На рис. 3 також зведено функції надійності (ймовірність безвідмовної роботи) гумових зразків матриці каркасу (брекеру) пневматичних шин за циклічного деформування з різними амплітудами деформацій.

Висновки. Загальний аналіз представлених результатів свідчить, що у гумових зразків каркасу (брекеру) пневматичних шин базове кількість циклів до відмови на фіксованому рівні амплітуд деформацій 50 % зменшилось у 55 разів, а за фіксованих критичних значень еквівалентних напружень – майже у 6 разів.

Література

1. Ayoub G. Multiaxial fatigue life prediction of rubber-like materials using the continuum damage mechanics approach / G. Ayoub, M. Naït-abdelaziz, F. Zaïri, J. M. Gloaguen // Procedia Engineering. – 2010. – Vol. 2, No. 1. – Pp. 985-993.
2. Ayoub G. A continuum damage model for the high-cycle fatigue life prediction of styrene-butadiene rubber under multiaxial loading / G. Ayoub, M. Naït-Abdelaziz, F. Zaïri et al. // International Journal of Solids and Structures. – 2011. – Vol. 48, No. 18. – Pp. 2458-2466.
3. Ларін О.О. Імовірнісна модель накопичення пошкоджуваності втоми в гумоподібних матеріалах / О.О. Ларін // Проблеми міцності : зб. наук. праць. – К. : Вид-во Ін-ту проблем міцності ім. Г.С. Писаренко НАН України. – 2015. – № 6. – С. 84-94.
4. Юрченко А.Н. Автомобильные шины (требования, эксплуатация, износ) / А.Н. Юрченко. – Харьков : Изд-во ДП ХМЗ "ФЭД", 2003. – 115 с.
5. Clark S.K. Mechanics of Pneumatic Tires, US Department of Transportation / S.K. Clark // Dot HS 805952, Washington, DC, 2006. – Pp. 123-129.
6. Ларин А.А. Исследование закономерностей деформирования пневматических шин в контакте с дорогой у учетом наличия эксплуатационной деградации материала / Ю.В. Арефин, А.А. Ларин // Механіка та машинобудування : нак.-техн. журнал. – Харків : Вид-во НТУ "ХПІ", 2011. – № 2. – С. 52-57.
7. Овчаров В.И. Свойства резиновых смесей и резин: оценка регулирование, стабилизация / В.И. Овчаров, М.В. Бурмистр, А.Г. Смирнов, В.А. Тютин, В.В. Вербас, А.П. Науменко. – М. : Изд-во "САНТ – ТМ", 2001. – 400 с.
8. Baldwin J.M. Rubber aging in tires. part 1: field results / J.M. Baldwin, D.R. Bauer, K.R. Ellwood // Polymer Degradation and Stability. – 2007. – Vol. 92, No. 1. – Pp. 103-109.
9. Bauer D.R. Rubber aging in tires. part 2: accelerated oven aging tests / D.R. Bauer, J.M. Baldwin, K.R. Ellwood // Polymer Degradation and Stability. – 2007. – Vol. 92, No. 1. – Pp. 110-117.
10. Ларін О.О. Дослідження характеристик опору втомі гумових сумішей, що входять до складу елементів пневматичних шин після штучного старіння матеріалу / О.О. Ларін // Вісник Національного технічного університету України "Київський політехнічний інститут". – Сер.: Нові рішення в сучасних технологіях. – К. : Вид-во НТУУ "КПІ". – 2015. – № 46. – С. 45-50.

Ларин О.О. **Исследование изменений вероятностных характеристик отказов усталости резиновых материалов в первоначальном состоянии и после старения**

Представлен анализ вероятностных характеристик отказов усталости в резиновых материалах при их циклической нагрузке. Исследования проведены на основе концепции континуальной механики повреждаемости. Кинетика роста повреждаемости определена по характеристикам кривых усталости, которые построены относительно эквивалентных напряжений, которые соответствуют приведению сложного напряженно-деформированного состояния к эквивалентному простому на умеренных деформациях резиновых материалов. Исследование проведено для материала, применяемого в качестве матрицы каркаса пневматических шин. Проведен сравнительный анализ изменения вероятности отказа вследствие усталости для материала до и после старения.

Ключевые слова: усталость, повреждаемость, резиновые материалы, старение.

Larin O.O. **The Investigation of the Change of Probability Characteristics of the Fatigue Failures of Rubber before and after Aging**

The analysis of the probability characteristics of fatigue failure in the rubber materials under cyclic loading is presented. A research has been carried out based on the continuum damage mechanics. Kinetics of damage is determined by the characteristics of fatigue curves. The fatigue S-N curves are built relative to equivalent stress that represents the complex stress strain state to an equivalent simple state subjected to the possibility of appearance of finite strains. The study has been carried out for a material that is used as a matrix of pneumatic tire carcass. A comparative analysis of changes in the probability of failure due to fatigue of the rubber material before and after aging has been done.

Keywords: fatigue, continuum damage, rubber materials, aging.

УДК 681.3.05:004.056.5

Проф. Ю.І. Грицюк, д-р техн. наук – НУ "Львівська політехніка"; здобувач П.Ю. Грицюк, магістр – НЛТУ України, м. Львів

МАТЕМАТИЧНІ ОСНОВИ ПРОЦЕСУ ГЕНЕРУВАННЯ КЛЮЧІВ ПЕРЕСТАВЛЯННЯ З ВИКОРИСТАННЯМ ШИФРУ КАРДАНО

Розглядаються особливості розроблення надійного алгоритму для генерування ключів переставляння, робота якого базується на класичному шифрі Кардано "квадратні ґратки" у його сучасному математичному формулюванні, що загалом дає змогу генерувати послідовності випадкових чисел у заданому діапазоні без повторення.

Встановлено, що алгоритм "квадратні ґратки", будучи алгоритмом маршрутного переставляння, в якому правило розміщення символів у блоці задається квадратним трафаретом, можна використовувати не тільки для шифрування блоку вхідного повідомлення, але й для генерування відповідної множини ключів переставляння. З використанням основних положень матричної алгебри розроблено математичне формулювання алгоритму "квадратні ґратки" для генерування ключів переставляння, а також математичне формулювання алгоритму переставляння рядків матриці вхідного повідомлення, кількість стовпців якої може бути довільною.

Ключові слова: захист інформації, шифр Кардано, шифрувальні трафарети, перестановні алгоритми, алгоритми маршрутного переставляння, алгоримт "прямокутні та квадратні ґратки", генерування ключів переставляння, криптоаналіз.

Вступ. В роботі [6] зазначено, що у сучасних складних алгоритмах шифрування/дешифрування інформації широко використовуються алгоритми маршрутного переставляння. Сутність таких алгоритмів полягає в тому, що в клітини прямокутної таблиці символи вхідного повідомлення вписують за одним маршрутом, а потім ці символи зчитують з таблиці за іншим маршрутом.

