

На рис. 3 а вказано графік функції $q(v)$, л/год., побудований при цих значеннях параметрів моделі. Оптимальне значення середньої швидкості, що розраховувалось за формулою (14), $v_{opt} = 66.21$ км/год. (рис. 3 б), при цьому витрати палива будуть становити 33.38 л/(100 км), що на маршруті в 111 км дає економію 8.9 л. Зауважимо, що реально водій рухався із середньою швидкістю 41.84 км/год., отже, запропонована швидкість руху дасть економію не лише палива, але й часу доставки вантажу. Розрахована швидкість близька до рекомендованих нормативами. Таким чином, запропонована модель і методика дає цілком адекватні результати, які можуть бути використані перевізниками.

Література

1. **Топливная** экономичность автомобилей с бензиновыми двигателями/ Т.У. Асмус, К. Боргнакке, С.К. Кларк и др.; Под ред. Д. Хиллиарда, Дж.С. Спрингера. – М.: Машиностроение, 1988. – 504 с.
2. **Гащук П.Н.** Оптимизация топливно-скоростных свойств автомобиля. – Львов: Вища шк. Изд-во при Львов. ун-те, 1987. – 168 с.
3. **Гащук П.Н.** Энергетическая эффективность автомобиля. – Львов: Свит, 1992. – 208 с.
4. **Гащук П.М.** Энергопреобразующие системы автомобиля. – Харьков: РИО ХГАДТИ, 1998. – 277 с.
5. **Библюк, Р.В. Зінько, Дадак Р.М., Маковейчук О.М.** Залежність динамічних властивостей дволанкового автопотяга від пружної характеристики зчпного пристрою// Наук. вісник НЛТУ України: Зб. наук.-техн. праць. – Львів: НЛТУУ. – 2005, вип. 15.4. – С. 90-95.
6. **Библюк, Р.В. Зінько, Дадак Р.М., Маковейчук О.М.** Дослідження динамічних властивостей дволанкового автопотяга при подоланні одиначної перешкоди типу "сходінка"// Наук. вісник НЛТУ України: Зб. наук.-техн. праць. – Львів: НЛТУУ. – 2006, вип. 16.1. – С. 113-119.
7. **Худсон Д.** Статистика для физиков: Лекции по теории вероятностей и элементарной статистике. – М.: Мир, 1967. – 242 с.
8. [Електрон. ресурс]. – Доступний з: <http://www.matlab.com>
9. **Клюфас С.І., Маковейчук О.М.** Новий алгоритм визначення опорних точок прив'язки зображень// Гідротехнологія, навігація, управління рухом та конструювання авіатехніки: Матер. 4-ї міжнар. наук.-техн. конф. – 2003, т. 2. – С. 12-16.

УДК 004.451(86)

*Ст. наук. співроб. Я.Г. Братівник, канд. техн. наук –
Львівський ДІНТіУ ім. Вячеслава Чорновола;
доц. Ю.І. Грицюк, канд. техн. наук – НЛТУ України, м. Львів*

ВИКОРИСТАННЯ ЧИСЕЛ ФІБОНАЧЧІ ДЛЯ КОДУВАННЯ ЧИСЛОВОЇ ІНФОРМАЦІЇ

Розглянуто методику матричного шифрування/дешифрування числової інформації з використанням послідовності чисел Фібоначчі (числа "Фі"), у якій використано класичний математичний апарат – теорію матриць. Запропоновано методику виявлення і виправлення помилок у зашифрованій матриці, які виникають у каналах зв'язку. У цій методиці відповідними об'єктами коректування є натуральні десяткові числа різної величини, що має принципове значення для розвитку теорії кодування інформації.

Senior research worker Ya.G. Brativnyk – L'viv state institute of the newest technologies and management after Vyacheslava Chornovola; assoc. prof. Yu.I. Grytcyuk – NUFWT of Ukraine, L'viv

The use of numbers Fibonacci for the code of numerical information

The method of the matrix enciphering/decoding of numerical information is considered with the use of sequence of numbers Fibonacci (numbers of "Fi"), a classic mathematical vehicle – theory of matrices is utilized in which. In the offered method of exposure and correction of errors in an in cipher matrix the proper objects of adjustment are natural decimal numbers, that has an of principle value for development of theory of code of information.

