УДК 004.01

Гуцуляк Д.В., студентка 1 курсу спеціальності 122 «Комп'ютерні науки»
Луценко А.В., асистент кафедри прикладної математики і кібербезпеки

ПРО ВИКОРИСТАННЯ ДІОФАНТОВИХ РІВНЯНЬ ДЛЯ ЗНАХОДЖЕННЯ СЕКРЕТНИХ КЛЮЧІВ В КРИПТОСИСТЕМАХ З ВІДКРИТИМ КЛЮЧЕМ

Донецький національний університет імені Василя Стуса

Діофантові рівняння та теорія чисел є важливими складовими багатьох криптографічних протоколів та систем шифрування, які застосовуються в різних сферах для захисту конфіденційної інформації та забезпечення інтегритету даних.

Історія діофантових рівнянь для знаходження секретних ключів в криптографії дійсно починається з розробки криптосистеми RSA у 1978 році Роном Рівестом, Аді Шамиром та Леонардом Адлеманом. Вони використали принцип розв'язування діофантових рівнянь для побудови своєї криптосистеми, яка базується на складності факторизації великих чисел [1].

Криптосистеми використовують два різні ключі - відкритий та закритий. Відкритий ключ використовується для зашифрування повідомлення, а закритий ключ використовується для розшифрування криптограми. Відкритий ключ можна передавати відкритим каналом, і навіть якщо зловмисник знає відкритий ключ, він не може розшифрувати повідомлення без закритого ключа [2].

Діофантове рівняння – це рівняння, що включає лише суми, добутки та степені, у якому всі константи є цілими числами, а єдині розв'язки, що представляють інтерес, є цілими числами [3].

Тепер детальніше розглянем різновиди криптосистем з відкритим ключем в яких використовуються діофантові рівняння для знаходження секретних ключів.

Криптосистема RSA. RSA — криптографічна система з відкритим ключем. RSA став першим алгоритмом такого типу, придатним і для шифрування і для цифрового підпису. Алгоритм використовується у великій кількості криптографічних застосунків. У криптосистемі RSA для генерації секретного ключа потрібно знайти таке число d, яке задовольняє рівняння $ed = 1 \mod (p-1)(q-1)$, де e - це відкритий ключ криптосистеми, а p та q - великі взаємно прості числа, які задовольняють діофантове рівняння $pq = n$, де n - відкритий ключ криптосистеми [4].

Приклад 1. Використання діафантового рівняння у криптосистемі RSA [2].

Маємо p = 11, q = 5, M = 15.
Обчислюємо діофантове рівняння: n = 11 * 5 = 55.
Визначаємо функцію Ейлера: φ (55) = (11–1)(5–1) = 40.
Обираємо ключ зашифровування e = 7, який задовольняє умовам 7 < 40;
НСД (7, 40) = 1.
Визначаємо d – ключ розшифровування з рівняння
7d = 1 (mod 40).
Для розв'язання рівняння 7d = 1 (mod 40) використовуємо алгоритм Евкліда:
40 = 7 * 5 + 5;
7 = 5 * 1 + 2;
5 = 2 * 2 + 1;
2 = 1 * 2 + 0.
Обернене підставляння дає
1 = 5 – 2 * 2 = 5 – (7 – 5 * 1)2 = 5 * 3 + 7(–2) = (40 – 7 * 5)3 + 7(–2)=
= 40 * 3 + 7(–17).
Оскільки –17 = 23 (mod 40), то d = 23.

Криптосистема ElGamal. Шифрування ElGamal є криптосистемою з відкритим ключем. Вона використовує шифрування з асиметричним ключем для спілкування між двома сторонами та шифрування повідомлення [2]. У криптосистемі ElGamal для генерації секретного ключа потрібно вирішити діофантове рівняння log_g(a) = x mod p-1, де p та g - великі взаємно прості числа, а a - відкритий текст.

