СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Мельник Ю. В. Конспект лекцій з дисципліни «Зовнішньоекономічна діяльність підприємства» для студентів денної та заочної форм навчання ступеня вищої освіти «бакалавр» Тернопіль: ТНЕУ, 2020. 62 с. URL: http://dspace.wunu.edu.ua/bitstream/316497/40407/1/konspekt_MZED.pdf (дата звернення: 28.09.2024).
2. Павленко О. В., Музильов Д. О. Стабільна модель функціонування логістики для постачання швидкопсувних продуктів маршрутами Україна–Польща. *Комунальне господарство міст*. 2023. URL: http://surl.li/obxuoy (дата звернення: 05.10.2024).
3. Литовченко О., Кузенко Т. структурно-функціональне моделювання процесу управління інвестиційною привабливістю підприємства. *Економіка та суспільство*, 2021. Вип. 34. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1253/1208 (дата звернення: 05.10.2024).
4. Волонтир Л. О. Інформаційна логістика бізнес-структур малих підприємств. *Причорноморські економічні студії.* 2018. Вип. 34. С. 198–202. URL: http://repository.vsau.org/getfile.php/19524.pdf (дата звернення: 05.10.2024).
5. Коренівська О. Л. Моделювання сигналів та процесів в біосистемах. Конспект лекцій. Лекція 3. URL: http://surl.li/sbtbqn (дата звернення: 05.10.2024).
6. Лукінський В. С. Логістика та управління ланцюгами поставок. 2016. URL: https://stud.com.ua/41379/logistika/klasifikatsiya_metodiv_modeley_logistiki (дата звернення: 07.10.2024).

УДК 511:003.26]:004.056.55

АНАЛІЗ ЗАСТОСУВАННЯ АЛГЕБРИ В ЗАХИСТІ ІНФОРМАЦІЇ

А. І. Родюк, А. В. Луценко

Анотація. У цій статті розглянуто математичні основи криптографії; застосування основних понять теорії чисел, як-от властивості простих та важкість факторизації великих чисел в RSA-шифруванні; як алгебраїчні структури – групи, кільця та поля – використовуються для побудови різних криптографічних схем, наприклад протоколів обміну ключами; використання неасоціативних алгебраїчних систем – квазігруп – у шифруванні, поліномів – у побудові схем розподілу секретів, а також хеш-функцій та хешування, що є невід'ємною частиною багатьох алгоритмів захисту даних.

Ключові слова: алгебра, квазігрупа, криптографія, шифрування, розшифрування.

Вступ. Наразі проблема захисту інформації як ніколи актуальна. Адже тепер вся важлива інформація зберігається не на папері, а на електронних пристроях зберігання. Природно, що за таких обставин комп'ютерні злочини дуже розповсюджені, наприклад, махінації в банках, які зводяться до зміни даних з метою одержання фінансової вигоди. Водночас громадськість стурбована порушенням їхньої конфіденційності, до того ж розкривається лише мала кількість комп'ютерних злочинів, адже про них воліють мовчати, щоб не втратити іміджу. Залежність суспільства від комп'ютерів привернула увагу до проблеми захисту приватних даних від незаконного доступу.

Метою статті є аналіз застосування деяких розділів алгебри та теорії чисел у захисті інформації, а саме розглянуто використання алгебраїчних структур для побудови різних криптографічних схем.

Безпека комунікації реалізується в основному за допомогою двох типів алгоритмів:

1. Симетричні алгоритми [1; 2; 3]: використовують один ключ для шифрування і дешифрування (наприклад, AES, DES). Алгебра тут застосовується для побудови стійких блокових шифрів.

2. Асиметричні алгоритми [4]: використовують пару ключів – відкритий і закритий (RSA, ElGamal). Багато з цих алгоритмів базуються на теорії чисел і модульній арифметиці.

До того ж криптографія дає змогу виконувати передачу інформації з використанням методів ідентифікації та автентифікації. Ці методи забезпечують підтвердження особи користувача або пристрою. Протоколи обміну ключами (наприклад, Діффі–Геллмана) дають змогу двом сторонам безпечно обмінюватися секретними ключами через незахищені канали.