Актуальність питання

Кодування інформації – одна з найпоширеніших проблем в сучасній інформатиці. Під кодуванням розуміють операцію ототожнення символів або їх груп одного коду з відповідними символами чи їх групами іншого коду. Необхідність кодування інформації виникає тоді, коли потрібно узгодити форму повідомлення з деяким каналом зв'язку або яким-небудь пристроєм, призначеним для її перетворення або зберігання. Теорія кодування має тривалу історію свого розвитку та становлення [2, 4]. Розвиток сучасної теорії кодування повсякчас стимулюється прогресом систем зв'язку. *Теорія інформації Шеннона*, яка базується на понятті ентропії, є математичною основою *ефективних кодів*. На сьогодні широко використовуються для *стиснення інформації* коди Шеннона і Хаффмена. Потреба захистити інформацію і канали зв'язку від так званих шумів сприяли розвитку *теорії надмірних кодів*, зокрема кодів Хеммінга чи циклічних кодів.

Таким чином, сучасна теорія кодування інформації – це сукупність, принаймні, чотирьох різних напрямів [4]: *теорія систем числення; теорія криптографії; теорія ефективних кодів; теорія надлишкових кодів*. Теорію кодування часто називають теорією шифрування інформації.

Для вирішення завдань процесу кодування широко використовують різні математичні апарати. Наприклад, в сучасній криптографії основним математичним апаратом є теорія чисел [1], у тому числі чисел Фібоначчі зокрема. Проте останніми роками для кодування числової інформації почали широко використовувати теорію матриць [3], елементами яких є бінарні числа. Отже, основна мета цієї роботи полягає у розробленні матричного методу кодування та відновлення числової інформації з використанням чисел Фібоначчі.

Використання теорії матриць в криптографії

Під матрицею A розуміють прямокутну таблицю чисел розміром $m \times n$. Квадратна матриця, розміром $n \times n$, називається матрицею n -го порядку. Кожній квадратній матриці відповідає число, яке називається *визначником матриці*, наприклад:

$$\text{Det} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Основна властивість визначників задається такою теоремою.

Теорема 1. Для будь-яких двох квадратних матриць A і B маємо:

$$\text{Det}(AB) = (\text{Det } A) \times (\text{Det } B).$$

З цієї теореми витікає, що $\text{Det}(A^n) = (\text{Det } A)^n$.

Загальна ідея матричної криптографії ґрунтується на застосуванні узагальнених Q_p^n -матриць для шифрування і дешифрування числової інформації, поданої у вигляді квадратної матриці M – так званого початкового повідомлення. Шифрувальним ключем тут використовується пара чисел p і n . Оскільки $p = 0, 1, 2, 3, \dots$ і $n = 1, 2, 3, \dots$, то розглянутий нижче метод теоретично має необмежену кількість шифрувальних ключів. Загалом метод матричного шифрування числової інформації має такий вигляд:

$$T = M \times Q_p^n, \quad (1)$$

а дешифрування – такий

$$M = T \times Q_p^{-n}. \quad (2)$$

Для усвідомлення механізму реалізації матричної криптографії виразом (1) розглянемо конкретний приклад. Нехай початкова матриця заповнена будь-якими натуральними числами:

$$M = \begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ m_5 & m_6 & m_7 & m_8 \\ m_9 & m_{10} & m_{11} & m_{12} \\ m_{13} & m_{14} & m_{15} & m_{16} \end{pmatrix}, \quad (3)$$

а кодувальна Q_1 -матриця має булеві значення елементів, тобто:

$$Q_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \quad (4)$$

Механізм отримання зашифрованої (таємної) матриці полягає у виконанні такої матричної дії:

$$T = M \times Q_1 = \begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ m_5 & m_6 & m_7 & m_8 \\ m_9 & m_{10} & m_{11} & m_{12} \\ m_{13} & m_{14} & m_{15} & m_{16} \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \quad (5)$$