Прикладом простого переставляння є запис блоку початкових даних у прямокутну таблицю рядками, а зчитування – стовпцями чи навпаки. Послідовність заповнення рядків таблиці та зчитування зашифрованих даних стовпцями називають ключем переставляння. Відомими алгоритмами переставляння [4] є: магічні квадрати та шахові дошки; класичні та табличні шифри переставляння; маршрутне переставляння з використанням трафаретів; маршрутне переставляння з використання складних геометричних фігур, наприклад, фігур Гамільтона. У кожному із цих алгоритмів ключі переставляння утворюються за рахунок різниці шляхів запису символів початкових даних і шляхів зчитування цих символів у межах деякої геометричної фігури [8]. Часто ці символи мають свою числову нумерацію, тому, як наслідок, отримані в такі способи послідовності чисел часто мають випадковий характер.

Отже, суть більшості відомих алгоритмів переставляння полягає в поділі початкових даних на блоки фіксованої довжини і в подальшому переставлянні символів усередині кожного блоку за певним алгоритмом [1, ст. 171; 7, ст. 11]. Такі криптографічні перетворення призводять тільки до зміни порядку розміщення символів у середині будь-якого блоку вхідного повідомлення. Наведені вище алгоритми переставляння не повністю відповідають ГПВЧ як таким, що мають довгий період повторення, чи послідовні значення чисел є незалежними і т.д. Тут важливо, щоб згенеровані послідовності випадкових чисел знаходилися у заданому діапазоні – від 1 до R і без повторень [2]. Вважається [5], що при достатній довжині блоку, в межах якого здійснюється переставляння вхідних символів, і складному неповторному його порядку можна досягти прийнятної криптографічної стійкості алгоритму для простих практичних застосувань.

У роботі [6] також було встановлено, що шифр "прямокутні ґратки", будучи алгоритмом маршрутного переставляння, в якому правило розміщення символів задається отворами в прямокутному трафареті, можна використовувати не тільки для шифрування блоку вхідного повідомлення, але й для генерування ключів переставляння. З використанням основних положень матричної алгебри розроблено математичне формулювання алгоритму "прямокутні ґратки" для генерування ключів переставляння, а також математичне формулювання алгоритму переставляння стовпців матриці вхідного повідомлення, кількість рядків якого може бути довільною.

Однак у жодній із відомих на сьогодні робіт не наведено реалізацію шифру Кардано "квадратні ґратки" у його сучасному математичному формулюванні, який би давав змогу генерувати послідовності випадкових чисел у заданому діапазоні без повторення. Також потрібно навести математичне формулювання алгоритму "квадратні ґратки", яке б давало змогу здійснити надійну програмну його реалізацію, та провести аналіз криптографічної його стійкості.

Об'єкт дослідження – генерування ключів переставляння.

Предмет дослідження – математичні основи реалізації шифру Кардано "квадратні ґратки" для генерування певної послідовності випадкових чисел у заданому діапазоні без повторення.

Мета роботи полягає в розробленні надійного алгоритму генерування ключів переставляння, який базується на класичному шифрі Кардано "прямокутні ґратки" у його сучасному математичному формулюванні, що дає змогу генерувати послідовності випадкових чисел у заданому діапазоні без повторення.

Для реалізації зазначеної мети потрібно виконати такі основні завдання:

1) відтворити історію появи шифру Кардано, який належить до класичних методів захисту інформації;
2) здійснити реалізацію шифру Кардано "прямокутні ґратки" у його сучасній його математичній інтерпретації, яка б давала змогу генерувати задані послідовності випадкових чисел у заданому діапазоні без повторення;
3) навести математичне формулювання алгоритму "прямокутні ґратки", яке б давало змогу здійснити надійну програмну його реалізацію;
4) провести аналіз криптографічної стійкості алгоритму маршрутного переставляння "прямокутні ґратки";
5) зробити відповідні висновки та надати рекомендації щодо використання.

1. Історія появи алгоритмів маршрутного переставляння

У 1550 році Джироламо Кардано (1501-1576 рр.) запропонував використовувати картонні прямокутні ґратки з отвори для зчитування послідовності окремих символів, з яких потім мали складатися слова та будуватися речення. При цьому вхідне послання записується у вигляді звичайного тексту, яке і є, вочевидь, криптограмою. Отже, Кардано маскував свої повідомлення під звичайне послання так, що б вони не були схожі на зашифровані тексти.

Загалом такі замасковані повідомлення вважаються прикладом стеганограми, яка є різновидом криптограми. Але ім'я Кардано стосується прямокутних ґраток, які, швидше за все, могли й не бути його винаходом. Тим не менше, шифри, реалізовані з використанням картонних прямокутних ґраток, прийнято називати шифрами Кардано.

Відомо, що Кардинал Рішельє (1585-1642 рр.) був прихильником шифру Кардано і використовував їх у особистому та діловому листуванні. Освічені мешканці Європи XVII ст. були знайомі з грою слів у літературі, в т.ч. з акровіршем, анаграмою і шифрами [1]. До кінця XVII ст. перші картонні ґратки Кардано вже майже не використовувалися, але іноді вони все ж таки з'являлися у вигляді зашифрованих повідомлень, а також як літературні шедеври. Наприклад, Джордж Гордон Байрон часто користувався картонними ґратками Кардано швидше за все для демонстрації своїх літературних навиків, ніж для серйозного шифрування інформації.

Одна з різновидів ґратки Кардано – поворотна ґратка або сітка, в основі якої знаходиться шахова дошка, яка використовувалася в кінці XVI ст. Поворотна ґратка знову з'явилася в більш складній формі в кінці XIX ст., але до цього часу будь-який зв'язок з ґраткою Кардано залишився тільки в назві. Вочевидь прямокутні ґратки з отворами для записування певних символів за одним порядком і зчитування їх у іншому порядку можна назвати в честь Кардано, але їх також називають просто картонними шифрувальними ґратками.

2. Реалізація шифру Кардано "квадратні ґратки". Одним із прикладів алгоритму маршрутного переставляння є відомий шифр Кардано, який вважається блоковим алгоритмом з періодом $R = n^2$, де n – парне число. В цьому шифрі як ключ виготовляється квадратний трафарет розміром $n \times n$, четверту частину (тобто, $n^2/4$) клітин якого вирізають. На рис. 1 наведено приклад квадратного трафарету для $n = 4$, де сам квадрат показано штрих-пунктирною лінією, а контури чотирьох вирізаних отворів виділено суцільною лінією.

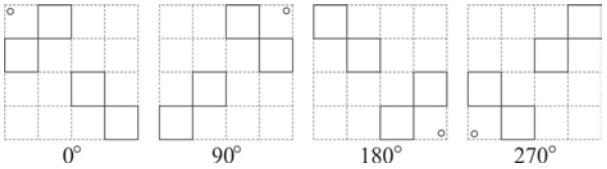

Рис. 1. Квадратний трафарет та правило його повертання

Нехай потрібно зашифрувати блок вхідного повідомлення, у якому знаходиться n^2 символів. Повідомлення будемо записувати у клітини квадратного трафарету розміром $n \times n$, яку назвемо матрицею майбутньої криптограми. Про-

цедура шифрування займає чотири кроки. На першому кроці на початкову матрицю криптограми накладаємо трафарет і вписуємо перші $n^2/4$ символи у отвори, починаючи з верхнього рядка. На другому кроці трафарет повертаємо на 90° за годинниковою стрілкою відносно його центра і у отвори знову вписуємо наступні $n^2/4$ символи повідомлення. Аналогічно виконуємо третій і четвертий кроки, повертаючи щоразу трафарет на 90°, після чого у нові позиції отворів вписуємо наступні символи повідомлення.

Дешифрування криптограми виконаємо у зворотному порядку з зазначенням положень квадратного трафарету і маршрутів зчитування його отворів. Одержувач повідомлення, котрий має точно такий самий трафарет, без жодних труднощів прочитає початкове повідомлення, накладаючи його на матрицю криптограми за встановленим порядком у чотири положення.

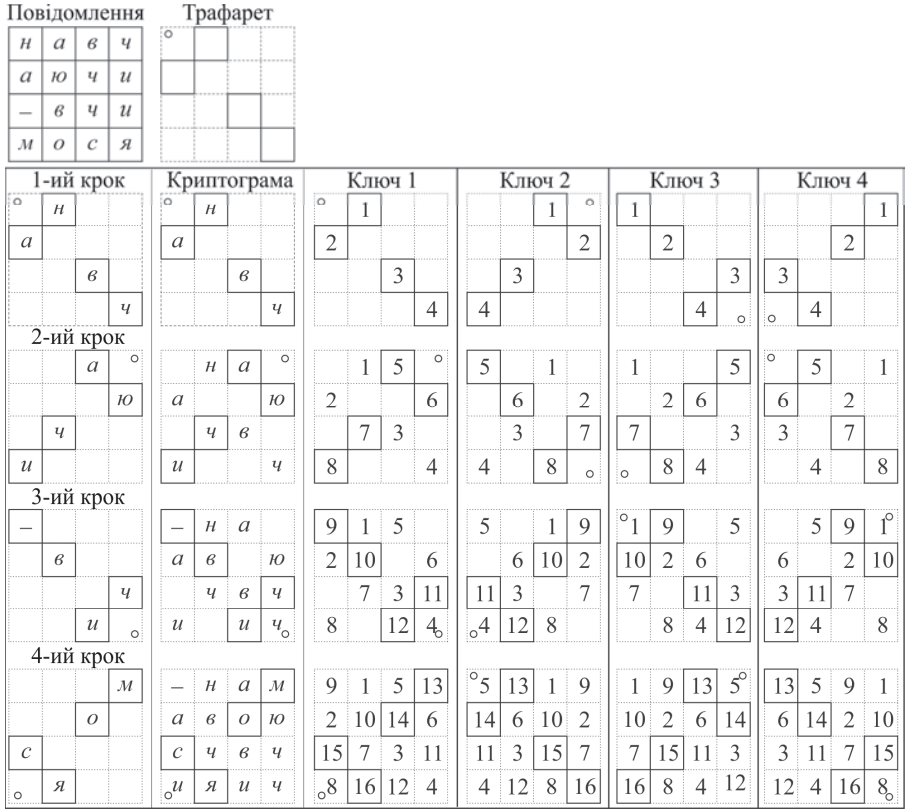

Рис. 2. Кроки шифрування вхідного повідомлення та можливі ключі переставляння

Квадратний трафарет (тобто ключ вписування символів) потрібно виготовити так, щоб при кожному його повертанні вирізані у ньому отвори потрапили на вільні клітини матриці криптограми, і в жодному разі не накладалися на ті її клітини, які вже було попередньо заповнено. Внаслідок виконання таких дій після четвертого кроку всі символи блоку вхідного повідомлення будуть

розміщені у матриці криптограми за порядком, визначеним ключем їх вписування. Зчитавши ці символи за рядками чи стовпцями, отримаємо зашифроване повідомлення. На рис. 2 показано криптографічне перетворення вхідного повідомлення *навчаючи вчимося* (docendo discimus[1]) у таку криптограму *_намаво-юсчвчияич*.

Шифрування даних з використанням квадратного трафарету є блоковим шифром з розміром блоку $R = n^2$. У наведеному вище прикладі $R = 4\times4 = 16$ символів. Кількість можливих трафаретів $Q_n = 4^{n^2/4}$ різко зростає зі збільшенням значення n. Наприклад, для трафарету розміром 2×2 – $Q_2 = 4^{2^2/4} = 4$, для 4×4 – $Q_4 = 4^{4^2/4} = 256$, а для 6×6 – $Q_6 = 4^{6^2/4} = 262144$. У кожному з цих ключів переставляння послідовні значення чисел хоча і матимуть малий період повторення, однак будуть незалежними між собою, що і є одним із основних їх достоїнств.

Шифр Кардано є алгоритмом маршрутного переставляння, в якому правило переставлення символів у блоці задається квадратним трафаретом, тобто є зручним для реалізації на папері ручним способом. Загалом цей алгоритм також дає змогу переставляти $R = n^2$ чисел у довільному порядку з періодом їх повторення $R!$ У нашому прикладі алгоритм "квадратні ґратки" можна використовувати для генерування ключів переставляння довжиною $R = 4^2 = 16$ чисел. Кількість всіх можливих переставлянь у ключі такої довжини становить $16! = 2{,}09\cdot10^{13}$, що в багато разів більше за кількість трафаретів Q_4. Вирішення завдання перебору ключів переставляння у цьому випадку навіть для сучасних ЕОМ представляє істотну складність.

Ключ переставляння зручно задавати у вигляді такого одновимірного масиву:

$$\tilde{K} = \{k_j, j = \overline{1,R}\} = \begin{Bmatrix} 1 & 2 & & j & & R \\ k_1 & k_2 & \dots & k_j & \dots & k_R \end{Bmatrix},$$

який показує, що перший символ блоку вхідного повідомлення займає k_1 позицію у блоці криптограми, другий символ переміщається на позицію k_2 і т.д. Наприклад, при $R = 4^2$ ключ переставляння (ключ 1), отриманий при реалізації наведеного вище прикладу (рис. 2), при зчитуванні чисел рядками матриці зліва на право має такий вигляд:

$$\tilde{K}_1 = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 9 & 1 & 5 & 13 & 2 & 10 & 14 & 6 & 15 & 7 & 3 & 11 & 8 & 16 & 12 & 4 \end{Bmatrix},$$

а для ключа 3 – такий вигляд:

$$\tilde{K}_3 = \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 9 & 13 & 5 & 10 & 2 & 6 & 14 & 7 & 15 & 11 & 3 & 16 & 8 & 4 & 12 \end{Bmatrix}.$$

Зрозуміло, якщо зчитувати числа стовпцями матриці зверху вниз, то відповідні ключі переставляння будуть мати зовсім інший вигляд.

[1] Docendo discimus (з лат., дослівно – навчаючи навчаюсь) – латинська сентенція, сформульована Сенекою (молодшим в його листах до свого друга Луцілія Молодшого – римського губернатора Сицилії в часи правління Нерона. В сьомому листі "Моральних листів до Луцілія" (лат. – Epistulae morales ad Lucilium) Сенека, серед іншого, зазначає, що люди навчаючи когось, навчаються самі.

Алгоритм маршрутного переставляння "квадратні ґратки" є легким у використанні. Проте дешифрування зашифрованої інформації є не з легких. Щоб її дешифрувати потрібно: мати квадратний трафарет; знати послідовність заповнення його клітин; правильно використовувати даний трафарет.

Без трафарету зловмисник не в змозі навіть зрозуміти значення інформації. Якщо зловмисник отримає тільки трафарет, то ймовірність розшифрування інформації є мінімальною. Якщо ж він буде знати ще й послідовність його заповнення, то для одержання бажаного результату піде менше зусиль і часу.

Можна використовувати як квадратні, так і прямокутні трафарети **[6]**. Легшим у використанні є квадратні трафарети. Вони можуть бути різних розмірів і різних шаблонів. Кожен шаблон – це різний ключ шифрування. Існує рівно стільки методів шифрування одного шаблону, скільки є прорізів у трафареті. Втрата одного з трафаретів призводить до втрати всієї секретної переписки.

Врахувавши усі наведені вище пункти можна вважати, що алгоритм маршрутного переставляння "квадратні ґратки" є криптографічно стійким. Його використання є прогресивним. Але, як і будь що у цьому світі, він має свої недоліки: метод є повільним; вимагає наявності літературних навиків; шифрувальний апарат може бути загублений або конфіскований.

Отже, шифр Кардано "квадратні ґратки" можна використовувати не тільки для шифрування блоку вхідного повідомлення, але й для генерування ключів переставляння. Проте, як зазначалося вище, цей шифр є зручним для реалізації на папері ручним способом. Насправді це далеко не так. Спробуємо його дещо математизувати, тобто наведемо математичне формулювання алгоритму Кардано "квадратні ґратки" для генерування ключів переставляння, а також математичне формулювання алгоритму переставляння рядків матриці вхідного повідомлення, кількість стовпців якого може бути довільною. Для цього використаємо інструментарій матричної алгебри[1] **[3]**.

3. Математичне формулювання алгоритму "квадратні ґратки". Вхідні елементи шифру Кардано при N=4 подано на рис. 3.

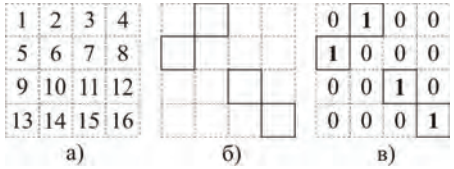

Рис. 3. Вхідні елементи алгоритму "квадратні ґратки": *а) – вхідне повідомлення; б) – квадратний трафарет з отворами; в) – матричне подання трафарету*

З рисунку видно, що вхідне повідомлення (рис. 3, а) складається з $R=N^2=16$ символів (чисел – у нашому випадку). Подамо його у вигляді такого одновимірного масиву:

$$\tilde{C}=\left\{c_j=j, j=\overline{1,R}\right\}\Rightarrow \tilde{C}^{(l)}=\left\{c^{(l)}_{(l-1)\cdot N+j}, j=\overline{1,N}\right\}, l=\overline{1,L}= \\ =\left\{\underbrace{1\ \ 2\ \ 3\ \ 4}_{l=1\ блок}\ \ \underbrace{5\ \ 6\ \ 7\ \ 8}_{l=2\ блок}\ \ \underbrace{9\ \ 10\ \ 11\ \ 12}_{l=3\ блок}\ \ \underbrace{13\ \ 14\ \ 15\ \ 16}_{l=4\ блок}\right\}, \quad (1)$$

[1] Матрична алгебра [matrix algebra] – розділ алгебри, присвячений правилам дій над матрицями.

де L=4 – кількість кроків процесу шифрування. У цьому масиві для l-го кроку виділено відповідні блоки чисел вхідного повідомлення.

Квадратний трафарет при 0° має таке матричне подання:

$$\bar{\bar{G}}^0=\left|\bar{G}^0_i=\left|g^0_{ij}, j=\overline{1,N}\right|, i=\overline{1,N}\right|=\left\|\begin{matrix}0&\mathbf{1}&0&0\\ \mathbf{1}&0&0&0\\ 0&0&\mathbf{1}&0\\ 0&0&0&\mathbf{1}\end{matrix}\right\|. \quad (2)$$

Матрицю інвертування рядків чи стовпців матриці подання трафарету сформуємо за допомогою такого виразу:

$$\bar{\bar{I}}=\left|\bar{I}_i=\left|i_{ij}=\begin{cases}1, \text{ якщо } i=N-j+1;\\ 0-\text{інакше},\end{cases} j=\overline{1,N}\right|, i=\overline{1,N}\right|=\left\|\begin{matrix}0&0&0&\mathbf{1}\\ 0&0&\mathbf{1}&0\\ 0&\mathbf{1}&0&0\\ \mathbf{1}&0&0&0\end{matrix}\right\|. \quad (3)$$

Початкова матриця криптограми має такий вигляд:

$$\bar{\bar{T}}^{(0)}=\left|\bar{T}^{(0)}_i=\left|t^{(0)}_{ij}=0,\ j=\overline{1,N}\right|, i=\overline{1,N}\right|=\left\|\begin{matrix}0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\end{matrix}\right\|. \quad (4)$$

***Крок* 1**. Процедура вписування символів (чисел) l=1-го блоку вхідного повідомлення через отвори трафарету при 0° у клітини матриці криптограми має таке математичне формулювання:

$$f:\{\tilde{C}^{(1)}, \bar{\bar{G}}^0\}\mapsto \bar{\bar{T}}^0\Rightarrow \bar{\bar{T}}^0=\left|\bar{T}^0_i=\left|t^0_{ij}=F(c^{(1)}_{0\cdot N+j}, g^0_{ij}),\ j=\overline{1,N}\right|, i=\overline{1,N}\right|= \\ =\{1\ \ 2\ \ 3\ \ 4\}\rightarrow\left\|\begin{matrix}0&\mathbf{1}&0&0\\ \mathbf{1}&0&0&0\\ 0&0&\mathbf{1}&0\\ 0&0&0&\mathbf{1}\end{matrix}\right\|=\left\|\begin{matrix}0&\mathbf{1}&0&0\\ \mathbf{2}&0&0&0\\ 0&0&\mathbf{3}&0\\ 0&0&0&\mathbf{4}\end{matrix}\right\|, \quad (5)$$

де $F()$ – функція, яка програмно реалізує дії зазначеної процедури.

Матриця криптограми на 1-му кроці має такий вигляд:

$$\bar{\bar{T}}^{(0)}+\bar{\bar{T}}^0=\bar{\bar{T}}^{(1)}=\left|\bar{T}^{(1)}_i=\left|t^{(1)}_{ij}=t^{(0)}_{ij}+t^0_{ij},\ j=\overline{1,N}\right|, i=\overline{1,N}\right|= \\ =\left\|\begin{matrix}0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\end{matrix}\right\|+\left\|\begin{matrix}0&\mathbf{1}&0&0\\ \mathbf{2}&0&0&0\\ 0&0&\mathbf{3}&0\\ 0&0&0&\mathbf{4}\end{matrix}\right\|=\left\|\begin{matrix}0&\mathbf{1}&0&0\\ \mathbf{2}&0&0&0\\ 0&0&\mathbf{3}&0\\ 0&0&0&\mathbf{4}\end{matrix}\right\|. \quad (6)$$

***Крок* 2**. Процедуру повертання трафарету на кут 90° реалізуємо, виходячи з попереднього його стану, за допомогою такого матричного виразу:

$$\bar{\bar{G}}^0\times\bar{\bar{I}}=\bar{\bar{G}}^{90}=\left|\bar{G}^{90}_i=\left|g^{90}_{ij}=\sum_{k=1}^{N}g^0_{ik}\cdot i_{kj}, j=\overline{1,N}\right|, i=\overline{1,N}\right|= \\ =\left\|\begin{matrix}0&\mathbf{1}&0&0\\ \mathbf{1}&0&0&0\\ 0&0&\mathbf{1}&0\\ 0&0&0&\mathbf{1}\end{matrix}\right\|\times\left\|\begin{matrix}0&0&0&\mathbf{1}\\ 0&0&\mathbf{1}&0\\ 0&\mathbf{1}&0&0\\ \mathbf{1}&0&0&0\end{matrix}\right\|=\left\|\begin{matrix}0&0&\mathbf{1}&0\\ 0&0&0&\mathbf{1}\\ 0&\mathbf{1}&0&0\\ \mathbf{1}&0&0&0\end{matrix}\right\|. \quad (7)$$

Процедура вписування символів (чисел) *l*=2-го блоку вхідного повідомлення через отвори трафарету при 90° у клітини матриці криптограми має таке математичне формулювання:

$$f:\{\tilde{C}^{(2)},\bar{\bar{G}}^{90}\}\mapsto\bar{\bar{T}}^{90}\Rightarrow\bar{\bar{T}}^{90}=\left|\bar{T}_i^{90}=\left|t_{ij}^{90}=F(c_{1\cdot N+j}^{(2)},g_{ij}^{90}),\ j=\overline{1,N}\right|,i=\overline{1,N}\right|=$$
$$=\{5\ \ 6\ \ 7\ \ 8\}\mapsto\begin{Vmatrix}0&0&\mathbf{1}&0\\0&0&0&\mathbf{1}\\0&\mathbf{1}&0&0\\\mathbf{1}&0&0&0\end{Vmatrix}=\begin{Vmatrix}0&0&\mathbf{5}&0\\0&0&0&\mathbf{6}\\0&\mathbf{7}&0&0\\\mathbf{8}&0&0&0\end{Vmatrix}. \quad (8)$$

Матриця криптограми на 2-му кроці має такий вигляд:

$$\bar{\bar{T}}^{(1)}+\bar{\bar{T}}^{90}=\bar{\bar{T}}^{(2)}=\left|\bar{T}_i^{(2)}=\left|t_{ij}^{(2)}=t_{ij}^{(1)}+t_{ij}^{90},\ j=\overline{1,N}\right|,i=\overline{1,N}\right|=$$
$$=\begin{Vmatrix}0&\mathbf{1}&0&0\\\mathbf{2}&0&0&0\\0&0&\mathbf{3}&0\\0&0&0&\mathbf{4}\end{Vmatrix}+\begin{Vmatrix}0&0&\mathbf{5}&0\\0&0&0&\mathbf{6}\\0&\mathbf{7}&0&0\\\mathbf{8}&0&0&0\end{Vmatrix}=\begin{Vmatrix}0&\mathbf{1}&\mathbf{5}&0\\\mathbf{2}&0&0&\mathbf{6}\\0&\mathbf{7}&\mathbf{3}&0\\\mathbf{8}&0&0&\mathbf{4}\end{Vmatrix}. \quad (9)$$

***Крок* 3**. Процедуру повертання трафарету на кут 180° реалізуємо, виходячи з попереднього його стану, за допомогою такого матричного виразу:

$$\bar{\bar{I}}\times\bar{\bar{G}}^{90}=\bar{\bar{G}}^{180}=\left|\bar{G}_i^{180}=\left|g_{ij}^{180}=\sum_{k=1}^{N}i_{ik}\cdot g_{kj}^{90},j=\overline{1,N}\right|,i=\overline{1,N}\right|=$$
$$=\begin{Vmatrix}0&0&0&\mathbf{1}\\0&0&\mathbf{1}&0\\0&\mathbf{1}&0&0\\\mathbf{1}&0&0&0\end{Vmatrix}\times\begin{Vmatrix}0&0&\mathbf{1}&0\\0&0&0&\mathbf{1}\\0&\mathbf{1}&0&0\\\mathbf{1}&0&0&0\end{Vmatrix}=\begin{Vmatrix}\mathbf{1}&0&0&0\\0&\mathbf{1}&0&0\\0&0&0&\mathbf{1}\\0&0&\mathbf{1}&0\end{Vmatrix}. \quad (10)$$

Процедура вписування символів (чисел) *l*=3-го блоку вхідного повідомлення через отвори трафарету при 180° у клітини матриці криптограми має таке математичне формулювання:

$$f:\{\tilde{C}^{(3)},\bar{\bar{G}}^{180}\}\mapsto\bar{\bar{T}}^{180}\Rightarrow\bar{\bar{T}}^{180}=\left|\bar{T}_i^{180}=\left|t_{ij}^{180}=F(c_{2\cdot N+j}^{(3)},g_{ij}^{180}),\ j=\overline{1,N}\right|,i=\overline{1,N}\right|=$$
$$=\{9\ \ 10\ \ 11\ \ 12\}\mapsto\begin{Vmatrix}\mathbf{1}&0&0&0\\0&\mathbf{1}&0&0\\0&0&0&\mathbf{1}\\0&0&\mathbf{1}&0\end{Vmatrix}=\begin{Vmatrix}\mathbf{9}&0&0&0\\0&\mathbf{10}&0&0\\0&0&0&\mathbf{11}\\0&0&\mathbf{12}&0\end{Vmatrix}. \quad (11)$$

Матриця криптограми на 3-му кроці має такий вигляд:

$$\bar{\bar{T}}^{(2)}+\bar{\bar{T}}^{180}=\bar{\bar{T}}^{(3)}=\left|\bar{T}_i^{(3)}=\left|t_{ij}^{(3)}=t_{ij}^{(2)}+t_{ij}^{180},\ j=\overline{1,N}\right|,i=\overline{1,N}\right|=$$
$$=\begin{Vmatrix}0&\mathbf{1}&\mathbf{5}&0\\\mathbf{2}&0&0&\mathbf{6}\\0&\mathbf{7}&\mathbf{3}&0\\\mathbf{8}&0&0&\mathbf{4}\end{Vmatrix}+\begin{Vmatrix}\mathbf{9}&0&0&0\\0&\mathbf{10}&0&0\\0&0&0&\mathbf{11}\\0&0&\mathbf{12}&0\end{Vmatrix}=\begin{Vmatrix}\mathbf{9}&\mathbf{1}&\mathbf{5}&0\\\mathbf{2}&\mathbf{10}&0&\mathbf{6}\\0&\mathbf{7}&\mathbf{3}&\mathbf{11}\\\mathbf{8}&0&\mathbf{12}&\mathbf{4}\end{Vmatrix}. \quad (12)$$

***Крок* 4**. Процедуру повертання трафарету на кут 270° реалізуємо, виходячи з попереднього його стану, за допомогою такого матричного виразу:

$$\bar{\bar{G}}^{180}\times\bar{\bar{I}}=\bar{\bar{G}}^{270}=\left|\bar{G}_i^{270}=\left|g_{ij}^{270}=\sum_{k=1}^{N}g_{ik}^{180}\cdot i_{kj},j=\overline{1,N}\right|,i=\overline{1,N}\right|=$$
$$=\begin{Vmatrix}\mathbf{1}&0&0&0\\0&\mathbf{1}&0&0\\0&0&0&\mathbf{1}\\0&0&\mathbf{1}&0\end{Vmatrix}\times\begin{Vmatrix}0&0&0&\mathbf{1}\\0&0&\mathbf{1}&0\\0&\mathbf{1}&0&0\\\mathbf{1}&0&0&0\end{Vmatrix}=\begin{Vmatrix}0&0&0&\mathbf{1}\\0&0&\mathbf{1}&0\\\mathbf{1}&0&0&0\\0&\mathbf{1}&0&0\end{Vmatrix}. \quad (13)$$

Процедура вписування символів (чисел) *l*=4-го блоку вхідного повідомлення через отвори трафарету при 280° у клітини матриці криптограми має таке математичне формулювання:

$$f:\{\tilde{C}^{(4)},\bar{\bar{G}}^{270}\}\mapsto\bar{\bar{T}}^{270}\Rightarrow\bar{\bar{T}}^{270}=\left|\bar{T}_i^{270}=\left|t_{ij}^{270}=F(c_{3\cdot N+j}^{(4)},g_{ij}^{270}),\ j=\overline{1,N}\right|,i=\overline{1,N}\right|=$$
$$=\{13\ \ 14\ \ 15\ \ 16\}\mapsto\begin{Vmatrix}0&0&0&\mathbf{1}\\0&0&\mathbf{1}&0\\\mathbf{1}&0&0&0\\0&\mathbf{1}&0&0\end{Vmatrix}=\begin{Vmatrix}0&0&0&\mathbf{13}\\0&0&\mathbf{14}&0\\\mathbf{15}&0&0&0\\0&\mathbf{16}&0&0\end{Vmatrix}. \quad (14)$$

Матриця криптограми на 4-му кроці має такий вигляд:

$$\bar{\bar{T}}^{(3)}+\bar{\bar{T}}^{270}=\bar{\bar{T}}^{(4)}=\left|\bar{T}_i^{(4)}=\left|t_{ij}^{(4)}=t_{ij}^{(3)}+t_{ij}^{270},\ j=\overline{1,N}\right|,i=\overline{1,N}\right|=$$
$$=\begin{Vmatrix}\mathbf{9}&\mathbf{1}&\mathbf{5}&0\\\mathbf{2}&\mathbf{10}&0&\mathbf{6}\\0&\mathbf{7}&\mathbf{3}&\mathbf{11}\\\mathbf{8}&0&\mathbf{12}&\mathbf{4}\end{Vmatrix}+\begin{Vmatrix}0&0&0&\mathbf{13}\\0&0&\mathbf{14}&0\\\mathbf{15}&0&0&0\\0&\mathbf{16}&0&0\end{Vmatrix}=\begin{Vmatrix}\mathbf{9}&\mathbf{1}&\mathbf{5}&\mathbf{13}\\\mathbf{2}&\mathbf{10}&\mathbf{14}&\mathbf{6}\\\mathbf{15}&\mathbf{7}&\mathbf{3}&\mathbf{11}\\\mathbf{8}&\mathbf{16}&\mathbf{12}&\mathbf{4}\end{Vmatrix}. \quad (15)$$

Перетворення елементів матриці криптограми у елементи одновимірного масиву при зчитуванні символів (чисел) рядками матриці зліва на право виконуємо за такою формулою:

$$f:\bar{\bar{T}}^{(4)}\to\tilde{K}\Rightarrow\tilde{K}=\left\{k_{(i-1)\cdot N+j}=t_{ij}^{(4)},j=\overline{1,N};\ i=\overline{1,N}\right\};\ R=N^2\Rightarrow$$
$$\tilde{K}=\{k_j,j=\overline{1,R}\}=\{9\ \ 1\ \ 5\ \ 13\ \ 2\ \ 10\ \ 14\ \ 6\ \ 15\ \ 7\ \ 3\ \ 11\ \ 8\ \ 16\ \ 12\ \ 4\}, \quad (16)$$

де $\tilde{K}$ – ключ переставляння рядка символів.

Роботу алгоритму завершено.

4. Математичне формулювання алгоритму переставляння

Для розуміння подальших дій ключ переставляння подамо у дещо меншому вигляді [6], а саме:

$$\tilde{K}=\{k_j,j=\overline{1,M}\}=\{3,5,2,6,1,4\}:M=6. \quad (17)$$

Матрицю переставляння рядків матриці під час виконання прямого ходу сформуємо за допомогою такого виразу:

$$\bar{\bar{P}}=\left|\bar{P}_j=\left|p_{ij}=\begin{cases}1,\text{ якщо}\,k_i=j;\\0-\text{інакше},\end{cases}i=\overline{1,M}\right|,j=\overline{1,M}\right|=$$

$k_i \setminus j$	1	2	3	4	5	6
3	0	0	**1**	0	0	0
5	0	0	0	0	**1**	0
2	0	**1**	0	0	0	0
6	0	0	0	0	0	**1**
1	**1**	0	0	0	0	0
4	0	0	0	**1**	0	0

(18)

Матрицю переставляння рядків матриці під час виконання зворотного ходу сформуємо за допомогою такого виразу:

$$\overline{\overline{P}}^{-1} = \left| \overline{P}_i^{-1} = \left| p_{ij}^{-1} = \begin{cases} 1, \text{ якщо } k_j = i; \\ 0 - \text{інакше}, \end{cases} j = \overline{1,M} \right|, i = \overline{1,M} \right| = \left| \begin{array}{c|cccccc} i \setminus k_j & \mathbf{3} & \mathbf{5} & \mathbf{2} & \mathbf{6} & \mathbf{1} & \mathbf{4} \\ \hline 1 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 2 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 3 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 5 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \end{array} \right|. \quad (19)$$

Прямий хід. Вхідне повідомлення: *До_булави_треба_мудрої_голови!* складається з R=30 символів. Подамо його у вигляді одновимірного масиву:

$$\tilde{C} = \{c_j, j = \overline{1,R}\} = \{\text{До\_булави\_треба\_мудрої\_голови!}\}. \quad (20)$$

Сформуємо таблицю символів вхідного повідомлення, у якій кількість рядків має відповідати розміру ключа, тобто M = 6, а кількість рядків таблиці обчислимо за такою формулою: $N = R / M = 30 / 6 = 5$. Якщо символів у останньому рядку таблиці не вистачає, їх потрібно додати випадково. Перетворення одновимірного масиву символів у двовимірний масив $f : \tilde{C} \to \tilde{\tilde{C}}$ виконуємо за такою формулою:

$$\tilde{\tilde{C}} = \left\{ \tilde{C}_i = \left\{ c_{ij} = c_{(j-1)\cdot M+i}, i = \overline{1,M} \right\}, j = \overline{1,N} \right\} = \left| \begin{array}{c|ccccc} i \setminus j & 1 & 2 & 3 & 4 & 5 \\ \hline 1 & Д & а & е & д & о \\ 2 & о & в & б & р & л \\ 3 & \_ & и & а & о & о \\ 4 & б & \_ & \_ & ї & в \\ 5 & у & т & м & \_ & и \\ 6 & л & р & у & г & ! \end{array} \right|. \quad (21)$$

Перетворення двовимірного масиву символів вхідного повідомлення у матрицю числових кодів символів (згідно з таблицею ASCII) $f : \tilde{\tilde{C}} \to \overline{\overline{T}}$ виконуємо за такою формулою:

$$\overline{\overline{T}} = \left| \overline{T}_i = \left| t_{ij} = KSym(c_{ij}), \ j = \overline{1,N} \right|, i = \overline{1,M} \right| = \begin{Vmatrix} 196 & 224 & 229 & 228 & 238 \\ 238 & 226 & 225 & 240 & 235 \\ 95 & 232 & 224 & 238 & 238 \\ 225 & 95 & 95 & 191 & 226 \\ 243 & 242 & 236 & 95 & 232 \\ 235 & 240 & 243 & 227 & 33 \end{Vmatrix}. \quad (22)$$

Для виконання дії переставляння рядків матриці числових кодів символів вхідного повідомлення використовуємо такий матричний вираз:

$$f : \overline{\overline{T}} \to \overline{\overline{T}}' \Rightarrow \overline{\overline{P}} \times \overline{\overline{T}} = \overline{\overline{T}}' = \left| \overline{T}_i' = \left| t_{ij}' = \sum_{k=1}^{N} p_{ik} t_{kj}, \ j = \overline{1,N} \right|, i = \overline{1,M} \right| =$$

$$= \begin{Vmatrix} 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \end{Vmatrix} \times \begin{Vmatrix} 196 & 224 & 229 & 228 & 238 \\ 238 & 226 & 225 & 240 & 235 \\ 95 & 232 & 224 & 238 & 238 \\ 225 & 95 & 95 & 191 & 226 \\ 243 & 242 & 236 & 95 & 232 \\ 235 & 240 & 243 & 227 & 33 \end{Vmatrix} = \begin{Vmatrix} 95 & 232 & 224 & 238 & 238 \\ 243 & 242 & 236 & 95 & 232 \\ 238 & 226 & 225 & 240 & 235 \\ 235 & 240 & 243 & 227 & 33 \\ 196 & 224 & 229 & 228 & 238 \\ 225 & 95 & 95 & 191 & 226 \end{Vmatrix}, \quad (23)$$

внаслідок чого отримуємо матрицю числових кодів символів зашифрованого повідомлення.

Перетворення матриці числових кодів символів зашифрованого повідомлення у двовимірний масив символів (згідно з таблицею ASCII) $f : \overline{\overline{T}}' \to \tilde{\tilde{C}}'$ виконуємо за такою формулою:

$$\tilde{\tilde{C}}' = \left\{ \tilde{C}_i' = \left\{ c_{ij}' = Sym(t_{ij}'), \ i = \overline{1,M} \right\}, j = \overline{1,N} \right\} = \begin{Vmatrix} \_ & и & а & о & о \\ у & т & м & \_ & и \\ о & в & б & р & л \\ л & р & у & г & ! \\ Д & а & е & д & о \\ б & \_ & \_ & ї & в \end{Vmatrix}. \quad (24)$$

Перетворення двовимірного масиву символів зашифрованого повідомлення у одновимірний масив $f : \tilde{\tilde{C}}' \to \tilde{C}'$ виконуємо за такою формулою:

$$\begin{gathered} \tilde{C}' = \left\{ c_{(j-1)\cdot M+i}' = c_{ij}', i = \overline{1,M}; \ j = \overline{1,N} \right\}; M \cdot N = R \Rightarrow \\ \tilde{C}' = \{c_j', j = \overline{1,R}\} = \{\text{\_уолДбитвра\_амбуе\_о\_ргдїоил!ов}\}. \end{gathered} \quad (25)$$

Отже, зашифроване повідомлення має такий вигляд:

_уолДбитвра_амбуе_о_ргдїоил!ов

Зворотний хід. Для виконання зворотного переставляння рядків матриці числових кодів символів зашифрованого повідомлення використаємо такий матричний вираз:

$$f : \overline{\overline{T}}' \to \overline{\overline{T}}'' \Rightarrow \overline{\overline{P}}^{-1} \times \overline{\overline{T}}' = \overline{\overline{T}}'' = \left| \overline{T}_i'' = \left| t_{ij}'' = \sum_{k=1}^{N} p_{ik}^{-1} t_{kj}', \ j = \overline{1,N} \right|, i = \overline{1,M} \right| =$$

$$= \begin{Vmatrix} 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \end{Vmatrix} \times \begin{Vmatrix} 95 & 232 & 224 & 238 & 238 \\ 243 & 242 & 236 & 95 & 232 \\ 238 & 226 & 225 & 240 & 235 \\ 235 & 240 & 243 & 227 & 33 \\ 196 & 224 & 229 & 228 & 238 \\ 225 & 95 & 95 & 191 & 226 \end{Vmatrix} = \begin{Vmatrix} 196 & 238 & 95 & 225 & 243 \\ 235 & 224 & 226 & 232 & 95 \\ 242 & 240 & 229 & 225 & 224 \\ 95 & 236 & 243 & 228 & 240 \\ 238 & 191 & 95 & 227 & 238 \\ 235 & 238 & 226 & 232 & 33 \end{Vmatrix}, \quad (26)$$

внаслідок чого отримуємо матрицю числових кодів символів розшифрованого повідомлення. Тут має виконуватися обов'язкова умова правильності прямого і зворотного ходів, а саме $\overline{\overline{T}}'' = \overline{\overline{T}}$, тобто матриці числових кодів символів вхідного повідомлення та розшифрованого повідомлення мають співпадати.

Перетворення матриці числових кодів символів розшифрованого повідомлення у двовимірний масив символів (згідно з таблицею ASCII) $f : \overline{\overline{T}}'' \to \tilde{\tilde{C}}''$ виконуємо за такою формулою:

$$\tilde{\tilde{C}}'' = \left\{ \tilde{C}_i'' = \left\{ c_{ij}'' = Sym(t_{ij}''), \ j = \overline{1,N} \right\}, i = \overline{1,M} \right\} = \begin{bmatrix} Д & а & е & д & о \\ о & в & б & р & л \\ \_ & и & а & о & о \\ б & \_ & \_ & ї & в \\ у & т & м & \_ & и \\ л & р & у & г & ! \end{bmatrix}. \quad (27)$$

Перетворення двовимірного масиву символів розшифрованого повідомлення у одновимірний масив $f:\tilde{\tilde{C}}''\to\tilde{C}''$ виконуємо за такою формулою:

$$\tilde{C}''=\left\{c''_{(j-1)\cdot M+i}=c''_{ij}, i=\overline{1,M};\ j=\overline{1,N}\right\}; R=M\cdot N\Rightarrow$$
$$\tilde{C}''=\{c''_j, j=\overline{1,R}\}=\{До\_булави\_треба\_мудрої\_голови!\} \quad (28)$$

Роботу алгоритму завершено.

Криптографічна стійкість алгоритму залежить від довжини блоку (розмірності матриці). Так, для блоку довжиною 64 символи (матриця 8×8) можливі $8!\cdot 8!\approx 1{,}6\cdot 10^9$ комбінацій ключа. Для блоку довжиною 256 символів (матриця 16×16) кількість ключів сягає $\approx 4{,}4\cdot 10^{26}$. Вирішення завдання перебору ключів у останньому випадку навіть для сучасних ЕОМ представляє істотну складність.

Отож, наведений алгоритм переставляння рядків матриці реалізується надзвичайно просто, але має два істотні недоліки. По-перше, цей алгоритм допускає розкриття криптограми за допомогою частотного аналізу. По-друге, якщо початковий текст поділити на блоки завдовжки R символів, то криптоаналітику для розкриття алгоритму достатньо направити в систему шифрування R-1 блок тестової інформації, в яких всі однакові символи, за винятком одного.

Висновки

1. Виявлено, що шифри переставляння дають змогу подати вхідне повідомлення у вигляді набору символів або впорядкованої послідовності чисел. Алгоритми маршрутного переставляння дають змогу шифрувати інформацію за допомогою трафарету – поворотних ґраток. Вони є різними як за розмірами і кількістю вирізаних отворів, так і за правилами повороту.

2. З'ясовано, шифр Кардано "квадратні ґратки" є алгоритмом маршрутного переставляння, в якому правило переставлення символів у блоці задається квадратним трафаретом, тобто є зручним для реалізації на папері ручним способом. Встановлено, цей шифр можна використовувати не тільки для шифрування блоку вхідного повідомлення, але й для генерування ключів переставляння.

3. З використанням основних положень матричної алгебри розроблено математичне формулювання алгоритму "квадратні ґратки" для генерування ключів переставляння, а також математичне формулювання алгоритму переставляння рядків матриці вхідного повідомлення, кількість стовпців якої може бути довільною.

Література

1. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов / М.В. Адаменко. – М. : Изд-во "ДМК Прес", 2012. – 256 с.

2. Архипов А.Е. О моделировании некоторых типов случайных последовательностей / А.Е. Архипов // Вестник Киевского политехнического института. – К. : Изд-во Киев. политехн. ин-та, 1988. – Вып. 12. – С. 39-44.

3. Василенко В.С. Матричні криптографічні перетворення в задачах захисту цілісності інформації / В.С. Василенко, О.В. Дубчак, М.Ю. Василенко // Захист інформації : наук.-практ. журнал. – К. : Вид-во НАУ. – 2012. – № 4. – С. 42-50.

4. Герасимчук М.В. Шифрування інформації методом переставляння / М.В. Герасимчук, Ю.І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2011. – Вип. 21.4. – С. 329-336.

5. Ємець В. Сучасна криптографія: основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : Вид-во "БаК", 2003. – 144 с.

6. Жвалюк Юлія. Використання шифру "прямокутні ґратки" для генерування ключів переставляння / Юлія Жвалюк, Юрій Грицюк // Захист інформації : зб. наук.-техн. праць. – К. : Вид-во НАУ. – 2013. – Т. 15, № 2, квітень-червень. – С. 175-184.

7. Захарченко М.В. Розвинення криптології та її місце в сучасному суспільстві : навч. посібн. / М.В. Захарченко, Л.Г. Йона, Ю.В. Щербина, О.В. Онацький. – Одеса : Вид-во ОНАЗ ім. О.С. Попова, 2003. – 180 с.

8. Dharwadker Ashay. A new algorithm for finding Hamiltonian circuits / Ashay Dharwadker. [Electronic resource]. – Mode of access http://www.dharwadker.org/hamilton/

Грыцюк Ю.И., Грыцюк П.Ю. **Математические основы процесса генерации ключей перестановки с использованием шифра Кардано**

Рассматриваются особенности разработки надежного алгоритма для генерации ключей перестановки, работа которого основана на классическом шифре Кардано "квадратные решетки" в его современной математической формулировке, что в целом позволяет генерировать заданную последовательности случайных чисел в заданном диапазоне без повтора.

Установлено, что алгоритм "квадратные решетки", будучи алгоритмом маршрутной перестановки, в котором правило размещения символов в блоке задается квадратным трафаретом, можно использовать не только для шифрования блока входного сообщения, но и для генерации соответствующего множества ключей перестановки. С использованием основных положений матричной алгебры разработана математическая формулировка алгоритма "квадратные решетки" для генерации ключей перестановки, а также математическая формулировка алгоритма перестановки строк матрицы входящего сообщения, количество столбцов которой может быть произвольным.

Ключевые слова: защита информации, шифр Кардано, шифровальные трафареты, алгоритмы перестановки, алгоритмы маршрутной перестановки, алгоритм "прямоугольные и квадратные решетки", генерация ключей перестановки, криптоанализ.

Gryciuk Yu.I., Grytsyuk P.Yu. **Mathematical Foundations of the generation of keys using a permutation cipher Cardano**

The features of the development of a reliable algorithm of key reshuffle generation has been considered. This system is based on a classical cipher Cardano "square lattice", which corresponds to the modern mathematical formulation. In general, the system allows you to generate a sequence of random numbers in a given range without repeat.

It was found that the algorithm "square lattice" is a permutation routing algorithm, in which the sequence of placement of symbols is given by holes of the square stencil. This algorithm can be used to encrypt the block of the incoming message, and for generating a plurality of permutation keys. With the use of the main provisions of matrix algebra, a mathematical formulation of the algorithm "square lattice" for the generation of permutation keys has been developed. Also shown the mathematical formulation of the algorithm permutation of the rows of an incoming message, where the number of columns can be arbitrary.

Keywords: information security, code Cardano, encryption stencils, permutation algorithms, algorithms for routing permutations, "rectangular and square lattice" algorithm, generation of the permutation keys, cryptanalysis.