УДК 004.056.5:681.3.05

ОСОБЛИВОСТІ ГЕНЕРУВАННЯ $G_p(\lambda)$-МАТРИЦЬ ФІБОНАЧЧІ – КЛЮЧІВ ДЛЯ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Ю. І. Грицюк, П. Ю. Грицюк

Національний університет "Львівська політехніка"

E-mail: yura.grycyuk@yandex.ru, pgrytsiuk1992@gmail.com

Розглянуто особливості ефективного генерування $G_p(\lambda)$-матриць Фібоначчі, які можна використати як ключі (де)шифрування для багатораундової матричної криптографічної системи перетворення даних. Розроблено процедуру генерування їх множини, яка за відомими значеннями степеня матриці (n) та $p(\lambda)$-чисел Фібоначчі дає змогу отримувати відповідну множину ключів (де)шифрування даних, розширювати ключі для кожного раунду, що забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й зручність під час передавання каналами зв'язку.

Ключові слова: *захист інформації, шифрування/дешифрування інформації, числа Фібоначчі, $G_p(\lambda)$-матриці Фібоначчі, криптографічна система, матричні афінні перетворення, багатораундова матрична криптографічна система.*

FEATURES OF THE GENERATION OF FIBONACCI $G_p(\lambda)$-MATRICES – KEYS FOR THE IMPLEMENTATION OF CRYPTOGRAPHIC CONVERSION

Yu. I. Gryciuk, P. Yu. Grytsyuk

National University "Lviv Polytechnic", Ukrainian National Forestry University

The features of effective generation of the Fibonacci $G_p(\lambda)$-matrix are considered. Those matrices are used as decryption/encryption keys for the multi-round matrix crypto-graphic system of the information transformation. It is found that in multi-round affinity matrix cryptosystem the main problem is to generate a plurality of the conventional and in-verse keys-matrices of the information encryption/decryption that are to be integers. The procedure for generating a plurality of Fibonacci $G_p(\lambda)$-matrix is developed. This procedure relies on the known degree of matrix values (n) and $p(\lambda)$-numbers of Fibonacci and allows us set the appropriate information on the encryption/decryption keys, implement expansion keys for each round. This provides an efficient way of their formation and storage and creates the convenience of transmitting channels.

Keywords: *information security, encryption/decryption information, Fibonacci numbers, Fibonacci $G_p(\lambda)$-matrix, cryptographic system, matrix Affine transformation, matrix multi-rounds cryptographic system.*

У праці [1] розглянуто особливості побудови надійної криптографічної системи захисту інформації, яка поєднує матричні афінні перетворення, багатораундові дії з різними ключами, а також перестановні алгоритми, що загалом істотно підвищує її криптостійкість до різних атак зловмисників. Зокрема, у відомій матричній Афінній криптосистемі [2] традиційно використовують такі матричні вирази для шифрування та дешифрування інформації:

$$\overline{\overline{K}} = \overline{\overline{A}} \underset{m}{\otimes} \overline{\overline{T}} \underset{m}{\oplus} \overline{B}\,;\; \overline{\overline{T}} = \overline{\overline{A}}' \underset{m}{\otimes} \overline{\overline{K}} \underset{m}{\oplus} \overline{B}'\,, \quad (1)$$

де m – кількість символів алфавіту; $\overline{\overline{A}} = [a_{ij},\, i,\, j = \overline{1,n}]$ – матриця (ключ) шифрування, елементи якої – спеціально підібрані цілі числа з діапазону $1 \le a_{ij} < m$, а

© Ю. І. Грицюк, П. Ю. Грицюк, 2016

також НСД(a, m) = 1; $a = \det(\overline{\overline{A}}) \bmod m$ – визначник матриці $\overline{\overline{A}}$ за модулем m; $\overline{B} = [b_i, i = \overline{1,n}]$ – стовпець (ключ) коригування, елементами якого є цілі числа з діапазону $1 \le b_i < m$; $\overline{\overline{T}} = [\overline{T}_j = [t_{ij} = KodSym(s_{(i-1)\cdot p+j}),\ i = \overline{1,n}],\ j = \overline{1,p} : p \ge n]$ – матриця, елементами якої є числові коди символів вхідного повідомлення $\overline{S} = \{s_j, j = \overline{1, n \cdot p}\}$; $\overline{\overline{K}} = [k_{ij}, j, i = \overline{1,n}]$ – матриця, елементами якої є числові коди символів зашифрованого повідомлення.