Більшість відомих конструкцій криптографічних примітивів, кодів виявлення і виправлення помилок використовують структури з асоціативної алгебри у вигляді груп, кілець і полів. Два видатні фахівці з квазігруп, Д. Денес і А. Д. Кідвелл [5], одного разу проголосили настання нової ери в криптології, що полягає у застосуванні неасоціативних алгебраїчних систем, як-от квазігрупи і неополі.

Квазігрупи та їх комбінаторні еквівалентні латинські квадрати дуже підходять для цієї мети через їх структуру, особливості, велику кількість, а також тому, що вони приводять до конкретних простих і водночас ефективних примітивів. Застосування квазігруп у криптографії обґрунтовується також концепцією мультиперестановки, яка поширена в криптографії і відповідає парам ортогональних латинських квадратів. Проте наразі дуже мало дослідників використовують ці інструменти, і криптографічне товариство все ще сумнівається щодо цього.

Алгебра є основою для багатьох сучасних алгоритмів захисту інформації. Без неї було б неможливо створити стійкі криптографічні схеми, що гарантують конфіденційність, цілісність та автентичність даних в інформаційних системах.

Теорія чисел

Основні поняття теорії чисел, як-от прості числа, взаємно прості числа та модульна арифметика, є важливими для алгоритмів шифрування.

Криптоалгоритм RSA

Криптосистема RSA [2], названа так на честь її винахідників R. Rivest, A. Shamir, L. Adleman, є найбільш застосовуваною криптосистемою з відкритим ключем. Вона базується на властивостях простих чисел і труднощах факторизації великих чисел. Може використовуватися як для шифрування інформації, так і для цифрового підпису.

Генерація ключів відбувається так:

Кожен учасник вибирає два великі прості випадкові числа, які не співпадають між собою, нехай p і q, приблизно одного розміру, обчислює $n = pq$ й $\varphi(n) = (p-1)(q-1)$ ($\varphi(n)$ – функція Ейлера), підбирає випадкове ціле число, $1 < e < d$, застосовуючи розширений алгоритм Евкліда, обчислює ціле, $1 < d < \varphi(n)$, таке, що $ed = 1(mod\,\varphi\,(n))$. Відкритим ключем є пара чисел (n, e), секретним ключем є пара чисел (n, d).

Алгоритм шифрування:

Перший учасник шифрує повідомлення m, яке потім надсилається другому. Для шифрування перший учасник бере відкритий ключ другого (n, e), представляє повідомлення у вигляді цілого числа m з інтервалу $[0, \text{n} - 1]$, обчислює $c = m^e(mod\,n)$ та надсилає шифрований текст.

Алгоритм розшифрування:

Другий учасник, використовуючи свій секретний ключ (n, d), обчислює $m = c^d(mod\,n)$.

Групи, кільця, поля

Група – множина, в якій визначено внутрішній асоціативний закон композиції, існує нейтральний елемент і до кожного елемента – симетричний.

Кільце – множина, в якій визначено два внутрішні закони композиції $(+)$ і $(\cdot)$, перший з яких – закон комутативної групи, а другий – асоціативний і подвійно дистрибутивний щодо першого.

Поле – комутативне кільце, множина ненульових елементів якого утворює групу відносно множення в кільці.

Ці структури алгебри використовуються для побудови різних криптографічних схем. Наприклад, еліптичних кривих: еліптична криптографія базується на складності розв'язування рівнянь для точок на еліптичних кривих, що використовують групові операції.

Групи за модулем простого числа застосовуються в протоколах обміну ключами, наприклад, упротоколі Діффі–Геллмана.

Протокол Діффі–Геллмана

Хотілося б мати такий протокол, за допомогою якого два учасники обмінювалися б повідомленнями m_1 і m_2 доти, допоки остаточно не домовилися б про деякий ключ k, при цьому визначити k знаючи лише m_1 і m_2 було б неможливо. Перший протокол, який досяг цієї бажаної мети, був запропонований Діффі (W. Diffie) і Геллманом (M. E. Hellman) [2] в 1976 році. Він ґрунтується на задачі дискретного логарифмування.

