УДК 004.056.55

І. П. Кулібабчук

ЕМПІРИЧНЕ ДОСЛІДЖЕННЯ СТІЙКОСТІ ОДНОЇ МОДЕЛІ КРИПТОСИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ

Вінницький національний технічний університет;

Анотація

За допомогою середовища системи комп'ютерної математики Maple наочно продемонстровано проблеми факторизації великих цілих чисел. Шляхом обчислювальних експериментів показано, що час факторизації для числа, що є добутком двох великих простих чисел зростає із збільшенням довжини цього числа. Для чисел довжиною >35 швидкість зміни вказаної залежності починає швидко збільшуватися. Тим самим підтверджено надійність алгоритму шифрування з відкритим ключем.

Ключові слова: факторизації цілих чисел, добуток двох простих чисел, алгоритм шифрування методом RSA, Maple.

Abstract

With the help of the Computer Algebra System Maple, problems of factorization of large integers are clearly demonstrated. By computational experiments it has been shown that the factorization time for a number, is the product of two large primes, increases with increasing length of this number. For numbers of length> 35, the rate of change of the indicated dependence begins to increase rapidly. This confirms the cryptoresistability of the public key encryption algorithm.

Keywords: integer factorization, product of two prime numbers, RSA encryption algorithm, Maple.

Вступ

Стійкість криптографічних алгоритмів з відкритим ключем (асиметричних алгоритмів) базується на існуванні односпрямованих функцій [1]. До односпрямованих відносять функції $F(x)$, що задовольняють дві властивості:

– існує алгоритм з поліноміальним часом обчислення значень $y = F(x)$;

– не відомий поліноміальний алгоритм інвертування функції $F(x) = y$.

Одною з найбільш відомих систем з відкритим ключем є криптосистема RSA. Стійкість цієї системи пов'язана з так званою проблемою факторизації цілих чисел. Питання про існування алгоритму факторизації з поліноміальною складністю на класичному комп'ютері є однією з важливих відкритих проблем сучасної теорії чисел [1].

Описання алгоритму шифрування методом RSA можна знайти в багатьох джерелах, зокрема в [1].

Для першого знайомства з проблемою факторизації великих цілих чисел бажано мати наочні розв'язки конкретних задач.

Метою роботи є розробка алгоритму та його програмної реалізації для емпіричного дослідження задачі факторизації великих цілих чисел.

Результати дослідження

Для дослідження задачі факторизації великих цілих чисел необхідно вибрати програмне середовище.

У працях [2, 3, 4, 5, 6, 7, 8, 9, 10, 11] продемонстровано ефективність використання системи комп'ютерної математики (СКМ) Maple під час розв'язання широкого кола типових задач вищої математики.

Автори [11] зазначають «Однією з найбільш популярних систем комп'ютерної алгебри є система Maple, фірми Waterloo Maple, Inc., яка успішно поєднує символьні маніпуляції, обчислювальну математику, потужну графіку та зручну мову програмування». Поступово подібні системи стають «незамінним інструментом наукових досліджень для студентів, інженерів та дослідників. Проте на

даний час ці технології, незважаючи на свою ефективність та наочність, в силу різних причин, ще недостатньо поширені в навчальному процесі, що не сприяє інтеграції системи вищої освіти України у світовий простір вищої освіти».

Отже, середовище цієї системи цілком придатне для нашого дослідження.

СКМ Maple має стандартну функцію *ifactor* для розкладання цілого числа на прості множники. Приклади роботи цієї функції:

```
printf("Задаємо деяке ціле число n. Це можна зробити, наприклад, за
допомогою одного або двох відомих в теорії простих чисел співвідношень");
m=2^k+1;
n=m^2 - 79*m + 1601;
subs(n=2^39+1,n^2 - 79*n + 1601);
#print(length(%));
ifactor(%);
```