Однак під час матричних афінних перетворень (1) виникає декілька проблем. Насамперед це стосується генерування множини матриць $\overline{\overline{A}}$ – ключів шифрування, а також генерування стовпців $\overline{B}$ – ключів додаткового коригування вже зашифрованого повідомлення. Якщо ж використовувати багатораундову матричну Афінну криптосистему [1], то на r-му раунді криптографічних перетворень (кількість яких може бути від 4 до 16 чи 24) з'являється потреба у різних матричних ключах, тобто необхідно розширити ключі для кожного раунду. Окрім цього, оскільки розміри ($n \times n$) матриць $\overline{\overline{A}}^{(r)}$ можуть бути різними (мінімальний 32×32, нормальний 128×128 чи 256×256, надмірний 1048×1048 та більше), а кількість раундів шифрування великою (R = 16, 32, 48, 64, …), то постає питання не тільки у їх зберіганні, але й передачі цих ключів каналами зв'язку з кожним повідомленням. А як відомо [3, 4], розмір зашифрованого повідомлення не має істотно відрізнятися від вхідної інформації. Водночас передані з повідомленням ключі шифрування не повинні викликати в криптоаналітиків підозри у цілісності зашифрованого повідомлення.

Отже, основне завдання багатораундової матричної Афінної криптосистеми – генерування множини звичайних і обернених матриць – ключів (де)шифрування інформації, елементами яких мають бути цілі числа, розширенні ключів для кожного раунду, а також у ефективній формі їх зберігання та передавання каналами зв'язку. Для його вирішення пропонуємо використовувати $G_p(\lambda)$-матриці, елементами яких є $p(\lambda)$-числа Фібоначчі [5, 6].

Досліджували матричні ключі (де)шифрування та їх розширення для багатораундової криптографічної системи перетворення даних, а також методи і засоби генерування $G_p(\lambda)$-матриць – ключів (де)шифрування та розширення їхньої множини для кожного раунду криптографічного перетворення даних, елементами яких є $p(\lambda)$-числа Фібоначчі.

Ставили за мету розробити методи і засоби генерування $G_p(\lambda)$-матриць Фібоначчі – ключів (де)шифрування для багатораундової криптографічної системи перетворення даних і розширення їхньої множини, що дасть змогу не тільки ефективно їх утворювати, але й зберігати та передавати каналами зв'язку. Для її реалізації потрібно виявити основні особливості побудови матриць на основі $p(\lambda)$-чисел Фібоначчі, які значно полегшать процес їх генерування та розширення потрібної множини для кожного раунду криптографічних перетворень; реалізувати багатораундову криптосистему на основі $G_p(\lambda)$-матриць Фібоначчі, яка суттєво підвищить криптостійкість алгоритму шифрування; зробити відповідні теоретичні висновки та надати рекомендації для практичного використання.

Особливості побудови $G(\lambda)$-матриць на основі $p(\lambda)$-чисел Фібоначчі. У праці [5] вказано, що трикутник Паскаля n-го степеня є джерелом утворення числових рядів, які викликають інтерес для реалізації криптографічних перетворень. Якщо у початковому трикутнику зсунути біноміальні коефіцієнти на p позицій (p = 1, 2, 3, …) вправо відносно попереднього рядка, то отримаємо p-ий "деформований" трикутник, який прийнято називати p-трикутником Паскаля. Підсумовуючи значення біноміальних коефіцієнтів, матимемо щоразу новий числовий ряд, який можна задати таким рекурентним співвідношенням:

$$\begin{cases} pF_p^j = 1;\ j = \overline{0, p}; \\ pF_p^{n+1} = pF_p^n + pF_p^{n-p}, \end{cases} \quad \forall\, n \ge p+1; \quad p = 0, 1, 2, 3, \ldots; \quad n = 1, 2, 3, 4, \ldots . \tag{2}$$

Числові ряди, які можна задати співвідношенням (2), винайдено ще в 1977 р. [7] і названо їх *p*-числами Фібоначчі (табл. 1).