Відкрито вибирається просте число p, так, щоб число $p-1$ мало достатньо великий простий множник $p` \geq 2^{160}$, та велике просте число n, а в групі G_n^* знаходимо елемент g – генератор (алгоритм пошуку g описаний нижче). Перший учасник генерує $a \in [1; n-1]$, обчислює $g_a = g^a(mod\,n)$ $(g_a \neq 1)$ й надсилає другому. Другий – генерує $b \in [1; n-1]$, обчислює $g_b =$

$g^b (mod\, n)$ ($g_b \neq 1$) й надсилає першому. Тоді перший учасник обчислює $k_1 \equiv g_b^a (mod\, n)$, а другий – $k_2 \equiv g_a^b (mod\, n)$. Обидва значення збігаються й дають величину загального ключа. Після закінчення протоколу учасники повинні стерти a і b.

Алгоритм випадкового вибору первісного кореня за простим модулем: означення: p – просте число, $q_1, q_2, \ldots, q_k$ – усі прості множники числа $p-1$.

INPUT: p, q_1, q_2, q_k.

OUTPUT: g.

1. Let $g \in [2, p-1]$.

2. For i: 1 ... k *Do If* $g^{\frac{p-1}{q_i}}$ *Go To (1).*

3. Return g.

Квазігрупи.

Квазігрупою називається групоїд $(Q;\cdot)$, такий, що для довільних a, b кожне з рівнянь $a \cdot x = b$, $y \cdot a = b$ має єдиний розв'язок.

Квазігрупова операція часто розглядається разом із оберненими операціями: лівим (\) та правим (/) діленням. Обернені операції визначені так: $xy = z$ тоді і тільки тоді, коли $x\backslash z = y$ тоді і тільки тоді, коли $z/y = x$.

Теорема. Групоїд з трьома операціями $(\cdot)$, (\), (/) є квазігрупою тоді і тільки тоді, коли:

$$x\backslash xy = y$$
$$x(x\backslash y) = y$$
$$xy/y = x$$
$$(x/y)y = x.$$

Подвійні операції $(\cdot)$, (\), (/) визначені так:

$$x * y = yx$$
$$x\backslash\backslash y = y\backslash x$$
$$x//y = y/x.$$

Ці шість операцій також є квазігруповими $(\cdot)$, (\\), (/), $(*)$, (\\), (//), вони називаються парастрофами (спряженими) одна до одної.

В. Щербаков у [6] оглянув можливі застосування квазігруп у криптографії. Одним із успішних методів є квазігрупова обробка рядків С. Марковського (детально [7; 8]):

Нехай $A = \{a_1, a_2, \ldots, a_n\}$ – алфавіт, $(A; \cdot)$ – квазігрупа. Позначимо A^+ множину усіх непорожніх слів з A. Візьмемо елемент a з A і визначимо унарну операцію F над A^+ так:

$$F(u_1, u_2, \ldots, u_k) = v_1, v_2, \ldots, v_k, k > 0, \text{де } v_1 = a \cdot u_1,$$
$$v_i = v_{i-1} \cdot u_i, 1 < i \leq k.$$

А також:

$$G(v_1, v_2, \ldots, v_k) = u_1, u_2, \ldots, u_k, k > 0, \text{де } u_1 = a\backslash v_1,$$
$$u_i = v_{i-1}\backslash v_i, 1 < i \leq k.$$

Множина A, операція $(\cdot)$ і (\), елемент a і функції F і G визначають шифр алфавіту A. Функція G розшифровує текст, зашифрований функцією F.

Складність методу полягає у ретельному підборі квазігрупи. Будь-який вид внутрішньої симетрії (наприклад, комутативність, асоціативність, ліва симетрія, повна симетрія та ін.) послабить опір атакам.

Д. Глігороський і С. Марковський у [9] експериментально дійшли висновку, що з наявних 576 квазігруп четвертого порядку тільки 192 придатні для використання в шифрі. Однак для алфавіту з 256 буквами (більш реалістичний випадок) існує більше 10^{58000} квазігруп кандидатів для вибору [7].

Також існує метод, де послідовність квазігруп використовується для багаторазового повторного шифрування. Це значно підвищує стійкість, оскільки слабкі сторони однієї квазігрупи нівелюються іншими. Але ціна такого методу полягає в обсязі використовуваної пам'яті для реалізації шифру [10].

