетике им. Е. Пухова, Киев, 2017.

Обязательным условием обработки информации с ограниченным доступом в национальных информационно-телекоммуникационных системах является применение средств технической и/или криптографической защиты информации. Допуск таких средств к эксплуатации принимается по результатам тематических исследований, одним из элементов которых является оценка криптографической стойкости криптоалгоритмов и протоколов, используемых в объектах исследований.

В настоящее время достаточно широкое применение получили криптографические системы, построенные на асимметричных криптоалгоритмах, наиболее распространенным среди которых считается алгоритм RSA. Известно, что криптографическая стойкость RSA-алгоритма основана на сложности решения задачи разложения на множители его криптомодуля – задачи факторизации.

Диссертационная работа Максименко Е.В. посвящена совершенствованию вычислительных методов на основе алгоритма Ферма, используемых при проведении исследований криптоалгоритмов и протоколов. Основными научными результатами проведенных исследований являются: 1. Метод многократного прореживания пробных значений неизвестной X с неравномерным шагом, в котором предложено использование первичного базового основания модуля. Данное решение позволило существенно уменьшить количество допустимых пробных значений X, анализируемых с помощью дополнительных оснований. Кроме того, предложенный метод прореживания позволяет учитывать особенности факторизуемого числа для случая близких значениях его множителей. 2. Метод определения значения базового основания модуля с максимальным коэффициентом

ускорения для факторизуемого числа при ограничении на максимально допустимую величину объема памяти ЭВМ. 3. Метод представления допустимых пробных X в виде приращений, позволяющий все операции с многоразрядными числами заменить на операции с числами типа *long*.

На основании оценки числа элементарных операций при ограничении на размер памяти, необходимой для хранения 10^7 чисел типа *long* и факторизации чисел порядка 2^{1024}, предложенный комплексный метод в среднем в 10^7 раз эффективнее классического метода Ферма и не менее чем в 300 раз эффективнее метода множественного сита.

Результаты работы позволяют повысить быстродействие аппаратно-программных средств, применяемых при проведении тематических исследований средств криптографической защиты информации и протоколов, основанных на использовании RSA-алгоритма.

Ключевые слова: факторизация, многоразрядные числа, метод Ферма, RSA, метод прореживания, модульные операции, асимметричный криптоалгоритм, криптоанализ.