Таблиця 1. Найпоширеніші *p*-числа Фібоначчі для різних значень *n*

$p \backslash n$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
0	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
1	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946
2	1	1	1	2	3	4	6	9	13	19	28	41	60	88	129	189	277	406	595	872	1278
3	1	1	1	1	2	3	4	5	7	10	14	19	26	36	50	69	95	131	181	250	345
4	1	1	1	1	1	2	3	4	5	6	8	11	15	20	26	34	45	60	80	106	140
5	1	1	1	1	1	1	2	3	4	5	6	7	9	12	16	21	27	34	43	55	71

Поняття про *G*(λ)-матрицю Фібоначчі. Як відомо [8], існує теорія матриць спеціального типу [9], однією з яких є *G*(λ)-матриця [6]. Найпростішою *G*(λ)-матрицею є квадратна розміром 2×2 вигляду

$$\overline{\overline{G}}(\lambda) = \begin{bmatrix} \lambda & 1 \\ 1 & 0 \end{bmatrix}, \det \overline{\overline{G}}(\lambda) = -1, \tag{3}$$

де λ – будь-яке ціле число. Зрозуміло, що *G*(λ)-матриці безпосередньо стосуються чисел Фібоначчі, позаяк після піднесення такої матриці до *n*-го степеня утворюються такі послідовності звичайних і обернених матриць, а також їхні визначники.

Послідовність $\overline{\overline{G}}^n(2)$-матриць Фібоначчі:

n	0	1	2	3	4	5	6	7	8	9
$\overline{\overline{G}}^n(2)$	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}2&1\\1&0\end{bmatrix}$	$\begin{bmatrix}5&2\\2&1\end{bmatrix}$	$\begin{bmatrix}12&5\\5&2\end{bmatrix}$	$\begin{bmatrix}29&12\\12&5\end{bmatrix}$	$\begin{bmatrix}70&29\\29&12\end{bmatrix}$	$\begin{bmatrix}169&70\\70&29\end{bmatrix}$	$\begin{bmatrix}408&169\\169&70\end{bmatrix}$	$\begin{bmatrix}985&408\\408&169\end{bmatrix}$	$\begin{bmatrix}2378&985\\985&408\end{bmatrix}$
$\det\overline{\overline{G}}^n(2)$	1	-1	1	-1	1	-1	1	-1	1	-1
$\overline{\overline{G}}^{-n}(2)$	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&-1\end{bmatrix}$	$\begin{bmatrix}1&-1\\-1&2\end{bmatrix}$	$\begin{bmatrix}-1&2\\2&-3\end{bmatrix}$	$\begin{bmatrix}2&-3\\-3&5\end{bmatrix}$	$\begin{bmatrix}-3&5\\5&-8\end{bmatrix}$	$\begin{bmatrix}5&-8\\-8&13\end{bmatrix}$	$\begin{bmatrix}-8&13\\13&-21\end{bmatrix}$	$\begin{bmatrix}13&-21\\-21&34\end{bmatrix}$	$\begin{bmatrix}-21&34\\34&-55\end{bmatrix}$
$\det\overline{\overline{G}}^{-n}(2)$	1	-1	1	-1	1	-1	1	-1	1	-1

Послідовність $\overline{\overline{G}}^n(5)$-матриць Фібоначчі:

n	0	1	2	3	4	5	6	7
$\overline{\overline{G}}^n(5)$	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}5&1\\1&0\end{bmatrix}$	$\begin{bmatrix}26&5\\5&1\end{bmatrix}$	$\begin{bmatrix}135&26\\26&5\end{bmatrix}$	$\begin{bmatrix}701&135\\135&26\end{bmatrix}$	$\begin{bmatrix}3640&701\\701&135\end{bmatrix}$	$\begin{bmatrix}18901&3640\\3640&701\end{bmatrix}$	$\begin{bmatrix}98145&18901\\18901&3640\end{bmatrix}$
$\det\overline{\overline{G}}^n(5)$	1	-1	1	-1	1	-1	1	-1
$\overline{\overline{G}}^{-n}(5)$	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&-5\end{bmatrix}$	$\begin{bmatrix}1&-5\\-5&26\end{bmatrix}$	$\begin{bmatrix}-5&26\\26&-135\end{bmatrix}$	$\begin{bmatrix}26&-135\\-135&701\end{bmatrix}$	$\begin{bmatrix}-135&701\\701&-3640\end{bmatrix}$	$\begin{bmatrix}701&-3640\\-3640&18901\end{bmatrix}$	$\begin{bmatrix}-3640&18901\\18901&-98145\end{bmatrix}$
$\det\overline{\overline{G}}^{-n}(5)$	1	-1	1	-1	1	-1	1	-1

