УДК 004.056.2

ВИКОРИСТАННЯ ШИФРУ "ПРЯМОКУТНІ ҐРАТКИ" ДЛЯ ГЕНЕРУВАННЯ КЛЮЧІВ ПЕРЕСТАВЛЯННЯ

Юлія Жвалюк, Юрій Грицюк

У сучасних складних алгоритмах широкого розповсюдження набули шифри переставляння, котрі використовують певну прямокутну таблицю. Криптографічні перетворення у таких шифрах полягають у тому, що в клітини таблиці символи початкового повідомлення вписують, дотримуючись одного маршруту, а потім – за іншим маршрутом символи виписують з неї. Такі шифри називають шифрами маршрутного переставляння. З'ясовано, що шифр "прямокутні ґратки", будучи алгоритмом маршрутного переставляння, в якому правило розміщення символів у блоці задається прямокутним трафаретом, можна використовувати не тільки для шифрування блоку повідомлення, але й для генерування ключів переставляння. З використанням основних положень матричної алгебри розроблено математичне формулювання шифру "прямокутні ґратки" для генерування ключів переставляння, а також математичне формулювання алгоритму переставляння стовпців матриці вхідного повідомлення, кількість рядків якого може бути довільною.

***Ключові слова**: маршрутне переставляння, шифр "прямокутні ґратки", прямокутні трафарети, генерування випадкових чисел, генерування ключів переставляння.*

Вступ. Суть більшості відомих методів переставляння полягає в поділі початкового тексту на блоки фіксованої довжини і в подальшому переставлянні символів усередині кожного блоку за певним алгоритмом [1, ст. 171; 5, ст. 11]. Такі перетворення призводять до зміни тільки порядку розміщення символів у середині будь-якого блоку вхідного повідомлення. При достатній довжині блоку, в межах якого здійснюється переставляння, і складному неповторному його порядку можна досягти прийнятної криптографічної стійкості алгоритму для простих практичних застосувань [6].

Прикладом простого переставляння є запис блоку початкової інформації в матрицю рядками, а зчитування – стовпцями. Послідовність заповнення рядків матриці та зчитування зашифрованої інформації стовпцями називають ключем переставляння. Відомими алгоритмами переставляння [4] є: шифр Сцітала; магічний квадрат; класичні та табличні шифри переставляння; маршрутне переставляння з використанням трафаретів; переставляння з використання складних геометричних фігур (наприклад, фігур Гамільтона) чи шахових дощок. У кожному із цих алгоритмів ключі переставляння символів виходять за рахунок різниці шляхів запису початкової інформації та шляхів зчитування зашифрованої інформації в межах деякої геометричної фігури [7]. Отримані в такі способи послідовності чисел часто мають випадковий характер.

Різні криптографічні додатки використовують для генерування випадкових чисел особливі алгоритми [2], які реалізуються як програмно, так і апаратно. Ці алгоритми заздалегідь визначені і, як наслідок, генерують послідовність чисел, яка теоретично не може бути статистично випадковою. Водночас, якщо вибрати достатньо хороший алгоритм, то отримана числова послідовність проходитиме більшість тестів на випадковість. Такі числа називають псевдовипадковими числами.

Сучасна інформатика широко використовує псевдовипадкові числа в найрізноманітніших застосуваннях – від методу Монте-Карло та імітаційного моделювання до криптографії. При цьому від якості роботи ГПВЧ безпосередньо залежить і якість отримуваних результатів. Цю обставину підкреслює відомий афоризм Роберта Р. Кавью з ORNL: "генерування випадкових чисел дуже важлива проблема, щоб залишати її на волю випадку".

Названі вище алгоритми переставляння не вимагають використовуваних ГПВЧ як таких, що мають довгий період повторення, послідовні значення чисел мають бути незалежними і т.д. Тут важливо, щоб згенерована послідовність випадкових чисел була у заданому діапазоні – від 1 до R і без повторень [2]. Однак, ніякий детермінований алгоритм не може генерувати повністю випадкову послідовність чисел, він може тільки апроксимувати деякі їх властивості. Як сказав Джон фон Нейман, "всякий, хто має схильність до арифметичних методів отримання випадкових чисел, грішний поза всяких сумнівів".

Мета роботи полягає в тому, щоб показати можливість генерування послідовності випадкових чисел у заданому діапазоні без повторення (у нашому випадку – ключів переставляння) за допомогою шифру "прямокутні ґратки" (ґраток Кардано).

1. Шифр "прямокутні ґратки". Одним із алгоритмів маршрутного переставляння є шифр "прямокутні ґратки" [4, 6]. Для використання цього шифру виготовляють трафарет розміром $2m \times 2n$ клітин, верхній лівий кут якого має позначку (рис. 1). У трафареті вирізають $m \cdot n$ отворів так, що при накладанні його на прямокутну матрицю такого самого розміру у чотири можливих положення його отвори повністю покривають усю площу матриці. Символи вхідного повідомлення послідовно вписують у отвори трафарету переважно рядками в напрямку зліва на право при кожному його накладанні на матрицю майбутньої криптограми.

