УДК 004.942

К.т.н Боярінова Ю.Є., студент Муратова М.О.

**Національний технічний університет України
«Київський політехнічний інститут»**

КРИПТОГРАФІЧНИЙ АЛГОРИТМ RSA НА ОСНОВІ ГІПЕРКОМПЛЕКСНИХ ЧИСЛОВИХ СИСТЕМ ДРУГОГО ПОРЯДКУ

Abstract

Boyarinova Yu. Ye., PhD, Mouratova Maria, student

The cryptographic algorithm RSA based on hypercomplex number system

This paper concerns the task of sophistication of RSA cryptanalysis. The classical RSA algorithm is studied and discussed. The cryptographic algorithm RSA based on hypercomplex number system is implemented. The comparative analysis of efficiency of both the classical and the modified algorithms is fulfilled. The ways for further research are proposed as well.

Вступ

Проблема захисту інформації від несанкціонованого доступу помітно загострилась в зв'язку з широким розповсюдженням локальних і, особливо, глобальних комп'ютерних мереж. Все більша частина приватної інформації безперервно обробляється і зберігається в глобальній мережі. При цьому інформація не є жорстко прив'язаною до носія, може швидко передаватися по каналах зв'язку і копіюватися.

Однією з найважливіших проблем, що виникають при роботі в комп'ютерних мережах є перехват, або витік інформації. В цьому випадку цілісність інформації зберігається, проте її конфіденційність порушена. Для боротьби з цією проблемою розроблено дуже багато цифрових криптографічних алгоритмів для захисту не лише державних, а і наукових, політичних та особистих таємниць.

Існує дві основні криптосистеми: симетрична та асиметрична (криптографічна система з відкритим ключем). Для довготривалого захисту безпеки важливої інформації часто використовуються відкриті ключі.

Ідея криптографії з відкритими ключами полягає в тому, що ключі можна використовувати парами, ключ шифрування та ключ дешифрування, і що може бути неможливим отримання одного ключа без іншого. На сьогоднішній день запропонована велика кількість

криптографічних алгоритмів з відкритими ключами, проте лише деякі з них безпечні та практичні.

Одним із алгоритмів, які добре працюють як при шифруванні, так і для цифрового підпису є алгоритм RSA. Опис цього алгоритму, названого за першими літерами прізвищ його розробників (Rivest, Shamir та Adleman), було вперше опубліковано в серпні 1977 року Мартіном Гарднером в журналі Scientific American [1]. Він досі є найпростішим в реалізації поміж алгоритмів з відкритими ключами і успішно протистоїть активному криптоаналізу.

Криптографічні системи з відкритим ключем використовують так звані необоротні функції, які володіють наступними властивостями:

Якщо відомо *x*, то *f(x)* обчислити відносно просто.

Якщо відомо $y = f(x)$, то для обчислення *x* немає простого (ефективного) шляху.

Під однонаправленістю мається на увазі не теоретична однонаправленість, а практична неможливість обчислити обернене значення, використовуючи сучасні обчислювальні засоби, за прийнятний проміжок часу.

В основу RSA покладено задачу добутку двох великих простих чисел і розкладання складних чисел на прості множники, яка є однонаправленою обчислювальною задачею. Проте процес розкладання великих чисел на множники стає все простішим, причому із більшою швидкістю, ніж передбачувалось раніше. Дослідники певні, що, використовуючи їх метод факторизації, зламати 1024-бітний RSA-ключ буде можливо до 2012 року [2].

Важливим також є той факт, що відкриті ключі часто використовуються для довготривалого безпечного обміну та збереження важливої інформації. Причому робити досить точні передбачення щодо періоду надійної захищеності інформації певним ключем все складніше. А можливість використання дуже довгих ключів обмежена вартістю обчислень.

Постановка задачі

Довести, що можна збільшити час факторизації без збільшення кількості розрядів чисел, що використовуються, за рахунок розгляду даного алгоритму в області гіперкомплексних чисел.

Опис алгоритму RSA

1. *Створення відкритого та секретного ключів:*
   RSA-ключі генеруються наступним чином:[2]

- Обираються два випадкових простих числа p і q заданого розміру (наприклад, по 1024 біт кожне).
- Обчислюється їх добуток $n = pq$, який називається модулем.
- Обчислюється значення функції Ейлера від числа n:

$$\varphi(n) = (p-1)(q-1);$$

- Обирається ціле число e $(1 < e < \varphi)$, взаємно просте зі значенням функції $\varphi(n)$. Звичайно e – це просте число, що містить невелику кількість одиничних бітів у двійковому запису. Число e називається відкритою експонентою (англ. public exponent). Час, необхідний для шифрування з використанням швидкого підведення до степеня, пропорційний числу одиничних бітів в e.
- Обчислюється число d, мультиплікативно обернене до числа e по модулю $\varphi(n)$, тобто число, що задовольняє умові: $de \equiv 1(mod\varphi(n))$, або: $de = 1 + k\varphi(n)$, де k — деяке ціле число.

Число d називається секретною експонентою. Звичайно, воно обчислюється за допомогою розширеного алгоритму Евкліда.

Пара $P = (e, n)$ публікується в якості відкритого ключа RSA (англ. RSA public key).

Пара $S = (d, n)$ грає роль секретного ключа RSA (англ. RSA private key) і тримається в секреті.

