Шифрування з надійними ключами в асиметричних алгоритмах

УДК 003.26:511.41

Юлія Мисло[1], Михайло Пагіря[2]

Ужгородський національний університет,
[1]julia.mislo@uzhnu.edu.ua, [2]mykhaylo.pahirya@uzhnu.edu.ua

В сучасному інформаційному світі особливо важливою є проблема збереження конфіденційність даних, які передаються від одного абонемента до іншого. Найбільш важлива інформація пересилається учасниками обміну у зашифрованому вигляді. Для шифрування використовуються алгоритми як із симетричними, так із асиметричними ключами. Кожен класів алгоритмів має свої переваги та недоліки, а також сферу свого використання. В останні десятиліття широкої популярності набули алгоритми із асиметричним ключем, оскільки вони ґрунтуються на важко розв'язувані математичні задачі зокрема на задачі факторизації великих чисел. На криптосистеми із асиметричним ключем донині покладається велика надія.

З іншого боку, бурхливий розвиток інформаційних технологій безпосередньо пов'язаний із зростанням потужностей сучасних комп'ютерів. Це дозволяє проводити так звані лобові атаки на нових підкласах важко розв'язуваних задач. Щоб убезпечити себе від подібних несподіванок, доводиться проводити додатковий аналіз алгоритмів, які використовуються.

Ланцюгові дроби використовують при розв'язанні задач з різних розділів сучасної математики та її застосувань. В задачах теорії чисел, наприклад, ланцюгові дроби утворюють підґрунтя для аналізу надійності шифрів з асиметричними ключами.

Відомо [1,2], що при використанні одного із найбільш вживаних алгоритмів з асиметричним ключем --- алгоритму RSA, функція шифрування визначається наступним чином $E(x)=x^e \pmod n$, де модуль n рівний добутку двох великих простих чисел p та q, $n=pq$, які утворюють таємну частину ключа. Варто зауважити, що задача факторизації числа n належить до складних, важко розв'язуваних задач теорії чисел і перевершує за складністю задачу про перевірку числа на простоту. З іншого боку, і секретний ключ d в функції дешифрування $D(c)=c^d \pmod n$ знайти не легше, якщо залишається невідоме значення функції Ойлера $\varphi(n)=(p-1)(q-1)$.

Щоб виконати факторизацію числа n використовують метод пробних ділень, який вимагає $O(n^{1/2})$ двійкових операцій, ***ρ-метод Полларда,*** який здатний знайти один із співмножників після виконання $O(n^{1/4}(\log n)^3)$ двійкових операцій, ***метод Ферма***, який особливо ефективний у випадку, коли співмножники близькі, метод факторних баз, що вимагає виконання $O(\exp(C(r \log r)^{1/2}))$ двійкових операцій. На метод факторних баз спирається спосіб відшукання співмножників числа за допомогою розвинення числа в ланцюговий дріб, який ґрунтується на теоремі Лагранжа.

Метод дослідження стійкості алгоритмів з асиметричними ключами, який використовує результати з теорії ланцюгових дробів на прикладі алгоритму RSA розглянуто в роботі [3]. Якщо зроблені додаткові припущення про складові секретної частини ключа, тобто, якщо $q < p < 2q$, $d < n^{1/4}/3$, $e < \varphi(n)$, то можна відшукати розвинення відношення складових відкритої частини ключа e/n у правильний ланцюговий дріб і один із канонічних знаменників ланцюгового дробу

буде секретним ключем ***d*** для RSA шифру. Для того, щоб здійснити реалізацію алгоритму необхідно виконати перевірку ***O(ln n)*** підхідних дробів.

Було проведено дослідження розглянутих методів факторизації таємних складових ключів [4], здійснено порівняння по часу виконання кожного із методів. Це дозволяє виробити певні рекомендації щодо вибору надійних таємних складових ключів шифрування.

1. N.Koblitz A Course in Number Theory and Cryptography. 2-nd ed. Springer Science & Business Media, 1994.
2. M. Cozzens, S. J. Miller The Mathematics of Encryption: an Elementary Introduction. American Mathematical Society. Mathematical World 29, 2013.
3. M. Wiener Cryptanalysis of short RSA secret exponents *// IEEE Transactions on Information theory* 36.3 (1990): 553-558.
4. Ю.М. Мисло, М.М. Пагіря Криптоаналіз асиметричних ключів алгоритмами ланцюгових дробів. // ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф., (м. Ужгород, 2-4 трав. 2023 р.) Київ: НАУ, 2023. С. 36.