Лінійна алгебра

Лінійна алгебра, а саме кодова теорія, використовується в побудові кодів для захисту інформації під час передачі (наприклад, коди Хеммінга, Ріда–Соломона).

Векторні простори та матриці можуть використовуватися в деяких методах шифрування, наприклад, MDS-матриці в AES (Advanced Encryption Standard):

MDS-матриця (Maximum Distance Separable) – це матриця, що складається з $(m + n)$-кортежів, таких, що два різні $(m + n)$-кортежі не можуть збігатися у будь-яких m позиціях.

MDS-матриця є еквівалентною повному набору значень $(x, f(x))$, де $f(x)$ – код, що виправляє помилки, який досягає межі Сінглтона.

MDS-матриці використовуються у криптографічних примітивах для створення так званих мультиперестановок, не обов'язково лінійних функцій з довершеною дифузією та для забезпечення дифузії у блокових симетричних шифрах, наприклад, у AES.

Поліноми

Алгоритми для факторизації поліномів мають застосування в криптографічних алгоритмах, зокрема у криптосистемах на решітках. Поліноми застосовуються для побудови схем розподілу секретів, наприклад, схема Шаміра для розподілу ключів.

Схема Шаміра:

Ідея схеми полягає у тому, що щоб задати многочлен ступеня n, потрібно $(n + 1)$ точок.

Короткий опис алгоритму:

Нехай дано поле G. Фіксуємо n різних ненульових несекретних елементів даного поля. Кожен з цих елементів присвоюється певному члену групи. Далі вибирається довільний набір з t елементів поля G, з яких складається поліном $f(x)$ над полем G ступеня $t-1, 1 < t \leq n$. Після отримання полінома вираховуємо його значення в несекретних точках і повідомляємо отримані результати відповідним членам групи.

Відновити секрет можна за допомогою інтерполяційної формули.

Перевагою схеми Шаміра є те, що вона є легко масштабованою. Щоб додати членів групи, потрібно просто збільшити ступінь полінома на відповідне число, водночас компрометація k-тої частини секрету переводить поліном із (n, t) в $(n-k, t-k)$.

Хеш-функції та хешування

Хеш-функції є невід'ємною частиною багатьох алгоритмів захисту даних. Алгебра використовується для побудови стійких до колізій хеш-функцій, які гарантують, що зміна навіть одного біта в повідомленні призведе до кардинальної зміни хешу.

Хеш-функція – функція, що перетворює вхідні дані будь-якого (зазвичай великого) розміру в дані фіксованого розміру.

Хешування – перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини.

Однобічні хеш-функції

Однобічна функція $H(M)$ застосовується до повідомлення M довільної довжини й повертає значення h фіксованої довжини m:

$h = H(M)$.

У однобічних хеш-функцій є додаткові властивості:

1) знаючи M, легко обчислити h;

2) знаючи H, важко визначити M, для якого $h = H(M)$;

3) знаючи M, важко визначити інше повідомлення M', для якого $H(M) = H(M')$.

Зміст однобічних хеш-функцій полягає в забезпеченні для M унікального ідентифікатора.

У деяких моментах властивості однобічності недостатньо, необхідне виконання іншої вимоги, що називається стійкістю до зіткнень: повинно бути важко знайти два випадкові повідомлення M і M', для яких $H(M) = H(M')$.

Висновки. Криптографія є необхідною в сучасному світі як у політичному та військовому, так і у цивільному секторі. Адже усі ми маємо власні таємниці й приватні розмови та воліємо, щоб вони лишалися такими. В цьому нам допомагають криптографічні примітиви.

Алгебра є невід'ємною частиною захисту інформації, адже саме на ній побудовано алгоритми. Без неї було б неможливо створити стійкі криптографічні схеми, що гарантують конфіденційність, цілісність і автентичність даних в інформаційних системах, протоколи обміну ключами, схеми розподілу секретів та інші складники шифрування даних.