Задаємо деяке ціле число n. Це можна зробити, наприклад, за допомогою одного або двох відомих в теорії простих чисел співвідношень

$$m = 2^k + 1$$

$$n = m^2 - 79\,m + 1601$$

$$302231454861326096008691$$

$$(302231454861326096008691)$$

Для обчислення часу здійснення операцій в Maple використовується оператор time:

```
restart:
st:=time():
ifactor(725029762643432902359146696328827429471525302136680105935630195782720124747256629577928036026 7);
time()-st;
```

$$(31)\ (47)\ (221073919720733357899783)^3\ (473638939)^2\ (2053)$$

$$5.907$$

Отже, факторизація заданого цілого числа довжиною

```
length(725029762643432902359146696328827429471525302136680105935630195782720124747256629577928036026 7);
```

$$94$$

в середовищі Maple 9 на комп'ютері з процесором Intel® Core™ i5-4460 CPU @ 3.20GHz триває приблизно 6 сек. Звичайно це не означає, що для будь-якого цілого числа вказаної довжини тривалість операції факторизації буде такою самою або близькою. Цей факт демонструє приклад

```
restart:
932096485652802705563317 9*37425500205579491305090 09;
print(length(%));
st := time():
ifactor(%%);
time()-st;
```

$$34884177215418889024825337696077048345745058809611$$

$$50$$

$$(37425500205579491305090 09)\ (932096485652802705563317 9)$$

$$255.097$$

Тобто для цілого числа майже вдвічі меншої довжини тривалість операції факторизації зросла приблизно в 42 рази. Цей приклад демонструє , що розв'язання задачі факторизація числа, що є добутком двох великих простих чисел, вимагає значних обчислювальних ресурсів.

Слід підкреслити, що в порівнянні с задачею факторизації цілого числа задача розпізнавання

простоти числа є значно простішою, тобто за рівних інших умов виконується значно швидше:

```
restart:
st := time():
isprime(348841772154188890248253376960770483457450588809611);
time()-st;
```

$$false$$

$$0.$$

Слід зазначити, що в інтернеті запропоновано багато неякісних сервісів для здійснення операцій, що розглядуються, наприклад, на сайті https://planetcalc.ru/3754/ число (див. рис. 1.)

348841772154188890248253376960770483457450588809611

було подано увигляді добутку простих множників **2^{113}*178603*18808329503**, що насправді є іншим цілим числом

34884177215418888506482122325625646457804269027328

Отже, користуватися потрібно тільки перевіреними сервісами.