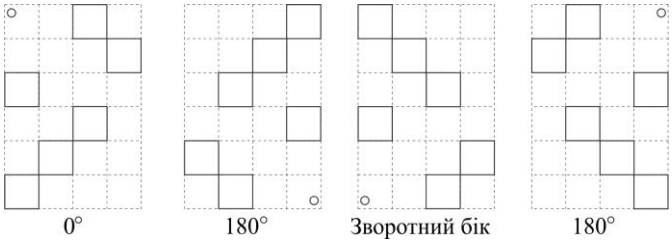

Рис. 1. Трафарет для шифру "прямокутні ґратки"

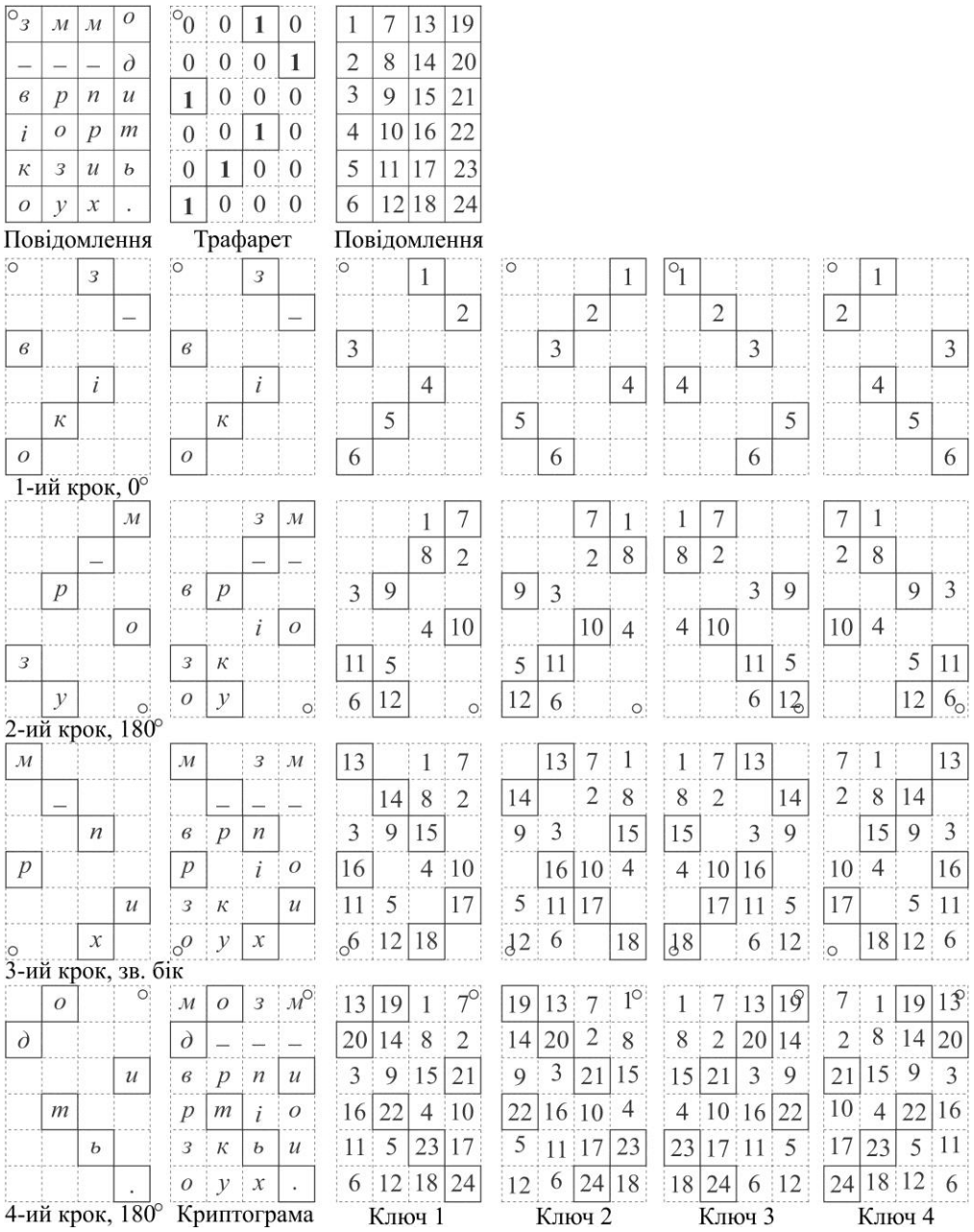

Рис. 2. Шифрування інформації прямокутними ґратками

Пояснимо процес шифрування на конкретному прикладі. Нехай за ключ використовуємо трафарет розміром 6×4 клітини, чотири можливі положення якого показано на рис. 1. Зашифруємо за допомогою нього таке вхідне повідомлення: "*з_віком_розум_приходить.*". Наклавши трафарет на матрицю майбутньої криптограми аналогічного розміру, вписуємо перші шість (за кількістю

отворів) символів вхідного повідомлення. Знявши трафарет, побачимо криптограму, яку наведено на рис. 2 (1-ий крок, 0°). Повернемо трафарет відносно його центру на кут 180°. У отворах з'являться нові, ще не заповнені клітини матриці криптограми. Вписуємо в них наступні шість символів. Потім обертаємо трафарет на зворотний бік відносно горизонтальної осі і за два його аналогічні положення записуємо залишок символів. Після внесення усіх символів у клітини матриці криптограми, отримуємо таке зашифроване повідомлення: *"мозмд___врпирттшозкъиоух."* за умови, якщо зчитувати символи рядками матриці зліва на право. Якщо ж зчитувати символи стовпцями матриці зверху вниз, то отримаємо таку фразу: "*мдврзоо_ртку з_піьхм_иои.*".

Дешифрування криптограми виконаємо у зворотному порядку з зазначенням положень 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.