Після виконання матричного множення $M \times Q_1$ зашифрована матриця T набуде такого вигляду:

$$T = \begin{pmatrix} m_1 + m_4 & m_1 & m_2 & m_3 \\ m_5 + m_8 & m_5 & m_6 & m_7 \\ m_9 + m_{12} & m_9 & m_{10} & m_{11} \\ m_{13} + m_{16} & m_{13} & m_{14} & m_{15} \end{pmatrix} = \begin{pmatrix} t_1 & t_2 & t_3 & t_4 \\ t_5 & t_6 & t_7 & t_8 \\ t_9 & t_{10} & t_{11} & t_{12} \\ t_{13} & t_{14} & t_{15} & t_{16} \end{pmatrix}. \quad (6)$$

Розглянемо тепер механізм дешифрування таємного повідомлення (6), який полягає у множенні зашифрованої матриці T на обернену до Q_1 -матри-

цю, тобто на так звану розкодувальну Q_1^{-1} -матрицю. Отже, механізм отримання початкової матриці (3) можна подати таким добутком матриць:

$$T \times Q_1^{-1} = \begin{pmatrix} m_1 + m_4 & m_1 & m_2 & m_3 \\ m_5 + m_8 & m_5 & m_6 & m_7 \\ m_9 + m_{12} & m_9 & m_{10} & m_{11} \\ m_{13} + m_{16} & m_{13} & m_{14} & m_{15} \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} m_1 & m_2 & m_3 & m_1 + m_4 - m_1 \\ m_5 & m_6 & m_7 & m_5 + m_8 - m_5 \\ m_9 & m_{10} & m_{11} & m_9 + m_{12} - m_9 \\ m_{13} & m_{14} & m_{15} & m_{13} + m_{16} - m_{13} \end{pmatrix} = \begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ m_5 & m_6 & m_7 & m_8 \\ m_9 & m_{10} & m_{11} & m_{12} \\ m_{13} & m_{14} & m_{15} & m_{16} \end{pmatrix} = M'.$$

Використаємо тепер матричний вираз (1) для обчислення відповідних визначників матриць в лівій і правій його частинах. Тоді, згідно з теоремою 1, отримаємо:

$$\text{Det } T = \text{Det } M \times \text{Det } Q_p^n. \quad (7)$$

Але, згідно з [2], визначникові притаманна така властивість:

$$\text{Det } Q_p^n = (-1)^{pn}. \quad (8)$$

Якщо підставити вираз (8) в (7), то механізм матричного шифрування числової інформації набуде такої властивості криптографії:

$$\text{Det } T = \text{Det } M \times (-1)^{pn}. \quad (9)$$

Тотожність (9) має теоретичне і практичне значення. Стосовно теоретичного значення, то вона відіграє роль головної контрольної властивості криптографії. Це означає, що ми можемо не тільки шифрувати початкове повідомлення M і робити його недоступним для несанкціонованого доступу (наприклад, "хакерів"), але й захищати таємне повідомлення T від випадкових збоїв ("шумів") у каналах зв'язку. Отож, використовуючи метод матричного шифрування/дешифрування, ми можемо проектувати надійні крипто-системи, які дадуть змогу захистити інформацію від "хакерів" і "шумів" одночасно. Практичне значення матричного методу полягає у можливості застосування наявних технічних і програмних засобів, які на сьогодні широко використовуються в інформаційній практиці. Теоретичну та програмну реалізацію такого криптографічного методу подано нижче.

Особливості матричного кодування інформації числами "Фі"

Розглянемо механізм реалізації матричної криптографії, яка також ґрунтується на застосуванні узагальнених Q_p^n -матриць, проте їх елементами є спеціально підібрані числа Фібоначі (далі – числа "Фі"). Як і раніше, початкове повідомлення M подамо у вигляді матриці 3-го порядку:

$$M = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix}, \quad (10)$$

позаяк початкове повідомлення¹ є послідовністю таких десяткових цифр:

$$1008\ 4864\ 537\ 3647\ 3566\ 4636\ 725\ 611\ 283. \quad (11)$$

Тепер це повідомлення подамо у вигляді такої матриці:

$$M = \begin{pmatrix} 1008 & 4864 & 537 \\ 3647 & 3566 & 4636 \\ 725 & 611 & 283 \end{pmatrix}. \quad (12)$$