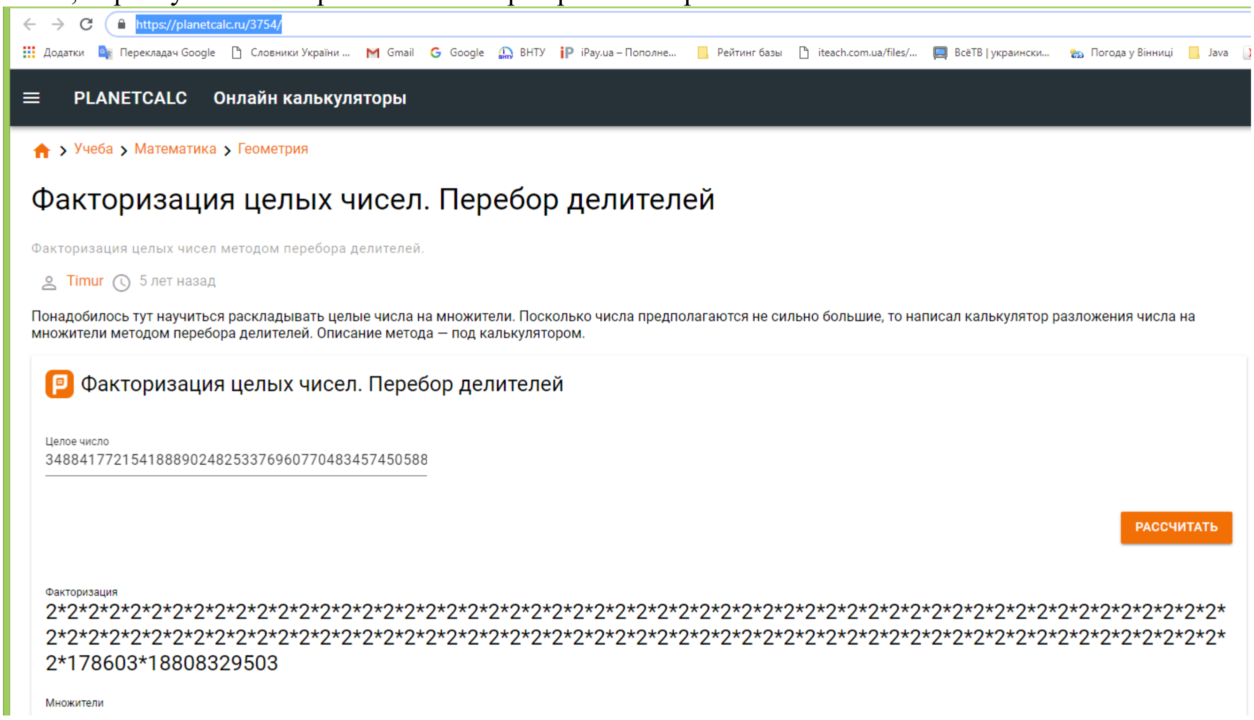

Рис. 1. Помилка онлайн-сервісу для факторизації цілого числа.

Для здійснення емпіричної оцінки стійкості одної моделі криптосистеми з відкритим ключем створено алгоритм та його програмна реалізація в середовищі СКМ Maple для визначення часу факторизації великого цілого числа, що є добутком двох простих чисел.

За отриманими результати побудовано графік, що наведений на рис. 2.

Висновки

Розроблено демонстраційний приклад, призначений для наочного висвітлення задачі факторизації великих цілих чисел.

Отримані результати моделювання в середовищі СКМ Maple щодо рекомендованої довжини ключа відповідають загальновідомим літературним даним.

Для отримання простих чисел за допомогою СКМ Maple краще користуватися функціями “prevprime” та “nextprime”, як більш швидкодіючих у порівнянні з функцією “ithprime”.

Графік залежності довжини простого числа від часу його пошуку не є лінійною залежністю.

Не всім онлайн-сервісам з факторизації цілих чисел можна довіряти.

Експериментальним шляхом підтверджено складність та надійність алгоритму шифрування з відкритим ключем.

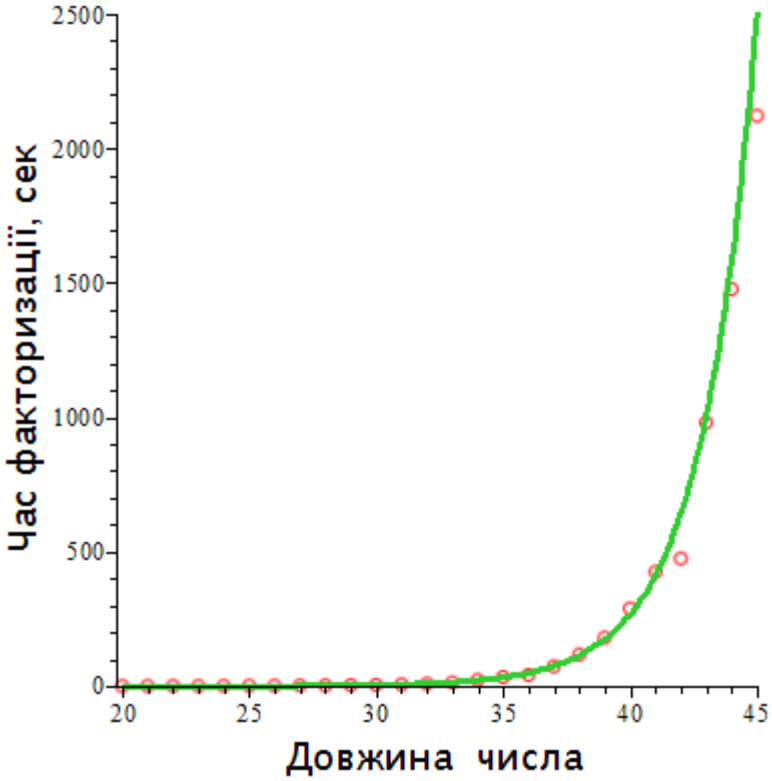

Рис. 2. Емпірична залежність тривалості факторизації цілого числа, що є добутком двох простих чисел, від довжини числа.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Захарченко М. В. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. / М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184 с. – (Криптографічні методи захисту інформації в телекомунікаційних системах та мережах: модуль 2 з дисципліни „Захист інформації в телекомунікаційних системах та мережах”)

2. Михалевич В. М. Використання систем компютерної математики у процесі навчання лінійного програмування студентів ВНЗ: монографія / В. М. Михалевич, О. І. Тютюнник. – Вінниця: ВНТУ, 2016. – 279 с.

3. Михалевич В. М. Використання СКМ Maple для проектування навчальних задач із застосування симплекс-методу / В. М. Михалевич, О. І. Тютюнник, Я. В. Крупський // Вісник Вінницького політехнічного інституту. — 2017. — № 1. — С. 106–117.

4. Щільність заповнення ряду натуральних чисел членами окремої зворотної послідовності другого порядку / В. А.Лужецький, В. М. Михалевич, О. В. Михалевич, В. А. Каплун. // Інформаційні технології та комп’ютерна інженерія. – 2010. – №1. – С. 46–51.

5. Михалевич В. М. Математична модель генерування завдань з невизначених інтегралів / В. М. Михалевич, Я. В. Крупський // Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми : [зб. наук. праць]. — Вип. 15 / редкол. : І. А. Зязюн (голова) та ін. — К.-Вінниця : ДОВ «Вінниця», 2007. — С. 193–197.

6. Михалевич В. М. Excel-VBA-Maple програма генерації задач з дисциплін математичного спрямування / В. М. Михалевич // Інформаційні технології та комп’ютерна інженерія. — 2005. — № 2. — С. 74–83.

7. Михалевич В. М. Ключові проблеми створення навчально-контролюючого комплексу з дисциплін математичного спрямування / В. М. Михалевич // Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми : [зб. наук. праць]. — Вип. 10 / редкол. : І. А. Зязюн (голова) та ін. — К.-Вінниця : ДОВ «Вінниця», 2006. — С. 391–397.

8. Михалевич В. М. Реалізації технології «живих сторінок» в Maple, MathCad, Excel / В. М. Михалевич // Вісник ВПІ. — 2004. — № 3. — С. 90–95.

9. Филимоненкова Н. Н. Обучение функциональному анализу в техническом вузе: практико-ориентированный курс / Н. Н. Филимоненкова. // Математика в высшем образовании. – 2015. – №13. – С. 65–80.

10. Шамрай С. Спецкурси з вивчення програмних засобів математичного спрямування: порівняльний аналіз./ С. Шамрай. // Фізико-математична освіта. Науковий журнал. – Суми : СумДПУ ім. А.С.Макаренка. – 2014. – №2. – С. 55–64.

11. Бедратюк Л. П. Використання системи комп'ютерної алгебри maple в класичних криптосистемах / Л. П. Бедратюк, Г. І. Бедратюк. // Вісник Хмельницького національного університету. – 2015. – №6. – С. 148–153.

Іван Павлович Кулібабчук — студент групи УБ-18б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: ivanp8577@gmail.com

Науковий керівник: ***Володимир Маркусович Михалевич*** — д-р техн. наук, професор, завідувач кафедри вищої математики, Вінницький національний технічний університет, м. Вінниця, e-mail: vmykhal@gmail.com

Kulibabchuk Ivan P. — *student* , Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: ivanp8577@gmail.com

Supervisor: ***Mykhalevych Volodymyr M.*** — Dr. Sc. (Eng.), Professor, Head of the Chair for Higher Mathematics, Vinnytsia National Technical University, Vinnytsia, vmykhal@gmail.com.