Можна довести, що кількість можливих трафаретів, тобто кількість ключів шифру "прямокутні ґратки", становить $Q = 4^{mn} = 4^{3\cdot2} = 4096$. Цей шифр призначено для шифрування блочних повідомлень довжиною $R = 4mn = 24$. Кількість всіх можливих переставлянь у повідомленні такої довжини становитиме $(4mn)! = 6.2\cdot10^{23}$, що в багато разів більше за кількість Q. Вирішення завдання перебору ключів у цьому випадку навіть для сучасних ЕОМ представляє істотну складність.

Шифр "прямокутні ґратки" є алгоритмом маршрутного переставляння, в якому правило переставлення символів у блоці задається прямокутним трафаретом, тобто є зручним для реалізації на папері ручним способом. Ключ переставляння зручно задавати у вигляді такого одновимірного масиву:

$$\tilde{K} = \{k_j, j = \overline{1,R}\} = \left\{\overset{1}{k_1}, \overset{2}{k_2}, \ldots, \overset{j}{k_j}, \ldots, \overset{R}{k_R}\right\}, \qquad (1)$$

який показує, що перший символ блоку вхідного повідомлення займає k_1 позицію у матриці криптограми, другий символ переміщається на позицію k_2 і т.д. Наприклад, ключ переставляння (ключ 1), отриманий при реалізації наведеного вище прикладу (рис. 2), при зчитуванні чисел стовпцями матриці зверху вниз має такий вигляд:

$$\tilde{K}_1 = \left\{\overset{1}{13}, \overset{2}{20}, \overset{3}{3}, \overset{4}{16}, \overset{5}{11}, \overset{6}{6}, \overset{7}{19}, \overset{8}{14}, \overset{9}{9}, \overset{10}{22}, \overset{11}{5}, \overset{12}{12}, \overset{13}{1}, \overset{14}{8}, \overset{15}{15}, \overset{16}{4}, \overset{17}{23}, \overset{18}{18}, \overset{19}{7}, \overset{20}{2}, \overset{21}{21}, \overset{22}{10}, \overset{23}{17}, \overset{24}{24}\right\},$$

а ключа 4 – такий вигляд:

$$\tilde{K}_4 = \left\{\overset{1}{7}, \overset{2}{2}, \overset{3}{21}, \overset{4}{10}, \overset{5}{17}, \overset{6}{24}, \overset{7}{1}, \overset{8}{8}, \overset{9}{15}, \overset{10}{4}, \overset{11}{23}, \overset{12}{18}, \overset{13}{19}, \overset{14}{14}, \overset{15}{9}, \overset{16}{22}, \overset{17}{5}, \overset{18}{12}, \overset{19}{13}, \overset{20}{20}, \overset{21}{3}, \overset{22}{16}, \overset{23}{11}, \overset{24}{6}\right\}.$$

Зрозуміло, якщо зчитувати числа рядками матриці зліва на право, то відповідні ключі переставляння будуть мати зовсім інший вигляд.

Отже, шифр "прямокутні 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 шифру "прямокутні ґратки" для генерування ключів переставляння, а також математичне формулювання алгоритму переставляння стовпців матриці вхідного повідомлення, кількість рядків якого може бути довільним. Для цього використаємо інструментарій матричної алгебри [3].

2. Математичне формулювання шифру "прямокутні ґратки". Вхідні елементи шифру "прямокутні ґратки" при M=6 і N=4 подано на рис. 3.

з	_	*в*	*і*	*к*	*о*
м	_	*р*	*о*	*з*	*у*
м	_	*п*	*р*	*и*	*х*
о	*д*	*и*	*т*	*ь*	.

а)

0	0	**1**	0
0	0	0	**1**
1	0	0	0
0	0	**1**	0
0	**1**	0	0
1	0	0	0

б)

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24

в)

Рис. 3. Вхідні елементи шифру "прямокутні ґратки":
а) – вхідне повідомлення;
б) – прямокутний трафарет з отворами;
в) – матричне подання трафарету

З рисунку видно, що вхідне повідомлення (рис. 3, а) складається з R=$M\cdot N$=6·4=24 символів, тобто чисел – у нашому випадку. Подамо їх у вигляді такого одновимірного масиву:

$$\tilde{C} = \left\{c_j = j,\ j = \overline{1,R}\right\} \Rightarrow \tilde{C}^{(l)} = \left\{c^{(l)}_{(l-1)\cdot N + j},\ j = \overline{1,N}\right\}, l = \overline{1,L} =$$
$$= \left\{\underbrace{1,\ 2,\ 3,\ 4,\ 5,\ 6,}_{l=1\ блок}\ \underbrace{7,\ 8,\ 9,\ 10,\ 11,\ 12,}_{l=2\ блок}\ \underbrace{13,\ 14,\ 15,\ 16,\ 17,\ 18,}_{l=3\ блок}\ \underbrace{19,\ 20,\ 21,\ 22,\ 23,\ 24}_{l=4\ блок}\right\}, \quad (2)$$

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

Прямокутний трафарет у початковому його положенні, тобто при 0°, має таке матричне подання:

$$\bar{\bar{G}}^{(1)} = \left|\bar{G}^{(1)}_i = \left|g^{(1)}_{ij} = random(0,1),\ j = \overline{1,N}\right|, i = \overline{1,M}\right| = \left\|\begin{matrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \end{matrix}\right\|. \quad (3)$$

Матрицю інвертування рядків матриці подання трафарету $\bar{\bar{G}}^{(l)},\ l = \overline{1,L}$ сформуємо за допомогою такого виразу:

$$\bar{\bar{I}}^{\,\mathrm{r}} = \left|\bar{I}^{\,\mathrm{r}}_i = \left|i^{\mathrm{r}}_{ij} = \begin{cases} 1, \text{ якщо } i = M - j + 1; \\ 0 - \text{інакше}, \end{cases} j = \overline{1,M}\right|, i = \overline{1,M}\right| = \left\|\begin{matrix} 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 \end{matrix}\right\|. \quad (4)$$

Матрицю інвертування стовпців матриці подання трафарету $\bar{\bar{G}}^{(l)},\ l = \overline{1,L}$ сформуємо за допомогою такого виразу:

$$\bar{\bar{I}}^{\,\mathrm{s}} = \left|\bar{I}^{\,\mathrm{s}}_i = \left|i^{\mathrm{s}}_{ij} = \begin{cases} 1, \text{ якщо } i = N - j + 1; \\ 0 - \text{інакше}, \end{cases} j = \overline{1,N}\right|, i = \overline{1,N}\right| = \left\|\begin{matrix} 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \end{matrix}\right\|. \quad (5)$$

Початкова матриця криптограми має такий вигляд:

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

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

$$f : \{\tilde{C}^{(1)}, \bar{\bar{G}}^{(1)}\} \mapsto \bar{\bar{S}}^{(1)} \Rightarrow \bar{\bar{S}}^{(1)} = \left|\bar{S}^{(1)}_i = \left|s^{(1)}_{ij} = F(c^{(1)}_{0\cdot N + j}, g^{(1)}_{ij}),\ j = \overline{1,N}\right|, i = \overline{1,M}\right| =$$
$$= \{1,\ 2,\ 3,\ 4,\ 5,\ 6\} \mapsto \left\|\begin{matrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \end{matrix}\right\| = \left\|\begin{matrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{2} \\ \mathbf{3} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{4} & 0 \\ 0 & \mathbf{5} & 0 & 0 \\ \mathbf{6} & 0 & 0 & 0 \end{matrix}\right\|, \quad (7)$$

де $F()$ – функція, яка програмно реалізує дії зазначеної процедури. Матриця криптограми на 1-му кроці має такий вигляд:

$$\overline{\overline{T}}^{(0)} + \overline{\overline{S}}^{(1)} = \overline{\overline{T}}^{(1)} = \left|\overline{T}_i^{(1)} = \left|t_{ij}^{(1)} = t_{ij}^{(0)} + s_{ij}^{(1)},\ j = \overline{1,N}\right|, i = \overline{1,M}\right| =$$

$$= \begin{Vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{Vmatrix} + \begin{Vmatrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{2} \\ \mathbf{3} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{4} & 0 \\ 0 & \mathbf{5} & 0 & 0 \\ \mathbf{6} & 0 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{2} \\ \mathbf{3} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{4} & 0 \\ 0 & \mathbf{5} & 0 & 0 \\ \mathbf{6} & 0 & 0 & 0 \end{Vmatrix}. \tag{8}$$

***Крок* 2**. Процедуру повертання трафарету на кут 180° реалізуємо, виходячи з попереднього його стану, за допомогою такого матричного виразу:

$$\overline{\overline{I}}^{\,\mathrm{r}} \times \overline{\overline{G}}^{(1)} \times \overline{\overline{I}}^{\,\mathrm{s}} = \overline{\overline{G}}^{(2)} = \left|\overline{G}_i^{(2)} = \left|g_{ij}^{(2)} = \sum_{l=1}^{N} i_{lj}^{\mathrm{s}} \cdot \sum_{k=1}^{M} i_{ik}^{\mathrm{r}} \cdot g_{kl}^{(1)},\ j = \overline{1,N}\right|, i = \overline{1,M}\right| =$$

$$= \begin{Vmatrix} 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 \end{Vmatrix} \times \begin{Vmatrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \end{Vmatrix} \times \begin{Vmatrix} 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \end{Vmatrix}. \tag{9}$$

Процедура вписування символів (чисел) l=2-го блоку вхідного повідомлення через отвори трафарету при 180° у клітини матриці криптограми має такий вигляд:

$$f : \{\tilde{C}^{(2)}, \overline{\overline{G}}^{(2)}\} \mapsto \overline{\overline{T}}^{(2)} \Rightarrow \overline{\overline{T}}^{(2)} = \left|\overline{T}_i^{(2)} = \left|t_{ij}^{(2)} = F(c_{1 \cdot N + j}^{(2)}, g_{ij}^{(2)}),\ j = \overline{1,N}\right|, i = \overline{1,N}\right| =$$

$$= \{7, 8, 9, 10, 11, 12\} \mapsto \begin{Vmatrix} 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & 0 & \mathbf{7} \\ 0 & 0 & \mathbf{8} & 0 \\ 0 & \mathbf{9} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{10} \\ \mathbf{11} & 0 & 0 & 0 \\ 0 & \mathbf{12} & 0 & 0 \end{Vmatrix}. \tag{10}$$

Матриця криптограми на 2-му кроці має такий вигляд:

$$\overline{\overline{T}}^{(1)} + \overline{\overline{S}}^{(2)} = \overline{\overline{T}}^{(2)} = \left|\overline{T}_i^{(2)} = \left|t_{ij}^{(2)} = t_{ij}^{(1)} + s_{ij}^{(2)},\ j = \overline{1,N}\right|, i = \overline{1,N}\right| =$$

$$= \begin{Vmatrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{2} \\ \mathbf{3} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{4} & 0 \\ 0 & \mathbf{5} & 0 & 0 \\ \mathbf{6} & 0 & 0 & 0 \end{Vmatrix} + \begin{Vmatrix} 0 & 0 & 0 & \mathbf{7} \\ 0 & 0 & \mathbf{8} & 0 \\ 0 & \mathbf{9} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{10} \\ \mathbf{11} & 0 & 0 & 0 \\ 0 & \mathbf{12} & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & \mathbf{1} & \mathbf{7} \\ 0 & 0 & \mathbf{8} & \mathbf{2} \\ \mathbf{3} & \mathbf{9} & 0 & 0 \\ 0 & 0 & \mathbf{4} & \mathbf{10} \\ \mathbf{11} & \mathbf{5} & 0 & 0 \\ \mathbf{6} & \mathbf{12} & 0 & 0 \end{Vmatrix}. \tag{11}$$

***Крок* 3**. Процедуру обертання трафарету на зворотний бік відносно його горизонтальної осі реалізуємо, виходячи з початкового його стану при 0°, за допомогою такого матричного виразу:

$$\overline{\overline{I}}^{\,\mathrm{r}} \times \overline{\overline{G}}^{(1)} = \overline{\overline{G}}^{(3)} = \left|\overline{G}_i^{(3)} = \left|g_{ij}^{(3)} = \sum_{k=1}^{N} i_{ik}^{\mathrm{r}} \cdot g_{kj}^{(1)},\ j = \overline{1,N}\right|, i = \overline{1,M}\right| =$$

$$= \begin{Vmatrix} 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 \end{Vmatrix} \times \begin{Vmatrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \end{Vmatrix}. \tag{12}$$

Процедура вписування символів (чисел) l=3-го блоку вхідного повідомлення через отвори трафарету зі зворотного боку у клітини матриці криптограми має такий вигляд:

$$f: F(\tilde{C}^{(3)}, \bar{\bar{G}}^{(3)}) \mapsto \bar{\bar{S}}^{(3)} \Rightarrow \bar{\bar{S}}^{(3)} = \left\| \bar{S}_i^{(3)} = \left| s_{ij}^{(3)} = F(c_{2\cdot N+j}^{(3)}, g_{ij}^{(3)}),\ j = \overline{1,N} \right|, i = \overline{1,M} \right| =$$

$$= \{13, 14, 15, 16, 17, 18\} \mapsto \begin{Vmatrix} \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \end{Vmatrix} = \begin{Vmatrix} \mathbf{13} & 0 & 0 & 0 \\ 0 & \mathbf{14} & 0 & 0 \\ 0 & 0 & \mathbf{15} & 0 \\ \mathbf{16} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{17} \\ 0 & 0 & \mathbf{18} & 0 \end{Vmatrix}. \tag{13}$$

Матриця криптограми на 3-му кроці має такий вигляд:

$$\bar{\bar{T}}^{(2)} + \bar{\bar{S}}^{(3)} = \bar{\bar{T}}^{(3)} = \left\| \bar{T}_i^{(3)} = \left| t_{ij}^{(3)} = t_{ij}^{(2)} + s_{ij}^{(3)},\ j = \overline{1,N} \right|, i = \overline{1,M} \right| =$$

$$= \begin{Vmatrix} 0 & 0 & \mathbf{1} & \mathbf{7} \\ 0 & 0 & \mathbf{8} & \mathbf{2} \\ \mathbf{3} & \mathbf{9} & 0 & 0 \\ 0 & 0 & \mathbf{4} & \mathbf{10} \\ \mathbf{11} & \mathbf{5} & 0 & 0 \\ \mathbf{6} & \mathbf{12} & 0 & 0 \end{Vmatrix} + \begin{Vmatrix} \mathbf{13} & 0 & 0 & 0 \\ 0 & \mathbf{14} & 0 & 0 \\ 0 & 0 & \mathbf{15} & 0 \\ \mathbf{16} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{17} \\ 0 & 0 & \mathbf{18} & 0 \end{Vmatrix} = \begin{Vmatrix} \mathbf{13} & 0 & \mathbf{1} & \mathbf{7} \\ 0 & \mathbf{14} & \mathbf{8} & \mathbf{2} \\ \mathbf{3} & \mathbf{9} & \mathbf{15} & 0 \\ \mathbf{16} & 0 & \mathbf{4} & \mathbf{10} \\ \mathbf{11} & \mathbf{5} & 0 & \mathbf{17} \\ \mathbf{6} & \mathbf{12} & \mathbf{13} & 0 \end{Vmatrix}. \tag{14}$$

***Крок* 4**. Процедуру повертання трафарету на кут 180° реалізуємо, виходячи з початкового його стану при 0°, за допомогою такого матричного виразу:

$$\bar{\bar{G}}^{(1)} \times \bar{\bar{I}}^{s} = \bar{\bar{G}}^{(4)} = \left\| \bar{G}_i^{(4)} = \left| g_{ij}^{(4)} = \sum_{k=1}^{N} g_{ik}^{(1)} \cdot i_{kj}^{s},\ j = \overline{1,N} \right|, i = \overline{1,M} \right| =$$

$$= \begin{Vmatrix} 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \end{Vmatrix} \times \begin{Vmatrix} 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \end{Vmatrix}. \tag{15}$$

Процедура вписування символів (чисел) l=4-го блоку вхідного повідомлення через отвори трафарету при 180° у клітини матриці криптограми має такий вигляд:

$$f: \{\tilde{C}^{(4)}, \bar{\bar{G}}^{(4)}\} \mapsto \bar{\bar{S}}^{(4)} \Rightarrow \bar{\bar{S}}^{(4)} = \left\| \bar{S}_i^{(4)} = \left| s_{ij}^{(4)} = F(c_{3\cdot N+j}^{(4)}, g_{ij}^{(4)}),\ j = \overline{1,N} \right|, i = \overline{1,M} \right| =$$

$$= \{19, 20, 21, 22, 23, 24\} \mapsto \begin{Vmatrix} 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} \end{Vmatrix} = \begin{Vmatrix} 0 & \mathbf{19} & 0 & 0 \\ \mathbf{20} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{21} \\ 0 & \mathbf{22} & 0 & 0 \\ 0 & 0 & \mathbf{23} & 0 \\ 0 & 0 & 0 & \mathbf{24} \end{Vmatrix}. \tag{16}$$

Матриця криптограми на 4-му кроці має такий вигляд:

$$\bar{\bar{T}}^{(3)} + \bar{\bar{S}}^{(4)} = \bar{\bar{T}}^{(4)} = \left\| \bar{T}_i^{(4)} = \left| t_{ij}^{(4)} = t_{ij}^{(3)} + s_{ij}^{(4)},\ j = \overline{1,N} \right|, i = \overline{1,M} \right| =$$

$$= \begin{Vmatrix} \mathbf{13} & 0 & \mathbf{1} & \mathbf{7} \\ 0 & \mathbf{14} & \mathbf{8} & \mathbf{2} \\ \mathbf{3} & \mathbf{9} & \mathbf{15} & 0 \\ \mathbf{16} & 0 & \mathbf{4} & \mathbf{10} \\ \mathbf{11} & \mathbf{5} & 0 & \mathbf{17} \\ \mathbf{6} & \mathbf{12} & \mathbf{13} & 0 \end{Vmatrix} + \begin{Vmatrix} 0 & \mathbf{19} & 0 & 0 \\ \mathbf{20} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{21} \\ 0 & \mathbf{22} & 0 & 0 \\ 0 & 0 & \mathbf{23} & 0 \\ 0 & 0 & 0 & \mathbf{24} \end{Vmatrix} = \begin{Vmatrix} \mathbf{13} & \mathbf{19} & \mathbf{1} & \mathbf{7} \\ \mathbf{20} & \mathbf{14} & \mathbf{8} & \mathbf{2} \\ \mathbf{3} & \mathbf{9} & \mathbf{15} & \mathbf{21} \\ \mathbf{16} & \mathbf{22} & \mathbf{4} & \mathbf{10} \\ \mathbf{11} & \mathbf{5} & \mathbf{23} & \mathbf{17} \\ \mathbf{6} & \mathbf{12} & \mathbf{13} & \mathbf{24} \end{Vmatrix}. \tag{17}$$

Перетворення елементів матриці криптограми у елементи одновимірного масиву при зчитуванні символів (чисел) стовпцями матриці зверху вниз виконуємо за такою формулою:

$$f:\overline{\overline{T}}^{(4)}\to\tilde{K}\Rightarrow\tilde{K}=\left\{k_{(j-1)\cdot M+i}=t_{ij}^{(4)},i=\overline{1,M};\ j=\overline{1,N}\right\}\Rightarrow$$
$$\tilde{K}=\{k_j,\ j=\overline{1,R}\}=\{13,20,3,16,11,6,19,14,9,\quad(18)$$
$$22,5,12,1,8,15,4,23,18,7,2,21,10,17,24\},$$

де $\tilde{K}$ – ключ переставляння рядка символів. Кількість комбінацій отриманих ключів при зчитуванні чисел з матриці криптограми залежить від її розміру. Так, для матриці розміром 6×4 можливі 6!·4!≈17280 комбінацій ключа, а для матриці розміром 8×8 їх кількість становить $8!\cdot 8!\approx 1{,}6\cdot 10^9$.

3. Математичне формулювання алгоритму переставляння. Для розуміння подальших дій ключ переставляння подамо у дещо меншому вигляді, а саме:

$$\tilde{K}=\{k_j,\ j=\overline{1,N}\}=\{3,5,2,1,4\}:\ N=5.\qquad(19)$$

Кодувальну матрицю, тобто матрицю переставляння стовпців матриці вхідного коду під час виконання прямого ходу сформуємо за допомогою такого виразу:

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

$i\setminus k_j$	**3**	**5**	**2**	**1**	**4**
1	0	0	0	**1**	0
2	0	0	**1**	0	0
3	**1**	0	0	0	0
4	0	0	0	0	**1**
5	0	**1**	0	0	0

. (20)

Декодувальну матрицю, тобто матрицю переставляння стовпців матриці перетворених кодів під час виконання зворотного ходу сформуємо за допомогою такого виразу:

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

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

. (21)

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

$$\tilde{C}=\{c_j,\ j=\overline{1,R}\}=\{\textit{До\_булави\_треба\_мудрої\_голови}!\}.\qquad(22)$$

Сформуємо таблицю символів вхідного повідомлення, у якій кількість стовпців має відповідати розміру ключа, тобто $N=5$, а кількість рядків таблиці обчислимо за такою формулою: $M=R/N=30/5=6$. 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:

$$\tilde{\tilde{C}}=\left\{\tilde{C}_i=\left\{c_{ij}=c_{i\cdot N+j},\ j=\overline{1,N}\right\},i=\overline{0,M-1}\right\}=$$

$i\setminus j$	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*	!

. (23)

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

$$\overline{\overline{T}} = \left|\overline{T_i} = \left|t_{ij} = KSym(c_{ij}),\ j = \overline{1,N}\right|, i = \overline{0,M-1}\right| = \begin{Vmatrix} 196 & 238 & 95 & 225 & 243 \\ 235 & 224 & 226 & 232 & 95 \\ 242 & 240 & 229 & 225 & 224 \\ 95 & 236 & 243 & 228 & 240 \\ 238 & 191 & 95 & 227 & 238 \\ 235 & 238 & 226 & 232 & 33 \end{Vmatrix}. \quad (24)$$

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

$$f : \overline{\overline{T}} \to \overline{\overline{T}}' \Rightarrow \overline{\overline{T}} \times \overline{\overline{P}} = \overline{\overline{T}}' = \left|\overline{T_i}' = \left|t'_{ij} = \sum_{k=1}^{N} t_{ik} p_{kj},\ j = \overline{1,N}\right|, i = \overline{0,M-1}\right| =$$

$$= \begin{Vmatrix} 196 & 238 & 95 & 225 & 243 \\ 235 & 224 & 226 & 232 & 95 \\ 242 & 240 & 229 & 225 & 224 \\ 95 & 236 & 243 & 228 & 240 \\ 238 & 191 & 95 & 227 & 238 \\ 235 & 238 & 226 & 232 & 33 \end{Vmatrix} \times \begin{Vmatrix} 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 95 & 243 & 238 & 196 & 225 \\ 226 & 95 & 224 & 235 & 232 \\ 229 & 224 & 240 & 242 & 225 \\ 243 & 240 & 236 & 95 & 228 \\ 95 & 238 & 191 & 238 & 227 \\ 226 & 33 & 238 & 235 & 232 \end{Vmatrix}, \quad (25)$$

внаслідок чого отримуємо матрицю числових кодів символів зашифрованого повідомлення.

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

$$\tilde{\tilde{C}}' = \left\{\tilde{C}'_i = \left\{c'_{ij} = Sym(t'_{ij}),\ j = \overline{1,N}\right\}, i = \overline{0,M-1}\right\} = \begin{Vmatrix} \_ & у & о & Д & б \\ в & \_ & а & л & и \\ е & а & р & т & б \\ у & р & м & \_ & д \\ \_ & о & ї & о & г \\ в & ! & о & л & и \end{Vmatrix}. \quad (26)$$

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

$$\tilde{C}' = \left\{c'_{i\cdot N+j} = c'_{ij},\ j = \overline{1,N};\ i = \overline{0,M-1}\right\} : M \cdot N = R \Rightarrow$$

$$\tilde{C}' = \{c'_j,\ j = \overline{1,R}\} = \{\_\ уоДбв\ \_\ алиеартбурм\ \_\ д\ \_\ оїогв!оли\}. \quad (27)$$

Отже, зашифроване повідомлення має такий вигляд: *_уоДбв_алиеартбурм_д_оїогв!оли*

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

$$f : \overline{\overline{T}}' \to \overline{\overline{T}}'' \Rightarrow \overline{\overline{T}}' \times \overline{\overline{P}}^{-1} = \overline{\overline{T}}'' = \left|\overline{T_i}'' = \left|t''_{ij} = \sum_{k=1}^{N} t'_{ik} p_{kj}^{-1},\ j = \overline{1,N}\right|, i = \overline{0,M-1}\right| =$$

$$= \begin{Vmatrix} 95 & 243 & 238 & 196 & 225 \\ 226 & 95 & 224 & 235 & 232 \\ 229 & 224 & 240 & 242 & 225 \\ 243 & 240 & 236 & 95 & 228 \\ 95 & 238 & 191 & 238 & 227 \\ 226 & 33 & 238 & 235 & 232 \end{Vmatrix} \times \begin{Vmatrix} 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 \end{Vmatrix} = \begin{Vmatrix} 196 & 238 & 95 & 225 & 243 \\ 235 & 224 & 226 & 232 & 95 \\ 242 & 240 & 229 & 225 & 224 \\ 95 & 236 & 243 & 228 & 240 \\ 238 & 191 & 95 & 227 & 238 \\ 235 & 238 & 226 & 232 & 33 \end{Vmatrix}, \quad (28)$$

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 та розшифрованого повідомлень мають між собою співпадати.

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

$$\tilde{\tilde{C}}'=\left\{\tilde{C}_i''=\left\{c_{ij}''=Sym(t_{ij}''),\ j=\overline{1,N}\right\},i=\overline{0,M-1}\right\}=\begin{bmatrix} Д & о & \_ & б & у \\ л & а & в & и & \_ \\ т & р & е & б & а \\ \_ & м & у & д & р \\ о & ї & \_ & г & о \\ л & о & в & и & ! \end{bmatrix}. \quad (29)$$

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

$$\tilde{C}''=\left\{c''_{i\cdot N+j}=c_{ij}'',\ j=\overline{1,N};\ i=\overline{0,M-1}\right\}\Rightarrow$$

$$\tilde{C}''=\{c_j'',\ j=\overline{1,K}\}=\{До\_булави\_треба\_мудрої\_голови!\}. \quad (30)$$

Роботу алгоритму завершено.

Отож, наведений алгоритм переставляння стовпців 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. З'ясовано, шифр "прямокутні ґратки" є алгоритмом маршрутного переставляння, в якому правило переставлення символів у блоці задається прямокутним трафаретом, тобто є зручним для реалізації на папері ручним способом. Встановлено, цей шифр можна використовувати не тільки для шифрування блоку повідомлення, але й для генерування ключів переставляння.

2. З використанням основних положень матричної алгебри розроблено математичне формулювання шифру "прямокутні ґратки" для генерування ключів переставляння, а також математичне формулювання алгоритму переставляння стовпців матриці вхідного повідомлення, кількість рядків якого може бути довільним.

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]. 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.

[6]. Рябко Б.Я. Криптографические методы защиты информации : учебн. пособ. [для студ. ВУЗов] / Б.Я. Рябко, Ф.Н. Фионов. – М. : Изд-во "Горячая линия–Телеком", 2005. – 229 с.

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

REFERENCES

[1]. Adamenko M.V. Osnovy klassicheskoy kriptologii: sekrety shifrov i kodov / M.V. Adamenko, M. : Izd-vo "DMK Pres", 2012, 256 p.

[2]. Arkhipov A.E. O modelirovanii nekotorykh tipov sluchaynykh posledovatelnostey / A.E. Arkhipov // Vestnik Kievskogo politekhnicheskogo instituta, K. : Izd-vo Kiev. politekhn. in-ta, 1988, Vyp. 12, pp. 39-44.

[3]. Vasylenko V.S. Matrychni kryptografichni peretvorennya v zadachakh zakhystu tsilisnosti informatsiyi / V.S. Vasylenko, O.V. Dubchak, M.Yu. Vasylenko // Zakhyst informatsiyi : nauk.-prakt. zhurnal. – K. : Vyd-vo NAU, 2012, № 4, pp. 42-50.

[4]. Gerasymchuk M.V. SHyfruvannya informatsiyi metodom perestavlyannya / M.V. Gerasymchuk, YU.I. Grytsyuk // Naukovyy visnyk NLTU Ukrayiny : zb. nauk.-tekhn. Prats, Lviv : RVV NLTU Ukrayiny, 2011, Vyp. 21.4, pp. 329-336.

[5]. Zakharchenko M.V. Rozvynennya kryptologiyi ta yiyi mistse v suchasnomu suspilstvi : navch. posibn. /

M.V. Zakharchenko, L.G. Yona, Yu.V. SCHerbyna, O.V. Onatskyy, Odesa : Vyd-vo ONAZ im. O.S. Popova, 2003, 180 p.
[6]. Ryabko B.YA. Kriptograficheskie metody zaschity informatsii : uchebn. posob. [dlya stud. VUZov] / B.YA. Ryabko, F.N. Fionov, M. : Izd-vo "Goryachaya liniya–Telekom", 2005, 229 p.
[7]. Dharwadker Ashay. A new algorithm for finding Hamiltonian circuits / Ashay Dharwadker. [Electronic resource]. – Mode of access http://www.dharwadker.org/hamilton/

ИСПОЛЬЗОВАНИЕ ШИФРА "ПРЯМОУГОЛЬНЫЕ РЕШЕТКИ" ДЛЯ ГЕНЕРИРОВАНИЯ КЛЮЧЕЙ ПЕРЕСТАНОВКИ

В современных сложных алгоритмах широкое распространение получили шифры перестановки, использующие определенную прямоугольную таблицу. Криптографические преобразование в таком шифре заключаются в том, что в клетки таблицы символы исходного сообщения вписывают, придерживаясь одного маршрута, а затем по другому маршруту символы выписывают из нее. Такие шифры получили название шифров маршрутной перестановки. Выяснено, что шифр "прямоугольные решетки", являясь алгоритмом маршрутной перестановки, в котором правило размещения символов в блоке задается прямоугольным трафаретом, можно использовать не только для шифрования блока сообщения, но и для генерирования ключей перестановки. С использованием основных положений матричной алгебры разработана математическая формулировка шифра "прямоугольные решетки" для генерирования ключей перестановки, а также математическая формулировка алгоритма перестановки столбцов матрицы исходного сообщения, количество строк которого может быть произвольным.
Ключові слова: маршрутная перестановка, шифр "прямоугольные решетки", прямоугольные трафареты, генерирование случайных чисел, генерирование ключей перестановки.

USE OF "RECTANGULAR GRID" CODE FOR PERMUTATION KEY GENERATION

In the complicated algorithms of today are widely used rearranging ciphers that use a rectangular table. The essence of cryptographic transformation in such ciphers are that the symbols of the original message are entered in the cells of the table following a route, and then – the symbols are write out in a different route from it. Such codes are called ciphers of route rearranging. It was determined that "rectangular grid" code is route permutation algorithm, in which a rule placing symbols in the block is given by a rectangular stencil, can be used not only to encrypt the message block, but also for permutation key generation. Using core provisions of the matrix al-gebra the mathematical formulation of the "rectangular grid" cipher for permutation key generation, as well as mathematical formulation of the permutation algorithm of matrix columns of the original message, the number of rows which can be random, were developed.
Keywords: route permutation, "rectangular grid" code, rectangular stencils, random number generation, permutation key generation.

Жвалюк Юлія Андріївна, курсант 5-го курсу, кафедра управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності.
E-mail: zhvaliuk.yula@gmail.com.
Жвалюк Юлия Андреевна, курсант 5-го курса, кафедра управления информационной безопасностью, Львовский государственный университет безопасности жизнедеятельности.
Zhvalyuk Yuliya Andriyivna, cadet 5-year student, Department of information security management, Lviv state university of life safety.

Грицюк Юрій Іванович, доктор технічних наук, професор, завідувач кафедра управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності.
E-mail: yura.grycyuk@yandex.ru.
Грицюк Юрий Иванович, доктор технических наук, профессор, заведующий кафедрой управления информационной безопасностью, Львовский государственный университет безопасности жизнедеятельности.
Grytsyuk Yuriy Ivanovych, doctor of technical sciences, professor, Head of department of information security management, Lviv state university of life safety.