Припустимо, що для матричного шифрування числами "Фі" використано такі значення елементів Q_p -матриці:

$$Q_{34} = \begin{pmatrix} 55 & 8 & 34 \\ 8 & 2 & 5 \\ 34 & 5 & 21 \end{pmatrix}, \quad (13)$$

а для матричного дешифрування Q_{34} -матриця, обернена до (13), матиме такий вигляд:

$$Q_{34}^{-1} = \begin{pmatrix} -17 & -2 & 28 \\ -2 & 1 & 3 \\ 28 & 3 & -46 \end{pmatrix}.$$

Тоді механізм матричного шифрування повідомлення (11) полягає у множенні початкової матриці (10) на кодувальну матрицю (13), внаслідок чого отримаємо таке зашифроване повідомлення:

$$\begin{aligned} M \times Q_{34} &= \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix} \times \begin{pmatrix} 55 & 8 & 34 \\ 8 & 2 & 5 \\ 34 & 5 & 21 \end{pmatrix} = \\ &= \begin{pmatrix} 55m_1 + 8m_2 + 34m_3 & 8m_1 + 2m_2 + 5m_3 & 34m_1 + 5m_2 + 21m_3 \\ 55m_4 + 8m_5 + 34m_6 & 8m_4 + 2m_5 + 5m_6 & 34m_4 + 5m_5 + 21m_6 \\ 55m_7 + 8m_8 + 34m_9 & 8m_7 + 2m_8 + 5m_9 & 34m_7 + 5m_8 + 21m_9 \end{pmatrix} = \begin{pmatrix} t_1 & t_2 & t_3 \\ t_4 & t_5 & t_6 \\ t_7 & t_8 & t_9 \end{pmatrix} = T. \end{aligned} \quad (14)$$

Застосуємо алгоритм обчислення матричного виразу (14) для шифрування початкової матриці (12):

$$M \times Q_{34} = \begin{pmatrix} 1008 & 4864 & 537 \\ 3647 & 3566 & 4636 \\ 725 & 611 & 283 \end{pmatrix} \times \begin{pmatrix} 55 & 8 & 34 \\ 8 & 2 & 5 \\ 34 & 5 & 21 \end{pmatrix} = \begin{pmatrix} 112610 & 20477 & 69869 \\ 386737 & 59488 & 239184 \\ 54385 & 8437 & 33648 \end{pmatrix} = T. \quad (15)$$

Зрозуміло, що після цього таке зашифроване повідомлення T можна передавати звичайними комунікаційними каналами зв'язку, наприклад, засобами Internet, не боячись за те, що хтось його зможе відразу ж розшифрувати.

Механізм дешифрування таємного повідомлення (14) виконується у зворотному порядку. Зокрема, розшифроване повідомлення M' представимо у такій матричній формі:

¹ код повідомлення радиста на планшет: 1008 – екстрене повідомлення; 4864 – тип літального апарату; 537 – приналежність країні; 3647 3566 4636 – відповідно широта, довгота і азимут; 725 611 283 – відповідно висота, швидкість, команда до виконання.

$$T \times Q_{34}^{-1} = \begin{pmatrix} t_1 & t_2 & t_3 \\ t_4 & t_5 & t_6 \\ t_7 & t_8 & t_9 \end{pmatrix} \times \begin{pmatrix} -17 & -2 & 28 \\ -2 & 1 & 3 \\ 28 & 3 & -46 \end{pmatrix} =$$

$$= \begin{pmatrix} -17t_1 - 2t_2 + 28t_3 & -2t_1 + 1t_2 + 3t_3 & 28t_1 + 3t_2 - 46t_3 \\ -17t_4 - 2t_5 + 28t_6 & -2t_4 + 1t_5 + 3t_6 & 28t_4 + 3t_5 - 46t_6 \\ -17t_7 - 2t_8 + 28t_9 & -2t_7 + 1t_8 + 3t_9 & 28t_7 + 3t_8 - 46t_9 \end{pmatrix} = \begin{pmatrix} m'_1 & m'_2 & m'_3 \\ m'_4 & m'_5 & m'_6 \\ m'_7 & m'_8 & m'_9 \end{pmatrix} = M'. \quad (16)$$

Застосуємо алгоритм обчислення матричного виразу (16) для дешифрування таємного повідомлення (15), внаслідок чого отримаємо:

$$T \times Q_{34}^{-1} = \begin{pmatrix} 112610 & 20477 & 69869 \\ 386737 & 59488 & 239184 \\ 54385 & 8437 & 33648 \end{pmatrix} \times \begin{pmatrix} -17 & -2 & 28 \\ -2 & 1 & 3 \\ 28 & 3 & -46 \end{pmatrix} =$$

$$= \begin{pmatrix} 1008 & 4864 & 537 \\ 3647 & 3566 & 4636 \\ 725 & 611 & 283 \end{pmatrix} = M'. \quad (17)$$

Як бачимо, отримані значення елементів матриці M' повністю збігаються з елементами початкової матриці M , представлені в (12).

Зрозуміло, що для матричного шифрування та дешифрування можна використати зовсім інші значення елементів Q_p -матриці, наприклад:

$$Q_{144} = \begin{pmatrix} 233 & 21 & 144 \\ 21 & 2 & 13 \\ 144 & 13 & 89 \end{pmatrix}, \quad Q_{144}^{-1} = \begin{pmatrix} 98 & 3 & -159 \\ 3 & 1 & -5 \\ 159 & -5 & 258 \end{pmatrix}.$$

У цьому випадку результат шифрування матриці (12) буде зовсім відрізнятися від матриці (15), проте отриманий на виході результат її дешифрування буде аналогічним до матриці (17).

Таким чином, нами показана можливість шифрування та однозначного дешифрування числової інформації з використанням матричних дій, використовуючи Q_p -матрицю, значеннями елементів якої є числа Фібоначі. Проте допитливий читач може поставити резонне запитання: у чому ж особливість матричного шифрування з використанням чисел "Фі"? Відповідь на це запитання подана у наступному підрозділі.

Виявлення помилок у зашифрованому повідомленні

Одне із завдань теорії кодування інформації є виявлення та виправлення помилок, які можуть виникати у зашифрованому повідомленні під впливом випадкових перешкод у комунікаційних каналах зв'язку.

Покажемо методику виявлення помилок у зашифрованому повідомленні, використовуючи матричне кодування числової інформації. Головна його ідея полягає у використанні властивості визначника початкової матриці M як контрольного критерію для переданого зашифрованого повідомлення T . Згідно з теорією матриць, визначник кодувальної Q^n -матриці можна задати таким виразом:

$$\text{Det } Q^n = (-1)^n. \quad (18)$$

Продemonструємо ідею виправлення помилок на прикладі початкового повідомлення M , заданого матрицею (10). Як зазначалося вище, визначник цієї матриці можна обчислити за такою формулою:

$$\text{Det } M = (m_1 m_5 m_9 + m_4 m_8 m_3 + m_2 m_6 m_7) - (m_7 m_5 m_3 + m_4 m_2 m_9 + m_8 m_6 m_1). \quad (19)$$

Застосуємо тепер теорему 1 для зашифрованого повідомлення $T = M \times Q^n$, представивши його у матричній формі:

$$\text{Det } T = \text{Det } [M \times Q^n] = \text{Det } M \times \text{Det } Q^n. \quad (20)$$

Тепер, використовуючи вираз (18), можна записати вираз (20) у такому вигляді:

$$\text{Det } T = \text{Det } M \times (-1)^n. \quad (21)$$

Формула (21) показує, що визначник початкової матриці ($\text{Det } M$) і визначник зашифрованої матриці ($\text{Det } T$) пов'язані між собою простим співвідношенням, тобто визначник переданого повідомлення T дорівнює визначнику початкового повідомлення M за абсолютною величиною. Знак визначника зашифрованого повідомлення T залежить від числа n , тобто:

$$\text{Det } T = \begin{cases} -\text{Det } M, & \text{якщо } n - \text{парне;} \\ \text{Det } M, & \text{якщо } n - \text{непарне.} \end{cases} \quad (22)$$

Математичні тотожності (20), (21), (22) є основою методу виявлення помилок, які трапляються у каналах зв'язку під час передачі зашифрованого повідомлення. Ідея методу полягає в такому. Відправник обчислює визначник початкового повідомлення M , представленого матрицею (10), і посилає його каналом зв'язку разом з зашифрованим повідомленням T . Адресат обчислює визначник отриманої матриці T і порівнює його з визначником початкової матриці M . Якщо таке порівняння відповідає умові (22), то зашифроване повідомлення T є коректним і адресат може дешифрувати його.

Апробуємо запропоновану методику виявлення помилок на розглянутому вище прикладі. Формула для обчислення значення визначника початкового повідомлення M показана в (19). Тоді, згідно з виразом (22), визначник зашифрованої матриці T повинен дорівнювати

$$\text{Det } T = -\text{Det } M = -(m_1 m_5 m_9 + m_4 m_8 m_3 + m_2 m_6 m_7) + (m_7 m_5 m_3 + m_4 m_2 m_9 + m_8 m_6 m_1).$$

Спробуємо довести це твердження спочатку теоретично. Дійсно, після обчислення визначника матриці від $M \times Q_{34}$, а також виконання нескладних математичних перетворень, отримаємо:

$$\text{Det } T = \text{Det } (M \times Q_{34}) = -\text{Det } M. \quad (23)$$

$$\text{Det } (M \times Q_{34}) = \text{Det} \begin{pmatrix} 55m_1 + 8m_2 + 34m_3 & 8m_1 + 2m_2 + 5m_3 & 34m_1 + 5m_2 + 21m_3 \\ 55m_4 + 8m_5 + 34m_6 & 8m_4 + 2m_5 + 5m_6 & 34m_4 + 5m_5 + 21m_6 \\ 55m_7 + 8m_8 + 34m_9 & 8m_7 + 2m_8 + 5m_9 & 34m_7 + 5m_8 + 21m_9 \end{pmatrix} =$$

$$\begin{aligned} \text{де} \quad &= (55m_1 + 8m_2 + 34m_3)(8m_4 + 2m_5 + 5m_6)(34m_7 + 5m_8 + 21m_9) + \\ &+ (55m_4 + 8m_5 + 34m_6)(8m_7 + 2m_8 + 5m_9)(34m_1 + 5m_2 + 21m_3) + \end{aligned}$$

$$\begin{aligned}
 & + (8m_1 + 2m_2 + 5m_3)(34m_4 + 5m_5 + 21m_6)(55m_7 + 8m_8 + 34m_9) - \\
 & - (55m_7 + 8m_8 + 34m_9)(8m_4 + 2m_5 + 5m_6)(34m_1 + 5m_2 + 21m_3) - \\
 & - (55m_4 + 8m_5 + 34m_6)(8m_1 + 2m_2 + 5m_3)(34m_7 + 5m_8 + 21m_9) - \\
 & - (8m_7 + 2m_8 + 5m_9)(34m_4 + 5m_5 + 21m_6)(55m_1 + 8m_2 + 34m_3) = \\
 & = m_1m_5m_9 + m_4m_8m_3 + m_2m_6m_7 - m_7m_5m_3 - m_4m_2m_9 - m_8m_6m_1.
 \end{aligned}$$

Це означає, що зашифроване повідомлення T є коректним, тобто його можна однозначно дешифрувати.

Тепер розглянемо числовий приклад, який підтвердить наше теоретичне припущення. Оскільки початкова матриця M має вигляд (12), то значення її визначника дорівнює

$$\text{Det } M = 92989519071, \quad (24)$$

а значення визначника зашифрованої матриці T становить:

$$\text{Det } T = -92989519071. \quad (25)$$

Порівнявши результати (24) і (25), бачимо, що $\text{Det } T = -\text{Det } M$, тобто вони відповідають контрольному співвідношенню (22).

Розглянемо випадок, коли зашифрована матриця (15) виявилася частково "зруйнованою" внаслідок передачі каналом зв'язку. Нехай "руйнування" цієї матриці відбулося з одним з її елементів, значення якого відрізняється від початкового значення. Наприклад, перший елемент зі значенням 112610 набув значення 212076, тобто, матриця T матиме такий вигляд:

$$T' = \begin{pmatrix} 212076 & 20477 & 69869 \\ 386737 & 59488 & 239184 \\ 54385 & 8437 & 33648 \end{pmatrix}. \quad (26)$$

Визначник цієї матриці дорівнюватиме:

$$\text{Det } T' = -1634889658815, \quad (27)$$

що значно відрізняється від $\text{Det } T$.

Порівнюючи (27) і (24), можемо побачити, що значення визначників матриць не відповідають фундаментальній умові (23) і, отже, матриця (26) є некоректною.

Проте, механізм виявлення помилок є тільки першим кроком у процесі роботи над дешифруванням таємного повідомлення. Завдання полягає в тому, щоб навчитися їх виправляти.

Виправлення помилок у зашифрованому повідомленні

Покажемо тепер можливість відновлення отриманого "зруйнованого" повідомлення T , використовуючи властивості Q_p -матриці, елементами якої є числа Фібоначчі. Продовжимо розгляд зазначеного вище прикладу, коли початкове повідомлення подано у вигляді матриці (10), а формулу для обчислення її визначника показано у виразі (19).

Оскільки кодувальна Q_{34} -матриця має вигляд (13), то зашифрована матриця T набуде вигляду (14). Сутність механізму відновлення "зруйнованих" елементів матриці T' полягає в такому. Паралельно з обчисленням зна-

чень елементів матриці T також обчислюємо визначник початкової матриці M згідно з (19). Зашифроване повідомлення разом зі значенням визначника $(m'_1, m'_2, m'_3, m'_4, Det M)$ посилаємо каналом зв'язку адресату.

Припустимо, що приймач каналу зв'язку адресата має спеціальні засоби для виявлення помилок (що мало ймовірно) у кожному з елементів зашифрованого повідомлення T . Нехай помилку виявлено в першому елементі матриці T . Тоді адресат "зруйноване" повідомлення отримає у такому вигляді:

$$T' = \begin{pmatrix} x & t_2 & t_3 \\ t_4 & t_5 & t_6 \\ t_7 & t_8 & t_9 \end{pmatrix}. \quad (28)$$

де x – "зруйнований" елемент зашифрованого повідомлення T , а решта елементів матриці є коректними і дорівнюють таким значенням:

$$T' = \begin{pmatrix} x & 8m_1 + 2m_2 + 5m_3 & 34m_1 + 5m_2 + 21m_3 \\ 55m_4 + 8m_5 + 34m_6 & 8m_4 + 2m_5 + 5m_6 & 34m_4 + 5m_5 + 21m_6 \\ 55m_7 + 8m_8 + 34m_9 & 8m_7 + 2m_8 + 5m_9 & 34m_7 + 5m_8 + 21m_9 \end{pmatrix} \quad (29)$$

Тоді, згідно з властивістю матричного шифрування, у випадку застосування кодувальної Q_{34} -матриці, значення визначника початкової матриці M має дорівнювати визначнику (19) з протилежним знаком. Тобто, можемо записати таке рівняння для відновлення "зруйнованого" елемента $x = t_1$:

$$\begin{aligned} Det T' = -Det M &\Rightarrow xt_5t_9 + t_4t_8t_3 + t_2t_6t_7 - t_7t_5t_3 - t_4t_2t_9 - t_8t_6x = \\ &= m_1m_5m_9 + m_4m_8m_3 + m_2m_6m_7 - m_7m_5m_3 - m_4m_2m_9 - m_8m_6m_1. \end{aligned} \quad (30)$$

Підставляючи у вираз (30) замість $t_2, t_3, \dots, t_9$ відповідні значення з виразу (29), отримаємо

$$\begin{aligned} &x(8m_4 + 2m_5 + 5m_6)(34m_7 + 5m_8 + 21m_9) + \\ &+ (55m_4 + 8m_5 + 34m_6)(8m_7 + 2m_8 + 5m_9)(34m_1 + 5m_2 + 21m_3) + \\ &+ (8m_1 + 2m_2 + 5m_3)(34m_4 + 5m_5 + 21m_6)(55m_7 + 8m_8 + 34m_9) - \\ &- (55m_7 + 8m_8 + 34m_9)(8m_4 + 2m_5 + 5m_6)(34m_1 + 5m_2 + 21m_3) - \\ &- (55m_4 + 8m_5 + 34m_6)(8m_1 + 2m_2 + 5m_3)(34m_7 + 5m_8 + 21m_9) - \\ &- (8m_7 + 2m_8 + 5m_9)(34m_4 + 5m_5 + 21m_6)x = \\ &= m_1m_5m_9 + m_4m_8m_3 + m_2m_6m_7 - m_7m_5m_3 - m_4m_2m_9 - m_8m_6m_1. \end{aligned}$$

Після виконання нескладних математичних перетворень над цим рівнянням, отримаємо такий його розв'язок:

$$x = 55m_1 + 8m_2 + 34m_3. \quad (31)$$

Покажемо реалізацію цього механізму на конкретному прикладі. Для матриці (28) "зруйнований" елемент $x = t_1$ визначаємо з такої рівності:

$$xt_5t_9 + t_4t_8t_3 + t_2t_6t_7 - t_7t_5t_3 - t_4t_2t_9 - t_8t_6x = -Det M,$$

звідки

$$x = \frac{-Det M - t_4t_8t_3 - t_2t_6t_7 + t_7t_5t_3 + t_4t_2t_9}{t_5t_9 - t_8t_6}.$$

Підставивши у цей вираз числові значення елементів з матриці (26), з'ясуємо, що $x = 112610$, тобто "зруйнований" елемент зашифрованої матриці

T відновлено. Порівнюючи це відновлене значення з елементом зашифрованої матриці T , яке задано виразом (14), можемо побачити, що $x = t_1$. Таким чином, ми відновили зашифроване повідомлення T , використовуючи властивості визначників відповідних матриць. За такою ж самою методикою можна відновити будь-які інші елементи матриці T .

Але в реальних ситуаціях адресат, зазвичай, не знає, які елементи зашифрованого повідомлення "зруйновані". Окрім того, таких "зруйнованих" елементів може бути не один, а декілька, тоді що робити у цих випадках. Розглянуті нижче міркування дають нам деякі відповіді на ці запитання.

У розглянутому вище числовому прикладі початкова матриця M , кодувальна Q_{34} -матриця і зашифрована матриця T представлені відповідно виразами (12), (13) і (15), а співвідношення для визначників представлено виразом (22). Припустимо, що після порівняння визначників $Det T$ і $Det M$ ми з'ясували, що їхні значення не відповідають співвідношенню (22), а це є ознакою появи помилок у зашифрованій матриці (15). Однак ми не маємо інформації щодо конкретного "зруйнованого" елемента матриці T . У цьому випадку виникає дев'ять різних гіпотез щодо можливого "зруйнованого" елемента цієї матриці. Для виявлення одного з них необхідно ці гіпотези перевірити за розглянутою вище методикою виправлення помилок. Проте тут є ще одна умова, яка стосується елементів зашифрованої матриці T : **всі її елементи мають бути цілими числами**. Ось чому під час перевірки дев'ятьох гіпотез до уваги необхідно брати як достовірні тільки ті результати, які приводять нас до отримання цілих чисел. Нарешті, якщо наші тести не отримали цілих чисел ні в одній з перевірок, то це означає, що можлива помилка виникла в двох, трьох і більше елементах зашифрованої матриці T , а вже такі помилки скоректувати практично неможливо.

Висновки

Розглянуто методику матричного шифрування/дешифрування числової інформації з використанням послідовності чисел Фібоначчі (числа "Фі"), у якій використано класичний математичний апарат – теорію матриць. У запропонованій методиці виявлення і виправлення помилок у зашифрованій матриці відповідними об'єктами коректування є не окремі біти або їх комбінації у двійкових кодах, як це прийнято в класичній теорії кодування, а натуральні десяткові числа, що значно спрощує роботу з ними. Таким чином, розглянутий вище метод матричного кодування має принципове значення для розвитку теорії кодування інформації.

Література

1. Воробьев Н.Н. Числа Фибоначчи. – М.: Наука, 1978. – 141 с.
2. Маркушевич А.И. Краткий курс теории аналитических функций. 5-е изд., испр. и доп. – СПб.: Наука, 2006. – 423 с.
3. Маркушевич А.И. Возвратные последовательности. – Л.: Гос. изд. техн. лит-ры, 1950. – 52 с.
4. Нікольський Ю.В., Пасічник В.В., Щербина Ю.М. Дискретна математика: Підручник. – Львів: Магнолія Плюс, 2006. – 608 с.