Abstract. This article discusses the mathematical foundations of cryptography. The application of basic concepts of number theory such as the properties of primes and the difficulty of factorizing large numbers in RSA encryption. How algebraic structures such as groups, rings, and fields are used to build various cryptographic schemes, such as key exchange protocols. Use of non-associative algebraic systems – quasigroups in encryption. Polynomials in the construction of secret distribution schemes. As well as hash functions and hashing, which are an integral part of many data protection algorithms.
Keywords: algebra, quasigroup, cryptography, encryption, decryption.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Diffie W., Hellman M. E. New directions in cryptography. *IEEE Transactions on Information Theory.* 1976. Vol. 22(6). P. 644–654.
2. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM.* 1978. Vol. 21(2). P. 120–126.
3. Brassard G. Modern Cryptology, Lecture Notes in Computer Science 325, Berlin: Springer Verlag, 1988.
4. Smid M. E., Branstad D. K. The date encryption standard: past and future. *Contemporary Cryptology, The science of Information Integrity.* Piscataway: IEEE Press, 1992. P. 43–64.
5. D'enes J., Keedwell A. D. Some applications of non-associative algebraic systems in cryptology. *Pure Mathematics and Applications.* 2001. Vol. 12(2). P. 147–195.
6. Shcherbacov V. On some known possible applications of quasigroups in cryptology: manuscript, 2003.
7. Markovski S., Gligoroski D., Andova S. Using quasigroups for one-one secure encoding. *Proceedings of VIIIth Conference for Logic and Computing – LIRA'97.* September 1997, Novi Sad, 1997.
8. Markovski S., Gligoroski D., Bakeva V. Quasigroup String Processing: Part 1, Maced. Acad. of Sci. and Arts, Sc. Math. Tech. Scien. XX 1–2, 1999.
9. Gligoroski D., Markovski S. Cryptographic Potentials of Quasigroup Transformations, manuscript, 2003.
10. Mileva A. Cryptographic Primitives with Quasigroup Transformations: Ph.D. dissertation, University Ss. Cyril and Methodius, Skopje, Macedonia, 2010.

УДК 004.056.2:004.042:53.083.8:53.088.4

ПОРІВНЯННЯ СТАБІЛЬНОСТІ ДАТЧИКІВ ТЕМПЕРАТУРИ НА ОСНОВІ МЕТОДУ ДИСПЕРСІЇ АЛЛАНА В СИСТЕМАХ КЛІМАТИЧНОГО КОНТРОЛЮ

Д. А. Росолик, В. Г. Крижановський

Анотація. Дослідження спрямоване на оцінку стабільності і точності вимірювання залежностей температури середовища за допомогою сенсорів DHT22 та DS18B20, які широко використовуються в кліматичному обладнанні, за допомогою методів дисперсії Аллана. Проаналізовано три основні методи обчислення дисперсії Аллана: класичний, модифікований та перекриваючий. На основі експериментальних даних, отриманих з прототипу сенсорного вузла Інтернету речей, проведено порівняльний аналіз стабільності сенсорів. Результати дослідження надають цінну інформацію для вибору датчиків залежно від специфіки застосування в системах кліматичного контролю.
Ключові слова: сенсори, дисперсія Аллана, кліматичне обладнання, стабільність вимірювання.

У сучасному світі кліматичне обладнання відіграє критичну роль у забезпеченні комфорту та безпеки людей, а також у підтримці оптимальних умов для різноманітних технологічних процесів. Ключовим аспектом ефективності такого обладнання є точність і надійність сенсорних даних, які воно отримує та обробляє. Однак сенсори піддаються впливу різноманітних факторів, що можуть призвести до нестабільності вимірювань, дрейфу показників та накопичення похибок з часом. Обчислення дисперсії Аллана дає змогу окремо аналізувати впливи, які відрізняються часовим масштабом, що дає змогу розділяти похибки вимірювальної системи від характерних сторонніх впливів [1].

Актуальність дослідження методів обчислення дисперсії Аллана для аналізу сенсорних даних кліматичного обладнання зумовлена зростаючими вимогами до точності та надійності систем кліматичного контролю [2], неефективність роботи яких призводить до перевитрат енергії на опалення та кондиціонування приміщень.

Метою дослідження є провести оцінку стабільності та точності процесу вимірювання сенсорів DHT22 і DS18B20 через аналіз дисперсії Аллана, що надає цінну інформацію для вибору датчика залежно від специфіки застосування.

Проблема стабільності й точності сенсорів у кліматичному обладнанні є критичною для багатьох галузей. Наприклад: