Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
https://doi.org/10.36930/40340720
Article received 13.11.2024
Article accepted 25.11.2024
UDC 004.(021+023+67+9):519.6
Correspondence author: P. Yu. Grytsiuk pavlo.y.hrytsiuk@lpnu.ua
ISSN 1994-7836 (print)
ISSN 2519-2477 (online)

П. Ю. Грицюк, Ю. І. Грицюк
Національний університет "Львівська політехніка", м. Львів, Україна

МЕТОДИ ГЕНЕРУВАННЯ ПОЛІНОМІВ ФІБОНАЧЧІ ТА ОСОБЛИВОСТІ ЇХ ВИКОРИСТАННЯ ДЛЯ ШИФРУВАННЯ ДАНИХ

Розроблено методи генерування послідовностей поліномів Фібоначчі n-го степеня як основи шифрування потокових і блокових даних, що дає можливість ефективно передавати каналами зв'язку відповідні повідомлення різної величини. З'ясовано, що за останнє десятиліття надруковано значну кількість публікацій, в кожній з яких обґрунтовано різні підходи до генерування поліномів Фібоначчі та доведено доцільність їх використання для шифрування даних. Проте, більшість досліджень стосується окремих процедур захисту даних, що в теорії та практиці криптографії трапляються вкрай рідко. Встановлено основну складність проблеми генерування послідовностей поліномів Фібоначчі n-го степеня, які є основою шифрування потокових і блокових даних, що дасть можливість здійснювати ефективний їх захист. Наведено відомі способи подання чисел Фібоначчі та Люка, а також поліномів Фібоначчі, які можна застосувати у традиційному методі шифрування даних. Встановлено, що в послідовностях чисел Фібоначчі та Люка, де відношення двох послідовних доданків наближається до золотого перерізу, їхні члени є наближеннями цілих степенів золотого перерізу. Запропоновано метод матричного подання поліномів Фібоначчі та їх обернених еквівалентів, які можна застосувати у традиційному методі шифрування даних. Для цього необхідно перемножити спеціальну матрицю n-го порядку з відповідними коефіцієнтами на поліном n-го степеня, внаслідок чого отримаємо набір поліномів Фібоначчі $F_n(x)$ відповідного степеня. Зазвичай, спеціальна матриця є нижньою трикутною матрицею, всі елементи головної діагоналі якої одиниці. Розроблено метод генерування поліноміальних матриць Фібоначчі n-го степеня та їх обернених матриць, елементами яких є поліноми Фібоначчі, які можна застосувати у традиційному методі шифрування даних. Оскільки поліноміальні оберненні матриці використовують для розшифрування даних, то їхнє генерування має мати загальний вигляд. Розроблено ПЗ, яке дає змогу генерувати поліноміальні матриці Фібоначчі n-го степеня та m-го поряду, а також їхні обернені поліноміальні матриці аналогічного степеня та поряду. За результатами виконаного дослідження зробити висновки та надано відповідні рекомендації щодо їх практичного використання як основи для шифрування потокових і блокових даних, що дасть змогу ефективно передавати каналами зв'язку відповідні повідомлення різної величини.

Ключові слова: числа Фібоначчі; рекурентна послідовність поліномів; золотий переріз; шифрування потокових і блокових даних; поліноміальна матриця Фібоначчі; обернена поліноміальна матриця.

Вступ / Introduction

Таємниче число Фібоначчі, яке становить 1,618, розбурхує фантазії багатьох вчених вже протягом останнього тисячоліття [48]. Хтось вважає це число початком світобудови, хтось називає його числом Бога, а хтось просто застосовує його на практиці й отримує неймовірні архітектурні творіння, мистецькі шедеври та унікальні математичні викладки. Числа Фібоначчі було виявлено навіть в пропорціях знаменитої "Вітрувіанської людини" Леонардо да Вінчі, який вважав, що знамените число, яке прийшло з математики, керує всім Всесвітом.

Числа Фібоначчі та Люка [20] є фундаментальною математичною основою, яка має важливе значення для сучасних інформаційних технологій (ІТ). Їх універсальність відчутна в різних ІТ-галузях – від розроблення ПЗ до криптографії та фінансових технологій. Розуміння послідовностей таких чисел допомагає програмістам поглибити свої знання з організації структур даних і алгоритмів їх оброблення, покращити навики програмування чи тестування, а також розробляти дещо ефективніші програми для різних областей знань. Тому, виходячи з їх широкого застосування, кожен програміст повинен бути ознайомлений з концепцією генерування послідовностей чисел Фібоначчі та Люка [51], щоб краще їх розуміти та використовувати у своїй роботі.

У 2005 році О. Стахов у своїй роботі [46] запропонував так звану теорію шифрування даних і коригування помилок p-числами Фібоначчі, метод дешифрування яких використовував певні властивості цих чисел, їх узагальнення та наближення до золотого перерізу [3]. Автор стверджував, що запропонований метод (роз)шифрування даних має здатність виправлення помилок 93,33 % і що такі коди мають надмірність 33,3 %. Проте, його обнадійливі заяви в багатьох дослідників [5, 6, 8] викликали деякі підозри насамперед з точки зору теорії інформації. Вони вважали, що потрібно провести дещо глиб-

Інформація про авторів:
Грицюк Павло Юрійович, магістр, аспірант, кафедра автоматизованих систем управління. **Email:** pavlo.y.hrytsiuk@lpnu.ua; https://orcid.org/0009-0003-5409-2043
Грицюк Юрій Іванович, д-р техн. наук, професор, кафедра програмного забезпечення. **Email:** yurii.i.hrytsiuk@lpnu.ua; https://orcid.org/0000-0001-8183-3466

Цитування за ДСТУ: Грицюк П. Ю., Грицюк Ю. І. Методи генерування поліномів Фібоначчі та особливості їх використання для шифрування даних. Науковий вісник НЛТУ України. 2024, т. 34, № 7. С. 161–173.
Citation APA: Grytsiuk, P. Yu., & Hrytsiuk, Yu. I. (2024). Methods for generating Fibonacci polynomials and features of their use for data encryption. *Scientific Bulletin of UNFU*, 34(7), 1615–173. https://doi.org/10.36930/40340720

ший і точніший аналіз результатів дослідження О. Стахова як щодо надмірності кодів, так і щодо їхньої можливості виявлення та виправлення помилок у зашифрованих повідомленнях.

Теорія шифрування даних упродовж багатьох десятиліть має важливе значення для інформаційно-комунікаційних технологій [27], внаслідок чого розроблено багато різних підходів до виявлення та виправлення можливих помилок, що виникають під час передачі зашифрованих повідомлень [18]. Водночас, застосування сучасних методів шифрування даних з виправленням помилок під час розроблення криптографічних систем [19, 22, 25], стійких до квантових атак, зацікавило багатьох науковців до творчих пошуків і сприяло появі результатів нових досліджень. Проте, основний недолік багатьох криптографічних методів шифрування даних з виправленням помилок у тому, що вони використовують ключі великої розмірності з недостатньою коригувальною здатністю [23, 24, 26]. Тому розроблення нових підходів до (роз)шифрування даних з виявленням і виправленням помилок є важливою дослідною роботою, а для криптографічних систем проблема пошуку компактних ключів досі є відкритою.

У багатьох роботах [4, 9, 16, 33, 38, 39, 45] наведено результати дослідження щодо особливостей генерування поліномів Фібоначчі та Люка і похідних від них. Автори вважають, що поліноми Фібоначчі та Люка є природним розширенням їхніх відповідних послідовностей чисел, тому їм притаманні багато їхніх безпосередніх властивостей. Також вони наводять похідні цих поліномів у формі відповідних згорток, що дало їм змогу сформувати сімейство відповідних послідовностей. Ними також доведено багато співвідношень для похідних поліномів Фібоначчі та Люка. Послідовність поліномів Фібоначчі та золотий переріз з'явилися в багатьох галузях науки, в т.ч. фізиці високих енергій, криптографії та шифруванні даних [3, 12].

Проте, виконана чимала кількість досліджень [2, 10, 17, 28, 42, 44, 49, 52] переважно стосується різних підходів до генерування поліномів Фібоначчі та Люка, а також їх використання для шифрування даних. Водночас, як окрема процедура такий підхід в практиці захисту та передачі даних трапляється вкрай рідко. Тому виникає потреба проведення додаткових досліджень щодо ефективних методів генерування поліномів Фібоначчі, а також встановлення певних особливості їх використання для шифрування даних тільки як локального методу.

Об'єкт дослідження – генерування поліномів Фібоначчі як основи для шифрування даних.

Предмет дослідження – алгоритми і методи генерування послідовностей поліномів Фібоначчі n-го степеня, які стануть основою шифрування потокових і блокових даних, що дасть можливість здійснювати ефективний їх захист.

Мета роботи – розробити методи генерування послідовностей поліномів Фібоначчі n-го степеня як основи шифрування потокових і блокових даних, що дасть змогу ефективно передавати каналами зв'язку відповідні повідомлення різної величини.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- проаналізувати останні дослідження і публікації та встановити основну складність проблеми генерування послідовностей поліномів Фібоначчі n-го степеня, які стануть основою шифрування потокових і блокових даних, що дасть можливість здійснювати ефективний їх захист;
- навести традиційні способи подання чисел Фібоначчі та Люка, а також поліномів Фібоначчі, що мають багато корисних властивостей, використати тільки ті із них, які можна застосувати у традиційному методі шифрування даних;
- запропонувати метод матричного подання поліномів Фібоначчі та їх обернених еквівалентів, які можна застосувати у традиційному методі шифрування даних, навести конкретний приклад їх застосування;
- розробити метод генерування поліноміальних матриць Фібоначчі n-го степеня та їх обернених матриць, елементами яких є поліноми Фібоначчі, які можна застосувати у традиційному методі шифрування даних, навести конкретний приклад їх застосування;
- зробити висновки за результатами виконаного дослідження та надати відповідні рекомендації щодо їх практичного використання.

Аналіз останніх досліджень та публікацій. Послідовності чисел Фібоначчі та Люка є основою математичного збагачення дослідників певними знаннями та здобули популярність через можливість широкого використання [46]. Водночас, різні послідовності поліномів Фібоначчі та Люка хоча й трапляються інколи в науковій літературі, позаяк вони тісно пов'язані між собою [2], однак вони значно менше досліджені. З розвитком комп'ютерної техніки поліноми Фібоначчі та Люка почали застосовувати в різних областях знань [33], в т.ч. й для шифрування даних, насамперед матричним методом [24].

У роботі [31] розглянуто особливості генерування чисел Фібоначчі та Люка з різними додатками, де зосереджено вичерпний аналіз найцікавіших чисельних математичних компонент. Автор вважає, що числа Фібоначчі та Люка протягом століття цікавлять математиків-аматорів і професійних математиків [51]. Їхня ж робота є першою спробою зібрати наявну історію та провести авторитетний аналіз цих відомих цілочисельних компонент разом із множиною захопливих програмних рішень, повних прикладів і цікавих вправ, які пропонують численні можливості для дослідження та експериментування. Числа Фібоначчі та Люка з додатками надають математикам велику кількість довідкового матеріалу в одному зручному зібранні та представляють глибокий і цікавий ресурс для ентузіастів будь-якого рівня та з будь-яким набутим досвідом.

У роботі [1] проаналізовано деякі властивості гаусових чисел Фібончі та Люка k-порядку. Автори визначили та вивчили числа Фібоначчі та Люка k-порядку з граничними умовами. Вони ідентифікували та підтвердили генеруючі функції, формули Біне, формули підсумовування, матричне подання гаусових чисел Фібоначчі k-порядку та деякі істотні зв'язки між гаусовими числами Фібоначчі k-порядку та числами Люка k-порядку, пов'язані зі звичайними числами Фібоначчі k-порядку.

У роботі [29] наведено деякі результати дослідження щодо непарних і парних індексованих послідовностей чисел Фібоначчі та Люка, доведено єдиність суми елементів їхніх скінченних підмножин. Показано, що непарні або парні індексовані послідовності чисел Фібоначчі та Люка є унікальними суперзростаючими послідовностями. Використовуючи встановлені властивості унікальності, авторами на прикладі показано новий метод криптографії, призначений для шифрування даних.

У роботі [53] розглянуто деякі тотожності узагальнених послідовностей чисел Фібоначчі та Люка. Спо-

чатку автори ввели поняття узагальненої послідовності чисел Люка, де навели перелік елементарних співвідношень щодо узагальнених послідовностей чисел Фібоначчі та Люка. Потім вони навели узагальнення формул Біне для узагальнених послідовностей чисел Фібоначчі та Люка, а також різні можливості їх застосування. Також дослідники вивели багато тотожностей і співвідношень відповідних конгруенції для узагальнених послідовностей чисел Фібоначчі та Люка за допомогою операторного методу.

Як зазначено в роботах [7, 41], так звані *p*-числа Фібоначчі також можна узагальнити, враховуючи деякі лінійні рекурентні їхні послідовності, такі як *p*-числа Люка [32, 42] або Пелля-Люка [39], які дещо узагальнюють *p*-числа Фібоначчі та методи (роз)шифрування даних з їхнім використанням. Наприклад, автор роботи [40] запропонував використовувати рекурентні послідовності $F_n^{(p)}(x,y)$, застосовуючи поліноми Фібоначі [9]. Подальші узагальнення результатів вирішення цієї проблеми можна знайти в роботах [4, 5, 38, 15, 35].

У роботі [10] наведено деякі зауваги щодо узагальнених чисел Фібоначчі-Люка та узагальнених кватерніонів Фібоначчі-Люка. Автори запропонували породжувальні функції для узагальнених чисел Фібоначчі-Люка та для їхніх узагальнених кватерніонів, а також для них тотожність Кассіні та інші їхні цікаві властивості, різні можливості застосування цих елементів.

У роботі [36] наведено ефективний чисельний метод, заснований на поліномах Фібоначчі, для розв'язування дробових диференціальних рівнянь. Встановлено, що послідовність чисел Фібоначчі важлива через так звану золоту пропорцію, яка описує передбачувані моделі для всього. Водночас, поліноми Фібоначчі пов'язані безпосередньо з числами Фібоначчі. У своїй роботі автор розширює їхню застосовність, використовуючи їх для розв'язання дробових диференціальних рівнянь FDE (англ. *Fractional Differential Equations)* і систем дробових диференціальних рівнянь SFDE (англ. *System of Fractional Fractional Differential Equations*). За допомогою дробового інтегрального оператора Рімана–Ліувіля для гібридної функції дробового порядку блочно-імпульсних функцій і поліномів Фібоначчі, визначених у цій роботі, розв'язок розглянутих FDE та SFDE зводиться до системи алгебраїчних рівнянь, яку можна розв'язати ітераційним методом Ньютона. Дробовий порядок виходить шляхом перетворення x в x^{α}, де $\alpha > 0$. Порівняно з іншими моделями, запропонований авторами метод у деяких ситуаціях кращий на дванадцять порядків. Бували ситуації, коли автори отримували дещо точніший розв'язок порівняно з результатами, отриманими класичними методами. Запропонований авторами метод виявляється простим і ефективним при розв'язуванні нелінійних задач із заданими початковими значеннями.

У роботі [41] наведено привабливі, як на перший погляд, показники надійності теорії шифрування даних поліномами Фібоначчі. Розроблено новий клас квадратних $Q_{pm}^{n}(x)$-матриць *n*-го степеня та *pm*-го порядку для шифрування даних, де $p \geq 3$, $m \geq 1$, $n \geq 1$, $x \geq 1$, елементами яких є поліноми Фібоначчі. Запропонований метод дешифрування даних випливає з можливості отримання відповідних обернених $Q_{pm}^{-n}(x)$-матриць, визначник яких становить ±1. При цьому спостерігалися як великі швидкості виконання таких процедур, так і отриманих зашифрованих повідомлень, стійких до криптографічних атак [19, 25].

У роботі [44] наведено результати побудови дуально-узагальнених комплексних кватерніонів Фібоначчі та Люка. Автори розглядали властивості як дуально-узагальненого комплексного числа, так і кватерніона. Також було отримано загальні рекурентні співвідношення для відповідних послідовностей кватерніонів, формули Біне, тотожності Тагіурі (або Вайди), Гонсбергера, д'Оканя, Кассіні та Каталана. Наведено набір матричних подань цих спеціальних кватерніонів і виражено добуток дуально-узагальнених комплексних кватерніонів Фібоначчі та Люка у вигляді їхніх різних матричних подань.

У роботі [49] розглянуто нове застосування теорії шифрування числами Фібоначчі та Люка. Автори вважають, що алгоритми (роз)шифрування мають велике значення для покращення інформаційної безпеки, яка в останні роки стала серйозною проблемою багатьох фірм і організацій. Вони навели два нових алгоритми (роз)шифрування з використанням *Q*-матриць і *R*-матриць Фібоначчі. Розроблені моделі засновані на використанні заблокованих матриць повідомлень і шифруванні кожної такої матриці різними ключами. Автори вважають, що нові алгоритми не тільки підвищують безпеку інформації, але й мають високу коригувальну здатність.

У роботі [3] розроблено узагальнені співвідношення між елементами матриці шифрування даних числами Фібоначчі. Автори розглядали клас квадратної матриці Фібоначчі (*p*+1)-порядку, елементи якої базуються на *p*-числах Фібоначчі з визначником, що становить ±1. Вони стверджують, що існує зв'язок між числами Фібоначчі з початковими членами, який відомий як формула Кассіні, а саме: $F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$, $n \geq 1$. Оригінальний метод (роз)шифрування даних числами Фібоначчі випливає з аналогічних матриць, де відомим залишається зв'язок між її елементами для випадку $p = 1$ [46]. Також автори встановили узагальнені співвідношення між елементами матриці шифрування даних для різних значень *p*. Наприклад, для $p = 2$ достовірність запропонованого методу становить 99,80 % і зростає зі збільшенням цього значення [50].

У роботі [33] розроблено метод шифрування будь-яких повідомлень на підставі поліномів Фібоначчі. Для цілих чисел $m \geq 2$, $x \geq 1$ і $n \geq 1$ було розроблено $\overline{\overline{Q}}_m^n$-матрицю *n*-го степеня розміром $m \times m$, яку названо $\overline{\overline{Q}}_m^n(x)$-матрицею шифрування даних, елементами якої є поліноми Фібоначчі. Для розшифрування даних автори ввели обернену $\overline{\overline{Q}}_m^{-n}(x)$-матрицю, особливість якої у тому, що їхній визначник становить ±1.

У роботі [4] наведено узагальнену теорію шифрування даних на (*m*,*t*)-розширенні поліномів *p*-числами Фібоначчі. Насамперед вони визначають (*m*,*t*)-розширення *p*-чисел Фібоначчі та золотих (*p*,*m*,*t*)-пропорцій, де $p \geq 0$ є цілим невід'ємним числом, $m > 0$ і $t > 0$. Автори встановили співвідношення між золотою (*p*,*m*,*t*)-пропорцією, між золотою (*p*,*m*)-пропорцією та між золотою *p*-пропорцією. У такий спосіб вони визначили квадратну $G_{p,m,t}$-матрицю Фібоначчі. Також автори показали, що, за умови правильного вибору початкових членів

для (m,t)-розширення p-чисел Фібоначчі, можна застосувати процедуру (роз)шифрування даних з використанням $G_{p,m,t}$-матриці Фібоначчі. Було зроблено висновок, що для $t = 1$ зв'язки між елементами матриці шифрування даних для різних значень p і m збігаються з аналогічними початковими членами чисел Фібоначчі [7].

У роботі [5] запропоновано нову теорію шифрування даних з використанням узагальнених n-крокових поліномів Фібоначчі. На підставі цих поліномів було визначено новий клас квадратної $M_{h,n}(x)$-матриці n-го порядку ($x \geq 1$) та отримано певні співвідношення між елементами цієї матриці. В результатах дослідження було обговорено достовірність цього методу, де показано, що для $n = 2$ його коригувальна здатність становить 93,33 %, тоді як для $n = 3$ його достовірність вже становить 99,80 %. Цікавою особливістю розробленого методу (роз)шифрування даних є те, що його достовірність не залежить від коефіцієнтів полінома Фібоначчі, за винятком n-го коефіцієнта $h_n(x) = 1$, і зростає зі збільшенням порядку квадратної $M_{h,n}(x)$-матриці.

У роботі [16] наведено результати дослідження щодо послідовностей k-чисел Фібоначчі, їхніх поліномів і похідних. Автори вважають, що k-поліноми Фібоначчі є природним розширенням k-чисел Фібоначчі, багато їхніх властивостей допускають пряме доведення. Також вони наводять похідні цих поліномів у формі згортки k-поліномів Фібоначчі, що дало їм змогу у легкій формі подати сімейство цілих послідовностей новим опосередкованим і прямим способом. Доведено багато співвідношень для похідних поліномів Фібоначчі. Наведені результати дослідження були отримані внаслідок дивовижної присутності золотого перерізу [3] в рекурсивному поділі трикутників у контексті методу скінченних елементів і трикутних уточнень. Водночас, у роботі [37] автори показали зв'язок між поділом найдовшого ребра 4-трикутника та k-числами Фібоначчі, як інший приклад зв'язку між геометрією та числами. З іншого боку, в роботі [16] k-числа Фібоначчі були задані в явному вигляді, де за допомогою простих аргументів було доведено багато їхніх властивостей. Зокрема, k-числа Фібоначчі були пов'язані з так званим 2-трикутником Паскаля.

У роботі [38] розглянуто 3-поліноми Фібоначчі в сімействі чисел Фібоначчі. Автори використовують нове сімейство чисел Фібоначчі, також визначено самі поліноми Фібоначчі. Було продемонстровано деякі важливі властивості цього полінома, а отримані авторами поліноми порівнювали з відомими поліномами Фібоначчі. Отриманий ними новий поліном був виражений як поліном Фібоначчі, де було наведено його вираз і доведено деякі теореми, пов'язані з цими поліномами.

У роботі [50] проаналізовано так звані відстані між елементами поліномів Фібоначчі. Автори наводять новий вид узагальнених поліномів Фібоначчі в сенсі відстані між його елементами. Наведено пряму формулу, твірну функцію та матричні генератори для цих поліномів. Окрім цього, вони наводять графову інтерпретацію цих поліномів, їх зв'язки з трикутником Паскаля та доводять деякі тотожності для них.

У роботі [37] проаналізовано поліноми Фібоначчі та детерміновані тотожності, пов'язані з ними. Встановлено, що поліноми Фібоначчі та поліноми Люка відомі тим, що володіють чудовими та дивовижними властивостями, а також відповідними детермінованими тотожностями, які було детально описано. З'ясовано, що записи детермінованих тотожностей задовольняють рекурентні співвідношення поліномів Фібоначчі та поліномів Люка.

Отже, за результатами проведеного аналізу останніх досліджень та публікацій стосовно наявних підходів до генерування поліномів Фібоначчі, а також особливостей їх використання для шифрування даних було встановлено, що навіть за останнє десятиліття виконано багато різноманітних досліджень, в кожному з яких тією чи іншою мірою обґрунтовано різні підходи до генерування таких поліномів і доведено доцільність їх використання для шифрування даних. Водночас, як окрема процедура захисту потокових і блокових даних поліномами Фібоначчі у теорії та практиці криптографії трапляються вкрай рідко. Тому проведення додаткових досліджень щодо ефективних методів генерування поліномів Фібоначчі, а також встановлення певних особливості їх використання для шифрування потокових і блокових даних тільки як локального методу є актуальною проблемою, яку й спробуємо частково вирішити в цьому дослідженні.

Результати дослідження та їх обговорення / Research results and their discussion

1. ***Подання чисел Фібоначчі та Люка***. Послідовність чисел Фібоначчі визначають таким рекурентним співвідношенням [46, 51]:

$$F_{n+1}(x) = xF_n(x) + F_{n-1}(x), \quad (1)$$

де: $F_0(x) = 0$, $F_1(x) = 1$ для $n \geq 2$. Послідовність чисел Фібоначчі для $x = 1$ має вигляд: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10916, ...

Послідовність чисел Фібоначчі для від'ємних індексів визначають як

$$F_{-n}(x) = (-1)^{n+1}F_n(x) \text{ для } n \geq 1. \quad (1)$$

Числа Люка – цілочисельна послідовність, названа на честь математика Франсуа Едуара Анатоля Люка (1842–1891), який вивчав як їхню послідовність, так і тісно пов'язані числа Фібоначчі [31]. Числа Люка та числа Фібоначчі утворюють доповняльні випадки послідовностей чисел Люка. В обох послідовностях чисел, де відношення двох послідовних доданків наближається до золотого перерізу, їхні члени фактично є наближеннями цілих степенів золотого перерізу [3].

Для генерування послідовності чисел Люка використовують таке рекурентне співвідношення з різними початковими значеннями [20]:

$$L_{n+1}(x) = xL_n(x) + L_{n-1}(x), \quad (2)$$

де $L_0(x) = 2$, $L_1(x) = x$ для $n \geq 2$ і $L_n(x) = F_{n+1}(x) + F_{n-1}(x)$ для $n \in \mathbb{Z}$. Послідовність чисел Люка для $x = 1$ має такий вигляд: 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, 3571, 5778, 9349, 15127, 24476, 39603, 64079, 103682, 167761, 271443... .

2. ***Подання поліномів Фібоначчі***. Метод генерування поліномів Фібоначчі полягає у використанні рекурентного співвідношення (1), згідно з яким спочатку потрібно змінну x помножити послідовно на елементи даного полінома, потім потрібно згрупувати схожі доданки з елементами попереднього полінома, внаслідок чого отримаємо елементи наступного полінома. Наприклад, за вхідних поліномів $F_6(x) = x^5 + 4x^3 + 3x$ і $F_7(x) = x^6 + 5x^4 + 6x^2 + 1$ наступний поліном має такий вигляд:

$$F_8(x) = xF_7(x) + F_6(x) = x(x^6 + 5x^4 + 6x^2 + 1) + (x^5 + 4x^3 + 3x) =$$

$= x^7 + 5x^5 + 6x^3 + x + x^5 + 4x^3 + 3x = x^7 + 6x^5 + 10x^3 + 4x.$

Декілька поліномів Фібоначчі мають такий вигляд:

$F_0(x) = 0;\ F_1(x) = 1;\ F_2(x) = x;$
$F_3(x) = x^2 + 1;$
$F_4(x) = x^3 + 2x;$
$F_5(x) = x^4 + 3x^2 + 1;$
$F_6(x) = x^5 + 4x^3 + 3x;$
$F_7(x) = x^6 + 5x^4 + 6x^2 + 1;$
$F_8(x) = x^7 + 6x^5 + 10x^3 + 4x;$
$F_9(x) = x^8 + 7x^6 + 15x^4 + 10x^2 + 1;$
$F_{10}(x) = x^9 + 8x^7 + 21x^5 + 20x^3 + 5x.$
… … … …
$F_{15}(x) = x^{14} + 13x^{12} + 66x^{10} + 165x^8 + 210x^6 + 126x^4 + 28x^2 + 1.$

Декілька поліномів Люка мають такий вигляд:

$L_0(x) = 2;\qquad L_1(x) = x;$
$L_2(x) = x^2 + 2;$
$L_3(x) = x^3 + 3x;$
$L_4(x) = x^4 + 4x^2 + 2;$
$L_5(x) = x^5 + 5x^3 + 5x;$
$L_6(x) = x^6 + 6x^4 + 9x^2 + 2;$
$L_7(x) = x^7 + 7x^5 + 14x^3 + 7x;$
$L_8(x) = x^8 + 8x^6 + 20x^4 + 16x^2 + 2;$
$L_9(x) = x^9 + 9x^7 + 27x^5 + 30x^3 + 9x;$
$L_{10}(x) = x^{10} + 10x^8 + 35x^6 + 50x^4 + 25x^2 + 2;$

$$L_{0-10}(x) = \begin{pmatrix} 2 \\ x \\ x^2+2 \\ x^3+3x \\ x^4+4x^2+2 \\ x^5+5x^3+5x \\ x^6+6x^4+9x^2+2 \\ x^7+7x^5+14x^3+7x \\ x^8+8x^6+20x^4+16x^2+2 \\ x^9+9x^7+27x^5+30x^3+9x \\ x^{10}+10x^8+35x^6+50x^4+25x^2+2 \end{pmatrix}.$$

Отже, послідовності поліномів Фібоначчі та Люка [2, 51] є природним розширенням відповідних послідовностей чисел Фібоначчі та Люка, тому багато їхніх властивостей допускають пряме доведення [38, 16, 53].

3. ***Матричне подання поліномів Фібоначчі***. Часто в математичних розрахунках, особливо це стосується криптографічних методів захисту даних, доводиться мати справу з матричним поданням поліномів Фібоначчі для прямого ходу та їх оберненим виглядом – для зворотного. Для цього необхідно перемножити спеціальну матрицю *n*-го порядку з відповідними коефіцієнтами на поліном *n*-го степеня, внаслідок чого отримаємо набір поліномів Фібоначчі $F_n(x)$ відповідного степеня. Зазвичай, під спеціальною матрицею розуміють нижню трикутну матрицю, всі елементи головної діагоналі якої є одиничними [38, 12, 21].

Для генерування поліномів Фібоначчі та їх обернених еквівалентів потрібно використати спеціальну матрицю *n*-го порядку з відповідними коефіцієнтами та поліном *n*-го степеня. Метод генерування поліномів Фібоначчі полягає у виконанні матричної дії множення спеціальної матриці *n*-го порядку на поліном *n*-го степеня, внаслідок чого отримаємо набір поліномів Фібоначчі і 1-го до *n*-го степеня. Метод генерування обернених еквівалентів поліномів Фібоначчі полягає у знаходженні матриці, оберненої до спеціальної матриці *n*-го порядку, та виконанні матричної дії множення оберненої матриці *n*-го порядку на поліном *n*-го степеня, внаслідок чого отримаємо набір обернених поліномів Фібоначчі від 1-го до *n*-го степеня.

Математично це матиме такий вигляд:

$$\bar{F}_n(x) = \bar{\bar{A}}_{n\times n} \times \bar{X}_n, \qquad (3)$$

де: $\bar{F}_n(x)$ – набір поліномів Фібоначчі від 1-го до *n*-го степеня; $\bar{\bar{A}}_{n\times n}$ – спеціальна матриця *n*-го порядку; $\bar{X}_n$ – елементи полінома *n*-го степеня.

Нижче наведено набір поліномів Фібоначчі $F_n(x)$ від 1-го до 7-го степеня, а саме:

$$\bar{F}_{1-7}(x) = \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 0&2&0&1&0&0&0&0 \\ 1&0&3&0&1&0&0&0 \\ 0&3&0&4&0&1&0&0 \\ 1&0&6&0&5&0&1&0 \\ 0&4&0&10&0&6&0&1 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \\ x^7 \end{pmatrix} = \begin{pmatrix} 1 \\ x \\ x^2+1 \\ x^3+2x \\ x^4+3x^2+1 \\ x^5+4x^3+3x \\ x^6+5x^4+6x^2+1 \\ x^7+6x^5+10x^3+4x \end{pmatrix}. \qquad (4)$$

Водночас, для отримання обернених поліномів Фібоначчі потрібно перемножити матрицю, обернену до матриці коефіцієнтів, на поліном, внаслідок чого отримаємо набір обернених поліномів Фібоначчі $F_n^{-1}(x)$ відповідного степеня, а саме:

$$\bar{F}_{1-7}^{-1}(x) = \begin{pmatrix} 100\,0\,0000 \\ 010\,0\,0000 \\ 101\,0\,0000 \\ 020\,1\,0000 \\ 103\,0\,1000 \\ 030\,4\,0100 \\ 106\,0\,5010 \\ 0401\,00601 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ x \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \\ x^7 \end{pmatrix} =$$
$$= \begin{pmatrix} 1&0&0&0&0&0&0\,0 \\ 0&1&0&0&0&0&0\,0 \\ -1&0&1&0&0&0&0\,0 \\ 0&-2&0&1&0&0&0\,0 \\ 2&0&-3&0&1&0&0\,0 \\ 0&5&0&-4&0&1&0\,0 \\ -5&0&9&0&-5&0&1\,0 \\ 0&-14&0&14&0&-6&01 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \\ x^7 \end{pmatrix} = \begin{pmatrix} 1 \\ x \\ x^2-1 \\ x^3-2x \\ x^4-3x^2+2 \\ x^5-4x^3+5x \\ x^6-5x^4+9x^2-5 \\ x^7-6x^5+14x^3-14x \end{pmatrix}. \qquad (5)$$

Математично це матиме такий вигляд:

$$\bar{F}_n^{-1}(x) = \bar{\bar{A}}_{n\times n}^{-1} \times \bar{X}_n, \qquad (6)$$

де: $\bar{F}_n^{-1}(x)$ – набір обернених поліномів Фібоначчі від 1-го до *n*-го степеня; $\bar{\bar{A}}_{n\times n}$ – матриця, до спеціальної матриці *n*-го порядку; $\bar{X}_n$ – елементи полінома *n*-го степеня. Оскільки елементи спеціальної матриці є цілі числа, розміщені нижче головної діагоналі, а її визначник становить 1 (одиниця), то обернену матрицю можна визначити звичайними методами, а її елементи також будуть цілими числами, в т.ч. й від'ємними.

Нижче наведено набір поліномів Фібоначчі $\bar{F}_n^3(x)$, піднесених до 3-го степеня, та їх обернених еквівалентів $\bar{F}_n^{-3}(x)$ від 1-го до 7-го степеня, а саме:

$$\bar{F}_{1-7}^{3}(x) = \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 0&2&0&1&0&0&0&0 \\ 1&0&3&0&1&0&0&0 \\ 0&3&0&4&0&1&0&0 \\ 1&0&6&0&5&0&1&0 \\ 0&4&0&10&0&6&0&1 \end{pmatrix}^3 \begin{pmatrix} 1 \\ x \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \\ x^7 \end{pmatrix} =$$
$$= \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 3&0&1&0&0&0&0&0 \\ 0&6&0&1&0&0&0&0 \\ 12&0&9&0&1&0&0&0 \\ 0&33&0&12&0&1&0&0 \\ 51&0&63&0&15&0&1&0 \\ 0&174&0&102&0&18&0&1 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \\ x^7 \end{pmatrix} = \begin{pmatrix} 1 \\ x \\ x^2+3 \\ x^3+6x \\ x^4+9x^2+12 \\ x^5+12x^3+33x \\ x^6+15x^4+63x^2+51 \\ x^7+18x^5+102x^3+174x \end{pmatrix}.$$

$$\vec{F}_{1\text{–}8}^{-3}(x)=\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\1&0&1&0&0&0&0&0\\0&2&0&1&0&0&0&0\\1&0&3&0&1&0&0&0\\0&3&0&4&0&1&0&0\\1&0&6&0&5&0&1&0\\0&4&0&10&0&6&0&1\end{pmatrix}^{-3}\begin{pmatrix}1\\x\\x^2\\x^3\\x^4\\x^5\\x^6\\x^7\end{pmatrix}=$$

$$=\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\-3&0&1&0&0&0&0&0\\0&-6&0&1&0&0&0&0\\15&0&-9&0&1&0&0&0\\0&39&0&-12&0&1&0&0\\-87&0&72&0&-15&0&1&0\\0&-264&0&114&0&-18&0&1\end{pmatrix}\begin{pmatrix}1\\x\\x^2\\x^3\\x^4\\x^5\\x^6\\x^7\end{pmatrix}=\begin{pmatrix}1\\x\\x^2-3\\x^3-6x\\x^4-9x^2+15\\x^5-12x^3+39x\\x^6-15x^4+72x^2-87\\x^7-18x^5+114x^3-264x\end{pmatrix}.$$

Отже, запропоновано метод матричного подання поліномів Фібоначчі та їх обернених еквівалентів, які можна застосувати у традиційному методі шифрування даних. Для цього необхідно перемножити спеціальну матрицю *n*-го порядку з відповідними коефіцієнтами на поліном *n*-го степеня, внаслідок чого отримаємо набір поліномів Фібоначчі $F_n(x)$ відповідного степеня. Зазвичай, спеціальна матриця є нижньою трикутною матрицею, всі елементи головної діагоналі якої є одиницями.

Приклад. Для розуміння зазначеного вище наведемо конкретний приклади шифрування даних з використанням полінома Фібоначчі.

Спробуємо зашифрувати таке повідомлення: *P* = {*До булави треба мудрої голови*!}. З врахуванням пропусків між словами, одновимірний масив символів вхідного повідомлення матиме такий вигляд: *P*' = {*До_булави_треба_мудрої_голови*!}, яке міститиме 30 символів. Для розуміння процесу шифрування цього повідомлення *P* запишемо його у вигляді двовимірного масиву символів ***P***, в якому буде *n* = 5 стовпців і *m* = 6 рядків, а символи повідомлення в цей масив заноситимемо рядками за такою формулою:

$$\boldsymbol{P}=\left\{P_i=\{p_{ij}=p_{(i-1)\cdot n+j}\},j=\overline{1,n};i=\overline{1,m}\right\}. \qquad (13)$$

Для шифрування даних застосуємо поліном Фібоначчі 3-го степеня такого вигляду:

$$F_4(x)=x^3+2x. \qquad (14)$$

Нижче наведено результати шифрування та розшифрування зазначеного вище повідомлення. Для виконання відповідних розрахунків було використано звичайне середовище MS Excel, яке дає змогу не тільки здійснювати складні обчислення, але й наочно їх подавати, що значно сприяє розумінню виконуваних дій.

Прямий хід. Спочатку символи повідомлення з масиву ***P*** перетворюємо у числові коди відповідно до таблиці ASCII, а саме:

$$\boldsymbol{A}=\left\{A_i=\{a_{ij}=Ord(p_{ij}),j=\overline{1,n};i=\overline{1,m}\right\}, \qquad (15)$$

де: *Ord*(*x*) – функція, аргументом якої є символ, повертає його код в межах від 0 до 255. Нагадаємо, ASCII (англ. *American Standard Code for Information Interchange*) – американський стандартний код для обміну інформацією. ASCII – 8-бітне (однобайтне) кодування, призначене для подання десяткових цифр, латинського та національних алфавітів, знаків пунктуації та керуючих символів, містить 2^8=256 (від 0 до 255) комбінацій кодів.

Застосовуючи поліном Фібоначчі (14), перетворюємо числові коди з масиву (15) у зашифровані повідомлення, а саме

$$\boldsymbol{F}=\left\{F_i=\{f_{ij}=a_{ij}^3+2a_{ij},j=\overline{1,n}\};i=\overline{1,m}\right\}. \qquad (16)$$

Далі, перемноживши отримані значення за модулем *m* = 256, отримуємо зашифровані числові коди

$$\boldsymbol{F'}=\left\{F_i'=\{f_{ij}'=f_{ij\otimes m},j=\overline{1,n}\};i=\overline{1,m}\right\}, \qquad (17)$$

які знову ж таки перетворюємо у символи зашифрованого повідомлення за формулою:

$$\boldsymbol{A'}=\left\{A_i'=\{a_{ij}'=Chr(f_{ij}'),j=\overline{1,n}\};i=\overline{1,m}\right\}, \qquad (18)$$

де: *Chr*(*x*) – функція, аргументом якої є число від 0 до 255, повертає символ із введеним кодом. І, на завершення, символи зашифрованого повідомлення з двовимірного масиву ***A′*** заноситимемо рядками у одновимірний масив *P′* за такою формулою:

$$P'=\left\{\{p'_{(i-1)\cdot n+j}=a_{ij}',j=\overline{1,n}\},i=\overline{1,m}\right\}. \qquad (19)$$

На цьому шифрування вхідного повідомлення завершено.

Зворотний хід. Спочатку символи зашифрованого повідомлення з масиву *P′* перенесемо у двовимірний масив символів ***A′***, в якому буде *n* = 5 стовпців і *m* = 6 рядків, а символи повідомлення в цей масив заноситимемо рядками за такою формулою:

$$\boldsymbol{A'}=\left\{A_i'=\{a_{ij}'=p'_{(i-1)\cdot n+j}),j=\overline{1,n}\};i=\overline{1,m}\right\}. \qquad (20)$$

Символи зашифрованого повідомлення з двовимірного масиву ***A′*** перетворюємо у числові коди відповідно до таблиці ASCII, а саме:

$$\boldsymbol{F'}=\left\{F_i'=\{f_{ij}'=Ord(a_{ij}'),j=\overline{1,n}\};i=\overline{1,m}\right\}. \qquad (21)$$

Застосовуючи поліном Фібоначчі (14), перетворюємо числові коди з масиву (21) у зашифровані повідомлення, а саме

$$\boldsymbol{F''}=\left\{F_i''=\{f_{ij}''=f_{ij}'^3+2f_{ij}',j=\overline{1,n}\};i=\overline{1,m}\right\}. \qquad (22)$$

Далі, перемноживши отримані значення за модулем *m* = 256, отримуємо розшифровані числові коди

$$\boldsymbol{A}=\left\{A_i=\{a_{ij}=f_{ij\otimes m}'',j=\overline{1,n}\};i=\overline{1,m}\right\}, \qquad (23)$$

які знову ж таки перетворюємо у символи розшифрованого повідомлення за формулою:

$$\boldsymbol{P}=\left\{P_i=\{P_{ij}=Chr(a_{ij}),j=\overline{1,n}\};i=\overline{1,m}\right\}. \qquad (24)$$

І, на завершення, символи розшифрованого повідомлення з двовимірного масиву ***P*** заноситимемо рядками у одновимірний масив *P* за такою формулою:

$$P=\left\{\{p_{(i-1)\cdot n+j}=p_{ij},j=\overline{1,n}\};i=\overline{1,m}\right\}. \qquad (25)$$

На цьому розшифрування зашифрованого повідомлення завершено.

Вхідне повідомлення:

P ={До_булави_треба_мудрої_голови!}

1. Прямий хід: ***шифрування повідомлення***

Кількість символів	30	шт.	
Кількість стовпців	5	шт.	
Кількість рядків	6,0	шт.	*m*= 256

P

	1	2	3	4	5
0	Д	о	_	б	у
1	л	а	в	и	_
2	т	р	е	б	а
3	_	м	у	д	р
4	о	ї	_	г	о
5	л	о	в	и	!

A

	1	2	3	4	5		
0	196	238	95	225	243		
1	235	224	226	232	95		
2	242	240	229	225	224		
3	95	236	243	228	240	max=	243
4	238	191	95	227	238	min=	33
5	235	238	226	232	33	S=	6164

F

	1	2	3	4	5
0	7529928	13481748	857565	11391075	14349393
1	12978345	11239872	11543628	12487632	857565
2	14172972	13824480	12009447	11391075	11239872
3	857565	13144728	14349393	11852808	13824480
4	13481748	6968253	857565	11697537	13481748
5	12978345	13481748	11543628	12487632	36003

F′ = F⊗m

	1	2	3	4	5		
0	200	20	221	99	81		
1	169	192	76	208	221		
2	44	224	231	99	192		
3	221	152	81	8	224	max=	231
4	20	189	221	129	20	min=	8
5	169	20	76	208	163	S=	4178

A′

	1	2	3	4	5	
0	И	▯	Э	с	Q	И▯ ЭсQ
1	©	A	L	P	Э	©ALPЭ
2	,	а	з	с	A	,азсA
3	Э		Q		а	Э Q▯ а
4	▯	S	Э	Ґ	▯	▯ SЭҐ▯
5	©	▯	L	P	J	©▯ LPJ

Зашифроване повідомлення:

P′ ={И▯ ЭсQ©ALPЭ,азсAЭ Q▯ а▯ SЭҐ▯ ©▯ LPJ}

2. Зворотний хід: ***розшифрування повідомлення***

Вхідне повідомлення:

P′ = {И▯ ЭсQ©ALPЭ,азсAЭ Q▯ а▯ SЭҐ▯ ©▯ LPJ}

A′

	1	2	3	4	5
0	И	▯	Э	с	Q
1	©	A	L	P	Э
2	,	а	з	с	A
3	Э		Q		а
4	▯	S	Э	Ґ	▯
5	©	▯	L	P	J

F′

	1	2	3	4	5		
0	200	20	221	99	81		
1	169	192	76	208	221		
2	44	224	231	99	192		
3	221	152	81	8	224	max=	231
4	20	189	221	129	20	min=	8
5	169	20	76	208	163	S=	4178

Кількість символів	30
Кількість стовпців	5
Кількість рядків	6,0

F″

	1	2	3	4	5
0	7999600	7960	10793419	970101	531279
1	4826471	7077504	438824	8998496	10793419
2	85096	11238976	12325929	970101	7077504
3	10793419	3511504	531279	496	11238976
4	7960	6750891	10793419	2146431	7960
5	4826471	7960	438824	8998496	4330421

A = F″⊗m

	1	2	3	4	5		
0	196	238	95	225	243		
1	235	224	226	232	95		
2	242	240	229	225	224		
3	95	236	243	228	240	max=	243
4	238	191	95	227	238	min=	33
5	235	238	226	232	33	S=	6164

P

	1	2	3	4	5	
0	Д	о	_	б	у	До_бу
1	л	а	в	и	_	лави_
2	т	р	е	б	а	треба
3	_	м	у	д	р	_мудр
4	о	ї	_	г	о	ої_го
5	л	о	в	и	!	лови!

Розшифроване повідомлення:

P ={*До_булави_треба_мудрої_голови!*}

4. ***Метод генерування матриць Фібоначчі n-го степеня, елементами яких є поліноми Фібоначчі***. Головним завданням будь-якого алгоритму шифрування є ефективне перемішування та розсіювання даних. Для цього часто використовують матриці Фібоначчі.

Якщо $\bar{\bar{X}}$ – квадратна матриця, де $\bar{\bar{X}}^2 = x\bar{\bar{X}} + \bar{\bar{I}}$, то $\bar{\bar{X}}^n = F_n(x)\bar{\bar{X}} + F_{n-1}(x)\bar{\bar{I}}, \forall n \in \mathbb{Z}$ – матриці Фібоначчі [23].

Нехай $\bar{\bar{Q}}(x) = \begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}$. Тоді $\bar{\bar{Q}}^n(x)$-матриця Фібоначчі *n*-го степеня матиме такий вигляд $\bar{\bar{Q}}^n(x) = \begin{bmatrix} F_{n+1}(x) & F_n(x) \\ F_n(x) & F_{n-1}(x) \end{bmatrix}_{2\times 2}$ для всіх $n \in \mathbb{Z}$, а її визначник матиме такий вигляд $det(\bar{\bar{Q}}^n(x)) = F_{n+1}(x)F_{n-1}(x) - F_n^2(x) = (-1)^n$, який ще називають тотожністю Кассіні [24].

З роботи [46] відомо, що $\bar{\bar{Q}}^{1}(x)$-матриці Фібоначчі 1-го степеня розміром 3×3, 4×4, 5×5 і m×m матимуть такий вигляд:

$$\bar{\bar{Q}}_3(x)=\begin{bmatrix} x & 1 & 0 \\ 0 & x & 1 \\ 0 & 1 & 0 \end{bmatrix}_{3\times 3};\ \bar{\bar{Q}}_4(x)=\begin{bmatrix} x & 1 & 0 & 0 \\ 0 & x & 1 & 0 \\ 0 & 0 & x & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{4\times 4};$$

$$\bar{\bar{Q}}_4(x)=\begin{bmatrix} x & 1 & 0 & 0 & 0 \\ 0 & x & 1 & 0 & 0 \\ 0 & 0 & x & 1 & 0 \\ 0 & 0 & 0 & x & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}_{5\times 5};\ \bar{\bar{Q}}_m(x)=\begin{bmatrix} x & 1 & 0 & 0 & \cdots & 0 \\ 0 & x & 1 & 0 & \cdots & 0 \\ 0 & 0 & x & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & x & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}_{m\times m}. \quad (26)$$

Водночас, $\bar{\bar{Q}}^{n}(x)$-матриці Фібоначчі n-го степеня, елементами яких є поліноми Фібоначчі n-го степеня, матимуть зовсім інший вигляд [43]. Наприклад, для m = 2 і 3 та n = 1, 2, 3 і 4, а також для m = 3 і n = 3 і 6 матимемо такі $\bar{\bar{Q}}_m^{n}(x)$-матриці Фібоначчі відповідно розміром 2×2 і 3×2 матимуть такий вигляд:

$$\bar{\bar{Q}}_2^{1}(x)=\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}_{2\times 2};\ \bar{\bar{Q}}_2^{2}(x)=\begin{bmatrix} x^2+1 & x \\ x & 1 \end{bmatrix}_{2\times 2};\ \bar{\bar{Q}}_2^{3}(x)=\begin{bmatrix} x^3+2x & x^2+1 \\ x^2+1 & x \end{bmatrix}_{2\times 2};$$

$$\bar{\bar{Q}}_2^{4}(x)=\begin{bmatrix} x^4+3x^2+1 & x^3+2x \\ x^3+2x & x^2+1 \end{bmatrix}_{2\times 2};\ \bar{\bar{Q}}_3^{3}(x)=\begin{bmatrix} x^3 & 3x^2+1 & 2x \\ 0 & x^3+2x & x^2+1 \\ 0 & x^2+1 & x \end{bmatrix}_{3\times 3}; \quad (27)$$

$$\bar{\bar{Q}}_5^{6}(x)=\begin{bmatrix} x^6 & 6x^5 & 15x^4 & 20x^3+5x & 10x^2+1 \\ 0 & x^6 & 6x^5 & 15x^4+10x^2+1 & 10x^3+4x \\ 0 & 0 & x^6 & 6x^5+10x^3+4x & 5x^4+6x^2+1 \\ 0 & 0 & 0 & x^6+5x^4+6x^2+1 & x^5+4x^3+3x \\ 0 & 0 & 0 & x^5+4x^3+3x & x^4+3x^2+1 \end{bmatrix}_{5\times 5}.$$

У подальшому $\bar{\bar{Q}}_m^{n}(x)$-матрицю будемо називати *поліноміальною матрицею Фібоначчі*. З функції визначника очевидно [43], що $det(\bar{\bar{Q}}_m^{n}(x))=(-x^{m-2})^{n}$. В нашому прикладі матимемо:

$$\det(\bar{\bar{Q}}_3^{3}(x))=x^3(-1)-(3x^2+1)\cdot 0+2x\cdot 0=-x^3;$$
$$\det(\bar{\bar{Q}}_5^{6}(x))=x^6x^{12}-6x^5\cdot 0+15x^4\cdot 0-(20x^3+5x)\cdot 0+$$
$$+(10x^2+1)\cdot 0=x^{18}.$$

Оскільки поліноміальні $\bar{\bar{Q}}_m^{n}(x)$-матриці Фібоначчі можна використовувати для реалізації операції шифрування даних, то аналогічні оберненні матриці також потрібні для процесу розшифрування даних. Інтуїтивно зрозуміло, що ці $\bar{\bar{Q}}_m^{-n}(x)$-матриці Фібоначчі мають бути оберненими до матриць шифрування даних, які прийнято називають *поліноміальними оберненими* $\bar{\bar{Q}}_m^{-n}(x)$*-матрицями Фібоначчі*. Подібно до поліноміальних матриць шифрування даних, відповідні поліноміальні обернені матриці Фібоначчі мають мати також загальний вигляд. Якщо $\bar{\bar{Q}}_2^{1}(x)=\begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix}$, то $\bar{\bar{Q}}_2^{-1}(x)=\begin{bmatrix} 0 & 1 \\ 1 & -x \end{bmatrix}$. Тоді усі співвідношення (27) легко можна поширити на загальний випадок подання поліноміальних обернених матриць Фібоначчі, внаслідок чого отримаємо:

$$\bar{\bar{Q}}_2^{-2}(x)=\begin{bmatrix} 1 & -x \\ -x & 1+x^2 \end{bmatrix}_{2\times 2};\ \bar{\bar{Q}}_2^{-3}(x)=\begin{bmatrix} -x & 1+x^2 \\ 1+x^2 & -2x-x^3 \end{bmatrix}_{2\times 2};$$

$$\bar{\bar{Q}}_2^{-4}(x)=\begin{bmatrix} x^2+1 & -x^3-2x \\ -x^3-2x & x^4+3x^2+1 \end{bmatrix}_{2\times 2}; \quad (28)$$

$$\bar{\bar{Q}}_3^{-3}(x)=\begin{bmatrix} \frac{1}{x^3} & \frac{x^2-1}{x^2} & \frac{-x^4-1}{x^3} \\ 0 & -x & -(-x^2-1) \\ 0 & x^2+1 & -x^3-2x \end{bmatrix}_{3\times 3};$$

$$\bar{\bar{Q}}_5^{-6}(x)=\begin{bmatrix} \frac{1}{x^6} & \frac{-6}{x^7} & \frac{21}{x^8} & \frac{x^2(-x^6-x^2+4)-15}{x^7} & \frac{-21+x^2(x^8+x^6-x^2+5)}{x^8} \\ 0 & \frac{1}{x^6} & \frac{-6}{x^7} & \frac{x^2(x^6+x^4-1)+5}{x^6} & \frac{6+x^2(-x^8-2x^6-1)}{x^7} \\ 0 & 0 & \frac{1}{x^6} & \frac{-x^6(x^2+2)-1}{x^5} & \frac{x^{10}+3x^8-1+x^6}{x^6} \\ 0 & 0 & 0 & x^4+3x^2+1 & -x^5-4x^3-3x \\ 0 & 0 & 0 & -x^5-4x^3-3x & x^6+5x^4+6x^2+1 \end{bmatrix}_{5\times 5}.$$

Покажемо, що матричний вираз $\bar{\bar{Q}}_3^{n}(x)\times\bar{\bar{Q}}_3^{-n}(x)=\bar{\bar{I}}_{3\times 3}$ можна виконати для будь-якого значення n, наприклад n=3, де $\bar{\bar{I}}_{3\times 3}$ – одинична матриця m=3-го порядку.

$$\bar{\bar{Q}}_3^{3}(x)\times\bar{\bar{Q}}_3^{-3}(x)=\bar{\bar{I}}_{3\times 3}\Rightarrow\begin{bmatrix} x^3 & 3x^2+1 & 2x \\ 0 & x^3+2x & x^2+1 \\ 0 & x^2+1 & x \end{bmatrix}\times$$
$$\times\begin{bmatrix} \frac{1}{x^3} & \frac{x^2-1}{x^2} & \frac{-x^4-1}{x^3} \\ 0 & -x & x^2+1 \\ 0 & x^2+1 & -x^3-2x \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \quad (29)$$

Отже, розроблено метод генерування поліноміальних матриць Фібоначчі n-го степеня та їх обернених матриць, елементами яких є поліноми Фібоначчі. Оскільки поліноміальні матриці Фібоначчі можна використовувати для реалізації операції шифрування даних, то аналогічні поліноміальні оберненні матриці також потрібні для процесу розшифрування даних, генерування яких має мати загальний вигляд. Розроблено ПЗ, яке дає змогу генерувати поліноміальні матриці Фібоначчі n-го степеня та m-го поряду, а також їхні обернені поліноміальні матриці аналогічного степеня та поряду.

5. ***Матричний метод шифрування даних поліномами Фібоначчі***. Далі розглянемо особливості реалізації матричного методу шифрування даних *поліномами Фібоначчі* [12, 38, 21]. Щоб використовувати цей метод, початкове повідомлення потрібно подати у вигляді квадратної $\bar{\bar{M}}$-матриці m-го порядку, яку називають *матрицею повідомлення*. Немає обмежень щодо такого подання, тому користувачеві залишається визначати розташування елементів у матриці – рядками чи стовпцями. Наприклад, повідомлення "*Фібоначчі*" можна подати матрицею 3-го порядку, заповнюючи її поелементно рядками:

$$\bar{\bar{M}}=\begin{bmatrix} Ф & і & б \\ о & н & а \\ ч & ч & і \end{bmatrix}\Rightarrow\begin{bmatrix} 212 & 179 & 225 \\ 238 & 237 & 224 \\ 247 & 247 & 179 \end{bmatrix}.$$

Після узгодження цілого числа $x\neq 0$ і цілого числа n між відправником і одержувачем $\bar{\bar{Q}}_m^{n}(x)$-матрицю шифрування даних отримують з виразу, наведеного вище. Потім цю матрицю потрібно помножити справа на матрицю повідомлення $\bar{\bar{M}}$, щоб отримати матрицю зашифрованого повідомлення $\bar{\bar{E}}$. Наприклад, для m = 3 і n = 3 маємо

$$\bar{\bar{E}}=\bar{\bar{Q}}_3^{3}(x)\times\bar{\bar{M}}=\begin{bmatrix} x^3 & 0 & 0 \\ 0 & x^3+2x & x^2+1 \\ 0 & x^2+1 & x \end{bmatrix}\times\begin{bmatrix} 212 & 179 & 225 \\ 238 & 237 & 224 \\ 247 & 247 & 179 \end{bmatrix}=$$
$$=\begin{bmatrix} 212x^3 & 179x^3 & 225x^3 \\ e_{21} & e_{22} & e_{23} \\ e_{31} & e_{32} & e_{33} \end{bmatrix},$$

де:

$$e_{21}=247(x^2+1)+238(x^3+2x);\ e_{22}=247(x^2+1)+237(x^3+2x);$$
$$e_{23}=179(x^2+1)+224(x^3+2x);\ e_{31}=247x+238(x^2+1);$$
$$e_{32}=247x+237(x^2+1);\ e_{33}=179x+224(x^2+1).$$

Елементи матриці зашифрованого повідомлення $\overline{\overline{E}}$ надсилають каналом зв'язку рядками в порядку e_1, e_2,..., e_9, за якими слідує окремо значення визначника матриці $\det(\overline{\overline{Q}}_3^3(x) = -x^3$.

Припускаючи, що передана послідовність чисел отримана без помилок, тоді, шляхом множення оберненої $\overline{\overline{Q}}_3^{-3}(x)$ -матриці на матрицю зашифрованого повідомлення $\overline{\overline{E}}$, отримують початкову матрицю повідомлення:

$$\overline{\overline{M}} = \overline{\overline{Q}}_3^{-3}(x) \times \overline{\overline{E}} = \begin{bmatrix} \frac{1}{x^3} & 0 & 0 \\ 0 & -x & x^2+1 \\ 0 & x^2+1 & -x^3-2x \end{bmatrix} \times \begin{bmatrix} 212x^3 & 179x^3 & 225x^3 \\ e_{21} & e_{22} & e_{23} \\ e_{31} & e_{32} & e_{33} \end{bmatrix} = \begin{pmatrix} 212 & 179 & 225 \\ 238 & 237 & 224 \\ 247 & 247 & 179 \end{pmatrix}.$$

Запропоновано матричний метод шифрування даних на підставі поліномів Фібоначчі над алфавітом {0, 1,..., 255}. Для цілих чисел $m \geq 2$, $x \geq 1$ і $n \geq 1$, використаної $\overline{\overline{Q}}_m^n(x)$ -матриці n-го степеню шифрування даних розміром $m \times m$, елементами якої є поліноми Фібоначчі [5]. Кожне вхідне повідомлення є $\overline{\overline{M}}$ -матрицею розміром $m \times m$, перетворену в матрицю зашифрованого повідомлення $\overline{\overline{E}} = \overline{\overline{M}} \times Q_m^n(x)$.

Отже, показана можливість вирішення проблеми генерування послідовностей поліномів Фібоначчі n-го степеня, які є основою шифрування потокових і блокових даних, що дає можливість здійснювати ефективний їх захист. Наведено відомі способи подання поліномів Фібоначчі n-го степеня, а також запропоновано метод матричного подання поліномів Фібоначчі n-го степеня та їх обернених еквівалентів, які застосовано у конкретному прикладі шифрування даних. Розроблено метод генерування поліноміальних матриць Фібоначчі n-го степеня, елементами яких є відповідні поліноми Фібоначчі, та їх обернених матриць, особливість застосування яких показана на прикладі традиційного методу шифрування даних.

Обговорення результатів дослідження. Числа Фібоначчі є популярною темою для математичного збагачення дослідників і їхньої популяризації серед них [46]. Водночас, різні послідовності поліномів під назвами поліномів Фібоначчі трапляються в науковій літературі хоча і давно, позаяк вони тісно пов'язані між собою, проте вони не так широко досліджені, як відповідні послідовності чисел Фібоначчі. Зазначені поліноми з'являються в різних областях застосування, в тому числі й для шифрування даних, насамперед матричним методом. У математиці поліноми Фібоначчі – це поліноміальна послідовність, яку можна розглядати як узагальнення чисел Фібоначчі [33].

У роботі [11] наведено поліноміальні матриці Фібоначчі–Гессенберга з визначником полінома Фібоначчі. Авторами наведено декілька класів поліноміальних матриць Фібоначчі–Гессенберга. Також введено поняття двовимірного масиву поліномів Фібоначчі та наведено три класи поліноміальних матриць Фібоначчі–Гессенберга, що задовольняють їхню властивість.

У роботі [17] наведено тотожності Фібоначчі та Люка, отримані з матриць Тепліца–Гессенберга. Автори розглянули визначники для деяких сімейств матриць Тепліца–Гессенберга, що мають різні переклади чисел Фібоначчі та Люка для ненульових елементів. Формули цих визначників можна також переписати як тотожності, що містять суми добутків чисел Фібоначчі та Люка, а також їхніх мультиноміальних коефіцієнтів. У дослідженні наведено комбінаторні докази кількох визначників, які використовують знакозмінні інволюції та визначення визначника як суми зі знаком над симетричною групою. Це призвело до узагальнення формул Фібоначчі та Люка в термінах так званих чисел Гібоначчі.

У роботі [52] розглянуто узагальнені Гумберта поліноми, отримані через узагальнені поліноми Фібоначчі. Автори визначили узагальнені (p,q)-Фібоначчі поліноми $u_{n,m}(x)$ і узагальнені (p,q)-Люка поліноми $v_{n,m}(x)$, а також ввели узагальнені Гумберта поліноми $u_{n,m}^{(r)}(x)$ як окремі згортки $u_{n,m}(x)$. Також дослідники навели багато виразів, їхніх розкладів, рекурентних співвідношень, в т.ч. й диференціальних, що дало їм змогу вивчати матриці та визначники, пов'язані з поліномами $u_{n,m}(x)$, $v_{n,m}(x)$ та $u_{n,m}^{(r)}(x)$. Автори запропонували алгебраїчну інтерпретацію для узагальнених Гумберта поліномів $u_{n,m}^{(r)}(x)$, де було вказано, що різні добре відомі поліноми є окремими випадками узагальнених поліномів $u_{n,m}(x)$, $v_{n,m}(x)$ або $u_{n,m}^{(r)}(x)$. Ввівши узагальнені поліноми $u_{n,m}(x)$, $v_{n,m}(x)$ і $u_{n,m}^{(r)}(x)$, автори мали єдиний підхід до роботи з багатьма спеціальними поліномами, відомими в наявній літературі.

У роботі [35] наведено новий метод (роз)шифрування даних з використанням Q-матриць Фібоначчі, заснований на матрицях заблокованих повідомлень. Головною перевагою такого методу є шифрування кожної матриці вхідного повідомлення ключами різної величини [24, 26]. Як стверджують автори, такий підхід не тільки підвищує безпеку зашифрованих повідомлень від криптографічних атак [19, 25], але й має високу коригувальну здатність, однак не вказують, чим саме чи як саме це забезпечується.

У роботі [7] запропоновано нову теорію шифрування даних з використанням m-розширення p-чисел Фібоначчі. Автори навели квадратну $G_{p,m}$-матрицю Фібоначчі, де $p \geq 0$ є цілим невід'ємним числом і $m > 0$. Також описали різні властивості $G_{p,m}$-матриці, яка є основою теорії шифрування даних, встановили зв'язки між елементами цієї матриці для різних значень p і m. Автори показали, що співвідношення між елементами $G_{p,m}$-матриці для різних значень p і $m = 1$ збігаються з відношенням між елементами матриці шифрування для різних значень p [6]. Загалом, достовірність запропонованого методу зростає зі збільшенням цього значення, але вона не залежить від значення m.

У роботі [6] розроблено узагальнені співвідношення між елементами матриці шифрування даних числами Фібоначчі. Автори розглядали клас квадратної матриці Фібоначчі $(p+1)$-порядку, елементи якої базуються на p-числах Фібоначчі з визначником, що становить ± 1. Вони стверджують, що існує зв'язок між числами Фібоначчі з початковими членами, який відомий як формула Кассіні, а саме: $F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$, $n \geq 1$. Було встановлено, що послідовність чисел Фібоначчі та золотий переріз мають важливе значення під час побудови відносно нової теорії простору-часу, яка відома як E-теорія нескінченності. Оригінальний метод (роз)шифрування

даних числами Фібоначчі випливає з аналогічних матриць, де відомим залишається зв'язок між її елементами для випадку $p = 1$ [46]. Також автори встановили узагальнені співвідношення між елементами матриці шифрування даних для різних значень p. Наприклад, для $p = 2$ достовірність запропонованого методу становить 99,80 % і зростає зі збільшенням цього значення.

У роботі [46] розроблено матрицю Фібоначчі, наведено узагальнення формули Кассіні та нову теорію шифрування даних. Автори розглядали новий клас квадратних матриць розміром $(p+1)\times(p+1)$, елементами яких були p-числа Фібоначчі ($p = 0, 1, 2, 3, \ldots$), а їхній визначник становить ±1. Ця унікальна властивість матриць Фібоначчі приводить до узагальнення формули Кассіні. Запропонований оригінальний метод (роз)шифрування даних числами Фібоначчі випливає з аналогічних матриць n-порядку. На відміну від класичних надлишкових кодів основною особливістю запропонованого методу є те, що він дає змогу коригувати зашифровані елементи матриці, які теоретично можуть бути необмеженими цілими числами. Для найпростішого випадку коригувальна здатність цього методу становить 93,33 %, що значно перевищує відомі коригувальні можливості інших методів.

У роботі [14] наведено новий клас кодів з можливістю виправлення помилок на підставі послідовності чисел Фібоначчі. Запропоновано клас квадратних M_p^n-матриць n-го степеня p-го порядку для (роз)шифрування даних і запропоновано методику контролю за появою помилок. Це значно розширює результати попередніх досліджень [46] щодо методів коригування помилок, зумовлених під час передачі зашифрованих повідомлень каналами зв'язку. Автори вважають, що для цілого числа p можна згенерувати двійкову M_p^n-матрицю n-го степеня розміром $(p+1)\times(p+1)$, ненульові елементи якої розташовані або на супердіагоналі, або в останньому рядку матриці. Звичайну M_p^n- та обернену M_p^{-n}-матриці n-го ступеня використовують як матриці шифрування та даних дешифрування відповідно. Також вони показали, що для достатньо великих значень n, незалежно від значень елементів матриці повідомлення M_p, між елементами зашифрованої матриці існують зв'язки $E_p = M_p \times M_p^n$. Ці відносини мають важливе значення під час виявлення та виправлення помилок у зашифрованих повідомленнях.

У роботі [43] розглянуто узагальнені співвідношення між елементами матриці шифрування даних, запропоновано нову комплексну $H_{p,n}$-матрицю Фібоначчі, елементами якої є відповідні числа. Розроблено метод (роз)шифрування, що випливає з цієї комплексної $H_{p,n}$-матриці Фібоначчі, а також встановлено зв'язки між її елементами. Запропоновано підхід до виявлення та виправлення помилок у зашифрованих повідомленнях, що ґрунтується на потребі розв'язування діофантових рівнянь.

У роботі [15] розроблено метод шифрування даних на підставі поліномів Фібоначчі з можливістю виявлення та виправлення помилок у зашифрованих повідомленнях. Для цілих чисел $m \geq 2$, $x \geq 1$ і $n \geq 1$ розроблено Q_m^n-матрицю n-го степеня розміром $m \geq m$, яку названо $Q_m^n(x)$-матрицю шифрування даних, елементами якої є поліноми Фібоначчі. Для дешифрування даних автори вводять обернену $Q_m^{-n}(x)$-матрицю, особливість яких у тому, що їхній визначник становить ±1. Наведено простий критерій виявлення помилок і відповідний метод їх виправлення для цього класу матриць. Також показано, що ймовірність появи помилок у зашифрованих повідомленнях майже дорівнює нулю за досить великих значень m. Наведено наочні приклади (роз)шифрування даних, а також різні випадки виявлення та виправлення помилок у зашифрованих повідомленнях.

У роботі [13] розроблено новий метод шифрування даних на підставі поліномів Фібоначчі з високою швидкістю їх генерування. Для цілих чисел m, n і $x \geq 1$ можна згенерувати квадратну $Q_{2m}^n(x)$-матрицю n-го степеня $2m$-го порядку, елементами якої є поліноми Фібоначчі, і відповідну обернену $Q_{2m}^{-n}(x)$-матрицю для їх дешифрування [23, 24, 26]. Також показано, що швидкість (роз)шифрування даних за допомогою цих матриць значно вища, ніж з оригінальними матрицями на підставі звичайних чисел Фібоначчі.

У роботі [40] запропоновано нову теорію шифрування даних на $(h(x), g(y))$-розширенні поліномів p-числами Фібоначчі. Визначено також золоті $(p, h(x), g(y))$-пропорції, де $p \geq 0$ – цілі числа, $h(x) > 0$, $g(y) > 0$ – поліноми з дійсними коефіцієнтами. Встановлено, що співвідношення між елементами квадратної $G_{p,h,g}$-матриці Фібоначчі повністю збігаються зі співвідношеннями між елементами матриці шифрування для різних значень p і поліномів $h(x) = m$ і $g(y) = t$ [4]. Також співвідношення між елементами матриці шифрування для поліномів $h(x) = 1$ і $g(y) = 1$ збігаються з узагальненими співвідношеннями між елементами матриці шифрування числами Фібоначчі [6]. Завдяки відповідному вибору початкових членів у $(h(x), g(y))$-розширенні поліномів p-числами Фібоначчі квадратну $G_{p,h,g}$-матрицю можна застосувати для (роз)шифрування даних різної величини. Під час обговорення результатів свого дослідження автори стверджують, що достовірність цього методу зростає зі збільшенням значення p, але вона не залежить від значень поліномів $h(x)$ і $g(y)$, які значно удосконалюють криптографічну стійкість зашифрованих повідомлень [18, 22]. Складність цього методу зростає зі збільшенням степеня поліномів $h(x)$ і $g(y)$. Також знайдено зв'язок між золотою $(p, h(x), g(y))$-пропорцією, між золотою $(p, h(x))$-пропорцією та між золотою p-пропорцією.

Проаналізовані вище роботи стосовно наявних підходів до генерування поліномів Фібоначчі, а також особливостей їх використання для шифрування даних вказали на те, що навіть за останнє десятиліття виконано багато різноманітних досліджень, в кожному з яких тією чи іншою мірою обґрунтовано різні підходи до генерування таких поліномів і доведено доцільність їх використання для шифрування даних. Водночас було з'ясовано, що як окрема процедура захисту потокових і блокових даних поліномами Фібоначчі у теорії та практиці криптографії трапляються вкрай рідко. Тому проведене нами дослідження щодо ефективних методів генерування поліномів Фібоначчі, а також встановлення певних особливості їх використання для шифрування потокових і блокових даних тільки як локального методу є актуальною проблемою, яку було частково вирішено в цьому дослідженні.

Отже, за результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – розроблено метод генерування поліноміальних матриць Фібоначчі n-го степеня та їх обернених матриць, елементи яких, на відміну від елементів традиційних матриць Фібоначчі, є відповідні поліноми Фібоначчі n-го степеня, які є основою шифрування блокових даних, що дає можливість здійснювати їх ефективний захист.

Практична значущість результатів дослідження – запропонований метод матричного подання поліномів Фібоначчі n-го степеня та їх обернених еквівалентів можна використовувати для шифрування потокових даних, а розроблений метод генерування поліноміальних матриць Фібоначчі n-го степеня, елементами яких є відповідні поліноми Фібоначчі, та їх обернених матриць, можна застосовувати в традиційному методі шифрування блокових даних, що загалом дасть можливість ефективно передавати каналами зв'язку потокові та блокові повідомлення різної величини.

Висновок / Conclusions

Розроблено методи генерування послідовностей поліномів Фібоначчі n-го степеня як основи шифрування потокових і блокових даних, що дасть змогу ефективно передавати каналами зв'язку відповідні повідомлення різної величини. За результатами виконаного дослідження можна зробити такі основні висновки.

1. Внаслідок проведеного аналізу наявних досліджень та публікацій з'ясовано, що навіть за останнє десятиліття надруковано значну кількість різноманітних публікацій, в кожній з яких тією чи іншою мірою обґрунтовано різні підходи до генерування поліномів Фібоначчі n-го степеня та доведено доцільність їх використання для шифрування даних. Проте, більшість досліджень стосується окремих процедур захисту потокових і блокових даних, що в теорії та практиці криптографії трапляються вкрай рідко. Виявлено основну складність проблеми генерування послідовностей поліномів Фібоначчі n-го степеня, які стануть основою шифрування потокових і блокових даних, що дасть можливість здійснювати ефективний їх захист.

2. Наведено відомі способи подання чисел Фібоначчі та Люка, а також поліномів Фібоначчі, що мають багато корисних властивостей, використано тільки ті із них, які можна застосувати у традиційному методі шифрування даних. Встановлено, що в послідовностях чисел Фібоначчі та Люка, де відношення двох послідовних доданків наближається до золотого перерізу, їхні члени фактично є наближеннями цілих степенів золотого перерізу.

3. Запропоновано метод матричного подання поліномів Фібоначчі та їх обернених еквівалентів, які можна застосувати у традиційному методі шифрування даних, наведено конкретний приклад їх застосування. Для цього необхідно перемножити спеціальну матрицю n-го порядку з відповідними коефіцієнтами на поліном n-го степеня, внаслідок чого отримаємо набір поліномів Фібоначчі $F_n(x)$ відповідного степеня. Зазвичай, спеціальна матриця є нижньою трикутною матрицею, всі елементи головної діагоналі якої є одиничними.

4. Розроблено метод генерування поліноміальних матриць Фібоначчі n-го степеня та їх обернених матриць, елементами яких є поліноми Фібоначчі, які можна застосувати у традиційному методі шифрування даних, наведено конкретний приклад їх застосування. Оскільки поліноміальні матриці Фібоначчі можна використовувати для реалізації операції шифрування даних, то аналогічні поліноміальні оберненні матриці також потрібні для процесу розшифрування даних, генерування яких має мати загальний вигляд. Розроблено ПЗ, яке дає змогу генерувати поліноміальні матриці Фібоначчі n-го степеня та m-го поряду, а також їхні обернені поліноміальні матриці аналогічного степеня та поряду.

5. За результатами виконаного дослідження зробити висновки та надано відповідні рекомендації щодо їх практичного використання як основи для шифрування потокових і блокових даних, що дасть змогу ефективно передавати каналами зв'язку відповідні повідомлення різної величини.

References

1. Asci, M., & Gurel, E. (2017). Some properties of *k*-order Gaussian Fibonacci and Lucas numbers. *Ars Combinatoria*, 135, 345–356. URI: https://hdl.handle.net/11499/23655
2. Asci, M., & Tasci, D. (2007). On Fibonacci, Lucas and special orthogonal polynomials. *Journal of Computational and Applied Mathematics*. https://doi.org/10.1016/J.CAM.2007.01.026
3. Basu, M., & Prasad, B. (2009). The Generalized relations among the code elements for Fibonacci coding theory. *Chaos, Solitons and Fractals*, Vol. 41, issue 5, 2517–2525. https://doi.org/10.1016/j.chaos.2008.09.030
4. Basu, M., & Prasad, B. (2011). Coding theory on the (*m*,*t*)-extension of the Fibonacci *p*-numbers. *Discrete Mathematics, Algorithms and Applications*, Vol. 3, 259–267. https://doi.org/10.1142/S1793830911001097
5. Basu, Manjusri, & Das, Monojit. (2017). Coding theory on generalized Fibonacci *n*-step polynomials. *Journal of Information and Optimization Sciences*, Vol. 38, issue 1, 83–131. https://doi.org/10.1080/02522667.2016.1160618
6. Basu, Manjusri, & Prasad, Bandhu. (2009). The generalized relations among the code elements for Fibonacci coding theory. *Chaos, Solitons, & Fractals*, Vol. 41, issue 5(14), 2517–2525. https://doi.org/10.1016/j.chaos.2008.09.030
7. Basu, Manjusri, & Prasad, Bandhu. (2009, November). Coding theory on the *m*-extension of the Fibonacci *p*-numbers. *Chaos, Solitons, & Fractals*, Vol. 42, issue 4, 30, 2522–2530. https://doi.org/10.1016/j.chaos.2009.03.197
8. Bellini, Emanuele, Marcolla, Chiara, & Murru, Nadir. (2020, March). On the decoding of 1-Fibonacci error correcting codes. *Discrete Mathematics, Algorithms and Applications*, Vol. 13, No. 05, article ID 2150056. https://doi.org/10.13140/RG.2.2.27280.97281; https://doi.org/10.1142/S1793830921500567
9. Chasnov, Jeffrey R. (2008). Fibonacci numbers and the golden ratio. *The Hong Kong University of Science and Technology*, 87 p. URL: https://www.math.hkust.edu.hk/~machas/fibonacci.pdf
10. Cristina Flaut, Diana Savin. (2017, April). Some remarks regarding generalized Fibonacci-Lucas numbers and generalized Fibonacci-Lucas quaternions. arXiv:1705.00361v2 [math.RA]. https://doi.org/10.48550/arXiv.1705.00361
11. Esmaeili, M., & Esmaeili, M. (2009). Polynomial Fibonacci-Hessenberg matrices. *Chaos, Solitons and Fractals*, Vol. 41, issue 5, 2820–2827. https://doi.org/10.1016/j.chaos.2008.10.012
12. Esmaeili, M., & Esmaeili, M. (2010). A Fibonacci-polynomial based coding method with error detection and correction. *Computers and Mathematics with Applications*, 60, 2738–2752. https://doi.org/10.1016/j.camwa.2010.08.091
13. Esmaeili, M., Esmaeili, M., & Gulliver, T. A. (2011). High-rate Fibonacci polynomial codes. In: *Proceedings of IEEE International Symposium on Information Theory Proceedings, St. Petersburg, Russia*, pp. 1921–1924. https://doi.org/10.1109/ISIT.2011.6033886

14. Esmaili, M., Moosavi, M., & Gulliver, T. A. (2017, January). A new class of Fibonacci sequence based error correcting codes. *Cryptography and Communications*, Vol. 9, 379–396. https://doi.org/10.1007/s12095-015-0178-x
15. Esmaili, Mostafa, & Esmaeili, Morteza (2010). A Fibonacci-polynomial based coding method with error detection and correction. *Computers and Mathematics with Applications*, 60, 2738–2752. https://doi.org/10.1016/j.camwa.2010.08.091
16. Falcon, S., & Plaza, A. (2009). On *k*-Fibonacci sequences and polynomials and their derivatives. *Chaos, Solitons and Fractals*, Vol. 39, issue 3, 1005–1019. https://doi.org/10.1016/j.chaos.2007.03.007
17. Goy, Taras, & Shattuck, Mark (2019, December). Fibonacci and Lucas Identities from Toeplitz–Hessenberg Matrices. *Applications and Applied Mathematics: An International Journal*, 14(2), 699–715. URL: https://www.researchgate.net/publication/337906242_Fibonacci_and_Lucas_Identities_from_Toeplitz-Hessenberg_Matrices
18. Gryciuk, Yurij, Grytsyuk, Pavlo (2015). Perfecting of the matrix Affine cryptosystem information security. Computer Science and Information Technologies: Proceedings of Xth International Scientific and Technical Conference (CSIT2015), 14–17 September, 2015, pp. 67–69. https://doi.org/10.1109/stc-csit.2015.7325433
19. Grytsiuk, P. Yu., & Hrytsiuk, Yu. I. (2015). Peculiarities of the implementation of the matrix Athena cryptosystem of information protection. *Scientific Bulletin of UNFU*, 25(5), 346–356. URL: https://nv.nltu.edu.ua/index.php/journal/article/view/1092
20. Hoggat, V. E. (1969). Fibonacci and Lucas numbers. *Palo Alto* (CA): Houghton-Mifflin. URL: https://www.peliti.org/Notes/fibonacciLucas.pdf
21. Hoggat, V. E., Bicknell, Marjorie. (1973). Roots of fibonacci polynomials. The Fibonacci Quarterly, Vol/ 11, issue 3, 271–274. https://doi.org/10.1080/00150517.1973.12430825
22. Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2015). Implementation of cryptographic transformations using Fibonacci $G(\lambda)$-matrices. *Mathematical and software support of intelligent systems: materials of the 13th International Scientific and Practical Conference*, (pp. 53–54), November 18–20, 2015, Dnipropetrovsk, Ukraine. Dnipropetrovsk: Department of Dnipropetrovsk National University named after Olesya Honchara.
23. Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2015). Methods and means of generating Fibonacci Q_p-matrices – keys for implementing cryptographic transformations. *Scientific Bulletin of UNFU*, 25(6), 334–351. URL: https://nv.nltu.edu.ua/index.php/journal/article/view/974
24. Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2016). Features of generating Fibonacci Q_p-matrices – keys for implementing cryptographic transformations. *Bulletin of the National University "Lviv Polytechnic". Series: Computer Science and Information Technology*, Vol. 843, 251–263. URL: https://vlp.com.ua/node/16094
25. Hrytsiuk, Yu. I., & Grytsiuk, P. Yu. (2016). Features of generating Fibonacci $G_p(\lambda)$-matrices for implementation of cryptographic transformations. *Information extraction and processing: interdepartmental collection of scientific papers*, 43(119), 86–95.
26. Hrytsiuk, Yuriy, & Grytsyuk, Pavlo (2016). Generation of Fibonacci $Q_p(\lambda)$-matrices – keys for data encryption. Information protection and security of information systems: materials of the 5th International Scientific and Technical Conference, (pp. 39–40), June 02–03, 2016, Lviv, Ukraine. Lviv: Lviv Polytechnic State University.
27. Hrytsiuk, Yuriy, Grytsyuk, Pavlo, Dyak, Tetiana, & Hrynyk, Heorhiy. (2019). Software Development Risk Modeling. IEEE 2019 14th *International Scientific and Technical Conference on Computer Sciences and Information Technologies* (CSIT 2019), (Vol. 2, pp. 134–137), 17–20 September, Lviv, Ukraine. Lviv: Lviv Polytechnic National University, 206 p. https://doi.org/10.1109/stc-csit.2019.8929778
28. Jin, Z. (2018). On the Lucas polynomials and some of their new identities. *Adv Differ Equ*, 126 (2018). https://doi.org/10.1186/s13662-018-1527-9
29. Kargın, Alparslan, Kişi, Emre, & Özdemir, Halim. (2019, September). Some Notes on Odd or Even Indexed Fibonacci and Lucas Sequences. *Sakarya University Journal of Science*, 23(5), 929–933. https://doi.org/10.16984/saufenbilder.536642
30. Knuth, Donald. (1968). The art of computer programming 1: Fundamental algorithms 2: Semi Numerical algorithms 3: *Sorting and searching*, MA: Addison-Wesley 30.
31. Koshy, Thomas. (2001). Fibonacci and Lucas Numbers with Applications. A Wiley-Interscience Publication, 654 p. https://doi.org/10.1002/9781118033067
32. Kuhapatanakul, K. (2015). The Lucas *p*-matrix. *International Journal of Mathematical Education in Science and Technology*. https://doi.org/10.1080/0020739X.2015.1026612
33. Mostafa Esmaili & Morteza Esmaeili. (2010). A Fibonacci-polynomial based coding method with error detection and correction. *Computers and Mathematics with Applications*, Vol. 60, issue 10, 2738–2752. https://doi.org/10.1016/j.camwa.2010.08.091
34. Neeraj Kumar Paul, & Helen K. Saikia. (2023). A generalization of Lucas sequence and associated identities. *Boletim da Sociedade Paranaense de Matematica*, Vol. 41, 1–20. https://doi.org/10.5269/bspm.53068
35. Nihal Tas, Sumeyra Ucar, Nihal Yilmaz Ozgur, & Oztunc Kaymak. (2018). A new coding/decoding algorithm using Fibonacci numbers. *Discrete Mathematics, Algorithms and Applications*, Vol. 10, No. 02, article ID 1850028. https://doi.org/10.1142/S1793830918500283; https://doi.org/10.48550/arXiv.1712.02262
36. Octavian Postavaru. (October 2023). An efficient numerical method based on Fibonacci polynomials to solve fractional differential equations. *Mathematics and Computers in Simulation*, Vol. 212, 406–422. https://doi.org/10.1016/j.matcom.2023.04.028
37. Omprakash Sikhwal, & Yashwant Vyas. (2014). Fibonacci Polynomials and Determinant Identities. *Turkish Journal of Analysis and Number Theory*, 2(5), 189–192. https://doi.org/10.12691/tjant-2-5-6
38. Özkan, Engin, Taştan, Merve & Aydoğdu, Ali. (2019). Fibonacci Sayılarının Ailesinde 3-Fibonacci Polinomları. Erzincan Üniversitesi Fen Bilimleri Enstitüsü Dergisi. Cilt: 12 Sayı: 2, 926–933. https://doi.org/10.18185/erzifbed.512100
39. Perumali, Sundarayya, & Prasad, M. G. Vara. (2019, October). Coding theory on Pell-Lucas *p*-numbers. *Journal of Physics Conference Series*, 1344(1), article ID 012017. https://doi.org/10.1088/1742-6596/1344/1/012017
40. Prasad, Bandhu. (2014). Coding theory on $(h(x), g(y))$-extension of Fibonacci *p*-numbers polynomials. *Universal Journal of Computational Mathematics*, Vol. 2(1), 6–10. https://doi.org/10.13189/ujcmj.2014.020102
41. Prasad, Bandhu. (2014). High rates of Fibonacci polynomials coding theory. *Discrete Mathematics, Algorithms and Applications*, Vol. 06, No. 04, article ID 1450053. https://doi.org/10.1142/S1793830914500530
42. Prasad, Bandhu. (2016). Coding theory on Lucas *p*-numbers. *Discrete Mathematics, Algorithms and Applications*, Vol. 08, No. 04, article ID 1650074. https://doi.org/10.1142/S1793830916500749
43. Prasad, Bandhu. (2019). The generalized relations among the code elements for a new complex Fibonacci matrix. *Discrete Mathematics, Algorithms and Applications*, Vol. 11, No. 02, article ID 1950026. https://doi.org/10.1142/S1793830919500265
44. Sentürk, G. Y., Gürses, N., & Yüce, S. (2022). Construction of dual-generalized complex Fibonacci and Lucas quaternions. *Carpathian Mathematical Publications*, 14(2), 406–418. https://doi.org/10.15330/cmp.14.2.406-418
45. Singh, B., Sikhwal, O., & Panwar, Y. K.. (2009). Generalized Determinantal Identities Involving Lucas Polynomials. *Applied Mathematical Sciences*, 3(8), 377–388. URL: https://www.researchgate.net/publication/228526069_Generalized_Determinantal_Identities_Involving_Lucas_Polynomials
46. Stakhov, A. P. (2006, October). Fibonacci matrices, a generalization of the "Cassini formula", and a new coding theory. *Chaos,*

Solitons, & Fractals, Vol. 30, issue 1, 56–66. https://doi.org/10.1016/j.chaos.2005.12.054
47. Stakhov, A., & Rozin, B. (2005). Theory of Binet formulas for Fibonacci and Lucas *p*-numbers. *Chaos, Solitons and Fractals*, 27, No. 5, 1162–1177. https://doi.org/10.1016/j.chaos.2005.04.106
48. Stakhov, Alexey, & Olsen, Scott. (2009). The Mathematics of Harmony: From Euclid to Contemporary Mathematics and Computer Science. *Series on Knots and Everything*, 22. World Scientific Publishing Company; First Edition, 748 p. https://doi.org/10.1142/6635
49. Uçar, Sümeyra, Tas, Nihal, & Özgür, Nihal. (2019, May). A New Application to Coding Theory via Fibonacci and Lucas Numbers. *Mathematical Sciences and Applications E-Notes*, 7(1), 62–70. https://doi.org/10.36753/mathenot.559251
50. Urszula Bednar, & Małgorzata Wołowiec-Musiał. (2020). Distance Fibonacci Polynomials. Symmetry, 12(9), 1540 p. https://doi.org/10.3390/sym12091540
51. Vajda, S. (1989). Fibonacci and Lucas Numbers and the Golden Section Theory and Applications. Ellis Harwood Limitted, 190 p. https://doi.org/10.2307/3619858
52. Wang, Weiping, & Wang, Hui. (2017, August). Generalized Humbert polynomials via generalized Fibonacci polynomials. *Applied Mathematics and Computation*, Vol. 307, 204–216. https://doi.org/10.1016/j.amc.2017.02.050
53. Yang, Jizhen, & Zhang, Zhizheng. (2018, December). Some identities of the generalized Fibonacci and Lucas sequences. *Applied Mathematics and Computation*, Vol. 339, 451–458. https://doi.org/10.1016/j.amc.2018.07.054

P. Yu. Grytsiuk, Yu. I. Hrytsiuk

Lviv Polytechnic National University, Lviv, Ukraine

METHODS FOR GENERATING FIBONACCI POLYNOMIALS AND FEATURES OF THEIR USE FOR DATA ENCRYPTION

Methods for generating sequences of Fibonacci polynomials of the *n*th degree as the basis for encrypting stream and block data have been developed, which makes it possible to effectively transmit corresponding messages of various sizes over communication channels. It has been found that a significant number of publications have been published over the past decade, each of which substantiates different approaches to generating Fibonacci polynomials and proves the feasibility of their use for data encryption. However, most of the research concerns individual data protection procedures that are extremely rare in the theory and practice of cryptography. The main complexity of the problem of generating sequences of Fibonacci polynomials of the *n*th degree, which are the basis for encrypting stream and block data, has been established, which will make it possible to effectively protect them. Known ways of representing Fibonacci and Luke numbers, as well as Fibonacci polynomials, which can be used in the traditional method of data encryption, are given. It is established that in the sequences of Fibonacci and Luke numbers, where the ratio of two consecutive terms approaches the golden ratio, their terms are approximations of integer powers of the golden ratio. A method is proposed for matrix representation of Fibonacci polynomials and their inverse counterparts for use in traditional data encryption. To do this, it is necessary to multiply a special matrix of the *n*th order with the corresponding coefficients by a polynomial of the nth degree, as a result of which we obtain a set of Fibonacci polynomials $F_n(x)$ of the corresponding degree. Typically, a special matrix is a lower triangular matrix, all elements of the main diagonal of which are units. A method of generating Fibonacci polynomial matrices of the *n*th degree and their inverse matrices, the elements of which are Fibonacci polynomials, which can be used in the traditional method of data encryption, is developed. Since polynomial inverse matrices are used to decrypt data, their generation must have a general form. Software has been developed that allows generating Fibonacci polynomial matrices of the *n*th degree and *m*th order, as well as their inverse polynomial matrices of the similar degree and order. Based on the results of the research, conclusions were drawn and appropriate recommendations were given regarding their practical use as a basis for encrypting stream and block data, which will allow for the effective transmission of corresponding messages of various sizes via communication channels.

Keywords: Fibonacci numbers; recurrent sequence of polynomials; golden ratio; encryption of stream and block data; Fibonacci polynomial matrix; inverse polynomial matrix.