2. *Шифрування та дешифрування*

Шифроване повідомлення передається у вигляді: $P_a(M) = M^e mod\ n$, де M – відкритий текст, e – відкритий ключ зі сторони A.

Прийняте повідомлення представляється у вигляді: $S_a(C) = C^d mod\ n$, де C – зашифроване повідомлення, d – секретний ключ.

Розглянемо приклад застосування гіперкомплексних числових систем другого порядку для даного алгоритму.

Для побудови алгоритму на основі комплексних чисел неможлива пряма підстановка комплексних чисел замість дійсних, тобто всі операції, за допомогою яких генеруються ключі, здійснюється шифрування та дешифрування необхідно реалізувати в полі комплексних чисел, таким чином необхідно реалізувати показникову функцію, для якої потрібні логарифмічна функція та експонента.

Показникова функція для комплексних $z = a + ib;\ m = c + id;$ буде мати вигляд: $m^z = e^{zln(m)} = e^{(a+ib)(\ln|m| + i\arg(m))} = \mathrm{e}^{(\mathrm{a+ib})(\ln(\mathrm{c}^2+\mathrm{d}^2)+\mathrm{i}\,\mathrm{arct}(\frac{\mathrm{d}}{\mathrm{c}}))}$, де $\arg(z) = arct(\frac{b}{a})$.

Оцінка стійкості алгоритму RSA

Безпека алгоритму RSA побудована на принципі складності факторизації, тобто вона повністю залежить від проблеми розкладання на множники великих чисел.

На сьогодні найкращим алгоритмом факторизації «Решето числового поля чисел» (Number field sieve, NFS)[4]. Оцінка його евристичного часу виконання: $e^{(1.923+O(1))(\ln(n))^{\frac{1}{3}}(\ln((\ln(n))))^{\frac{2}{3}}}$

Для комплексних чисел може бути запропонований такий алгоритм факторизації:

1. Обчислити норму комплексного числа $\alpha, N(\alpha)$
2. Розкласти *N(α)* на множники простих раціональних чисел $p_1 \cdot \ldots \cdot p_s$
3. Всі $p_i, (i = 1, 2, \ldots, s)$ виду $4k + 3$ залишити без змін, решту p_j виду $4k + 3$ розкласти на суму квадратів: $p_i = x^2 + y^2$, тоді отримаємо два додаткові множники: асоційовані з $x + yi$ та $y + xi$
4. Обчислити всі можливі добутки отримані в кожному з випадків для простих комплексних чисел до тих пір, поки не отримаємо число, асоційоване з вихідним числом α.

Цей алгоритм окрім розкладання дійсного числа *N(α)* на прості множники вимагає розкладання всіх отриманих при попередньому розкладі чисел виду $4k + 1$ на суму квадратів. Ефективних алгоритмів для представлення числа у вигляді суми квадратів згідно з [5] поки що немає.

Г. Хассе [6] дає таку оцінку часу виконання запропонованого ним алгоритму: $O(\sqrt{p})$, де p – це число, що розкладається. Звідси видно, що цей алгоритм засновано на прямому переборі можливих значень.

Таким чином, оцінка алгоритму факторизації для комплексних чисел буде: $O(e^{(1.923+O(1))(\ln(n))^{\frac{1}{3}}(\ln((\ln(n))))^{\frac{2}{3}}}) + O(\sqrt{f(n)})$, де n – це кількість розрядів у нормі *N(α)*, а $f(n) = p$ – це максимальне число вигляду $4k + 1$, отримане при розкладанні норми. Тобто $f(n)$ є показниковою функцією від n і залежність $O(\sqrt{f(n)})$ не є лінійною.

Висновки

При побудові алгоритму RSA на основі гіперкомплексних чисел другого порядку отримали більш складний алгоритм. Криптоаналіз RSA на основі алгоритму факторизації комплексних чисел виявився менш ефективним на $O(\sqrt{p})$. Це означає, що застосування гіперкомплексних

чисел при реалізації алгоритму RSA дозволяє ускладнити криптоаналіз алгоритму без збільшення довжини ключів.

У подальшому було б доцільно реалізувати алгоритм RSA на основі ГЧС вищих порядків.

Література

1. *M.Gardner* A New Kind of Cipher That Would Take Millions of Years to Break, Scientific American, v.237. –n. 8, Aug 1977. – pp. 120-124.
2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си, Applied Cryptography. Protocols, Algorithms and Source Code in C. - М.: Триумф, 2002. - 816 с.
3. *М.В. Синьков, Ю.Е. Бояринова, Я.А.Калиновский.* Конечномерные гиперкомплексные числовые системы. Основы теории. Применения.– К.: ИПРИ НАН Украины, 2010.– 389 с.
4. *A.K. Lenstra and H.W. Lenstra. Jr.*, eds., Lecture Notes in Mathematics 1554: The 967. Development of the Number Field Sieve, Springer-Verlag. 1993.
5. *М. Н. Вялый* О представлении чисел в виде суммы двух квадратов. - Матем. просв., сер. 3, 10, Изд-во МЦНМО. – М. – 2006. – С. 190–194
6. *Г.Хассе* Лекции по теории чисел//узд. Иностранной литературы. – 1953. – С. 179-183