Криптосистема DSA. DSA – це коли система порівнює пошуковий запит користувача і контент на сайті. Якщо вони є релевантними, вона автоматично створює заголовок оголошення та вибирає посадкову сторінку на основі контенту на сайті [5]. У криптосистемі DSA для генерації секретного ключа також використовуються діофантові рівняння. Для знаходження секретного ключа потрібно знайти таке число x, яке задовольняє рівнянню $k * x = H(m) + a * r \ mod \ q$, де k, a, r, q - великі взаємно прості числа, а $H(m)$ - хеш повідомлення m.

Приклад 2. Використання діафантового рівняння у криптосистемі DSA [2].

Нехай p = 211; q = 7; g = 144; k = 2; x = 3; h(M) = 15.
Відкритий ключ користувача: Y = 144^2(mod 211) = 58.
Створення підпису:
r = [144^3(mod 211)] mod 7 = 123 (mod 7) = 4;
s = [3^{-1}(15 + 2 * 4)] mod 7 = (3^{-1}* 23) mod 7 = 3.
Підпис: (4, 3). Перевірка підпису:
w = (3^{-1}) mod 7 = 5;
u1 = (15 * 5) mod 7 = 5;
u2 = (4 * 5) mod 7 = 6;
v = [(144^5* 58^6) mod 211] mod 7 = 123 (mod 7) = 4.
v = r = 4 – підпис є справжній.

Розрізняють такі типи діофантових рівнянь: лінійні діофантові рівняння, діофантові рівняння другого ступеня, діофантові рівняння третього ступеня, біномні діофантові рівняння, симетричні діофантові рівняння.

Один з прикладів використання діофантових рівнянь в IT-технологіях полягає у використанні алгоритму RSA для захисту комунікацій у мережах Інтернет. RSA використовує діофантові рівняння для знаходження секретних ключів, що використовуються для шифрування та розшифрування повідомлень.

Проаналізувавши усю інформацію вище можна виділити переваги і недоліки кожної з криптосистем за використанням діофантових рівнянь (табл.1).

Криптосистема	Переваги	Недоліки
RSA	- застосовується простий алгоритм генерації ключів; - високий рівень безпеки при правильному виборі параметрів; - швидкість зашифрування та розшифрування повідомлення досить висока.	- застосування алгоритму може бути затруднене при великих розмірах ключа, оскільки довжина ключа повинна бути достатньо великою для запобігання атакам перебору; - підтримка схеми RSA потребує великих ресурсів обчислювальної системи.
ElGamal	- є безпечна, якщо правильно вибрати параметри; - відсутність обмежень на довжину повідомлення, яке можна зашифрувати.	- повільніша за RSA, оскільки використовує великі прості числа. - Є питання щодо безпеки при використанні малих параметрів.
DSA	- більш ефективна за RSA та ElGamal, особливо для підписів повідомлень; - забезпечує достатній рівень безпеки при правильному виборі параметрів.	- не має підтримки шифрування повідомлень; - вимагає точного вибору параметрів, що може бути складним.

Таблиця 1. – Порівняльна таблиця криптосистем за використанням діофантових рівнянь.

Висновки. Діофантові рівняння є важливим інструментом для знаходження секретних ключів в криптосистемах з відкритим ключем і дозволяють забезпечити безпеку і захист конфіденційної інформації. Отже, використання діофантових рівнянь в інформаційних технологіях є доцільним, адже вони захищають конфіденційну інформацію.

Список літературних джерел.

1. *A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. Vol.21, Issue 20, 1978, 120-126.*
2. *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.*
3. *Britannica, The Editors of Encyclopaedia. "Diophantine equation". Encyclopedia Britannica, 26 Nov. 2014.*
4. *Алгоритм RSA. URL: http://surl.li/gytff*
5. *Динамічні пошукові оголошення (DSA): принцип роботи та інструкція по запуску. URL: https://pengstud.com/ua/blog/dsa-how-does-it-work-ua/*