Розглянувши уважно звичайні матриці, бачимо, що їхніми елементами є деякі числа Фібоначчі, утворені з коефіцієнтом λ (назвемо їх λ-числами Фібоначчі). Згенерувати λ-числа Фібоначчі можна за допомогою такого рекурентного співвідношення:

$$\lambda F_1^{n+1} = \lambda \cdot \lambda F_1^n + \lambda F_1^{n-1} \text{ при } n > 1,\ \lambda F_1^0 = \lambda F_1^1 = 1 . \tag{4}$$

Для коефіцієнта λ = 1 одержуємо звичайну послідовність чисел Фібоначчі (табл. 2). Для інших значень λ числа послідовності (4) мають зовсім інші значення, тобто маємо справу з т. зв. λ-числами Фібоначчі. Водночас для певної *G*(λ)-

матриці, піднесеної до n-го степеня, на головній діагоналі з трьох сусідніх λ-чисел Фібоначчі знаходяться найбільше та найменше з них, а на побічній – середнє. Загалом $G(\lambda)$-матриці [6], піднесені до n-го степеня, можна математично записати так:

$$\bar{\bar{G}}^n(\lambda) = \begin{bmatrix} \lambda F^{n+1} & \lambda F^n \\ \lambda F^n & \lambda F^{n-1} \end{bmatrix}, \quad \det \bar{\bar{G}}^n(\lambda) = (-1)^n , \tag{5}$$

де λF^{n-1}, λF^n, λF^{n+1} – сусідні λ-числа Фібоначчі. Окрім цього, у прямій та оберненій матрицях знаходяться одні і ті самі числа, тільки в оберненій матриці поміняні місцями числа на її головній діагоналі та мають протилежний знак на побічній. Задавати $G(\lambda)$-матриці n-го степеня можна за рекурентним співвідношенням

$$\bar{\bar{G}}^{n+1}(\lambda) = \lambda \cdot \bar{\bar{G}}^n(\lambda) + \bar{\bar{G}}^{n-1}(\lambda), \quad n = 2, 3, 4, \ldots , \tag{6}$$

або матричним виразом [10]

$$\bar{\bar{G}}^{n+1}(\lambda) = \bar{\bar{G}}^n(\lambda) \times \bar{\bar{G}}^1(\lambda), \quad n = 2, 3, 4, \ldots , \tag{7}$$

який придатніший для використання, ніж співвідношення (6), оскільки має узагальнену структуру розрахунку.

Таблиця 2. Послідовність λ-чисел Фібоначчі для деяких значень коефіцієнта λ

λ\\n	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
1	1	1	1	2	3	5	8	13	21	34	55	89	144	233
2	1	1	2	5	12	29	70	169	408	985	2378	5741	13860	33461
3	1	1	3	10	33	109	360	1189	3927	12970	42837	141481	467280	1543321
4	1	1	4	17	72	305	1292	5473	23184	98209	416020	1762289	7465176	31622993
5	1	1	5	26	135	701	3640	18901	98145	509626	2646275	13741001	71351280	370497401

Узагальнена $G_p(\lambda)$-матриця Фібоначчі. Спробуємо використати ідею побудови $G(\lambda)$-матриці з λ-чисел Фібоначчі, щоб отримати узагальнені $G_p(\lambda)$-матриці Фібоначчі. Як і в праці [11], введемо квадратну матрицю спеціального типу, яку назвемо $G_p(\lambda)$-матрицею:

$$\bar{\bar{G}}_p(\lambda) = \left[\begin{array}{c|cccccc} \lambda & \mathbf{1} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \mathbf{1} \\ \hline \mathbf{1} & 0 & 0 & 0 & \cdots & 0 & 0 \end{array}\right], \det \bar{\bar{G}}_p(\lambda) = \pm 1, \ p = 0, 1, 2, 3, \ldots . \tag{8}$$

Особливістю її будови є те, що вона має розміри $(p+1)\times(p+1)$, містить одиничну матрицю розміром $p\times p$, обмежену останнім рядком типу **1** 0 0 … 0 0 і першим стовпцем типу **λ** 0 0 … 0 **1**. Якщо $p = 0$, то $G_p(\lambda)$-матриця виглядає як $\bar{\bar{G}}_0(\lambda) = [\lambda]$, а для p = 1, 2, 3 і 4 відповідні матриці такі:

$$\bar{\bar{G}}_1(\lambda) = \left[\begin{array}{c|c} \lambda & 1 \\ \hline 1 & 0 \end{array}\right], \quad \bar{\bar{G}}_2(\lambda) = \left[\begin{array}{c|cc} \lambda & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & 0 & 0 \end{array}\right], \quad \bar{\bar{G}}_3(\lambda) = \left[\begin{array}{c|ccc} \lambda & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 \end{array}\right],$$

$$\det \bar{\bar{G}}_1(\lambda) = -1; \quad \det \bar{\bar{G}}_2(\lambda) = 1; \quad \det \bar{\bar{G}}_3(\lambda) = -1;$$

$$
\overline{\overline{G}}_4(\lambda) = \left[\begin{array}{c|cccc} \lambda & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & 0 \end{array}\right] \tag{9}
$$

$$
\det \overline{\overline{G}}_4(\lambda) = 1.
$$

Зрозуміло, що $G_p(\lambda)$-матриці безпосередньо стосуються p-чисел Фібоначчі. Якщо піднести $G_p(\lambda)$-матрицю до n-го степеня, для різних значень p отримаємо різні набори матриць з різними p-числами Фібоначчі, утворені з коефіцієнтом λ (назвемо їх $p(\lambda)$-числами Фібоначчі). Наприклад, для p = 2 та λ = 3 одержимо набір $\overline{\overline{G}}{}_2^n(3)$-матриць (див. нижче), елементами яких є 2(3)-числа Фібоначчі.

Послідовність $\overline{\overline{G}}{}_2^n(3)$-матриць Фібоначчі

n	0	1	2	3	4	5	6
$\overline{\overline{G}}{}_2^n(3)$	1 0 0	3 1 0	9 3 1	28 9 3	87 28 9	270 87 28	838 270 87
	0 1 0	0 0 1	1 0 0	3 1 0	9 3 1	28 9 3	87 28 9
	0 0 1	1 0 0	3 1 0	9 3 1	28 9 3	87 28 9	270 87 28
$\det \overline{\overline{G}}{}_2^n(3)$	1	1	1	1	1	1	1
$\overline{\overline{G}}{}_2^{-n}(3)$	1 0 0	0 0 1	0 1 0	1 0 -3	-0 -3 1	-3 1 9	1 9 -6
	0 1 0	1 0 -3	0 -3 1	-3 1 9	1 9 -6	9 -6 -26	-6 -26 27
	0 0 1	0 1 0	1 0 -3	-0 -3 1	-3 1 9	1 9 -6	9 -6 -26
$\det \overline{\overline{G}}{}_2^{-n}(3)$	1	1	1	1	1	1	1

та її продовження

n	7	8	9	10	11
$\overline{\overline{G}}{}_2^n(3)$	2601 838 270	8073 2601 838	25057 8073 2601	77772 25057 8073	241389 77772 25057
	270 87 28	838 270 87	2601 838 270	8073 2601 838	25057 8073 2601
	838 270 87	2601 838 270	8073 2601 838	25057 8073 2601	77772 25057 8073
$\det \overline{\overline{G}}{}_2^n(3)$	1	1	1	1	1
$\overline{\overline{G}}{}_2^{-n}(3)$	9 -6 -26	-6 -26 27	-26 27 72	27 72 -107	72 -107 -189
	-26 27 72	27 72 -107	72 -107 -189	-107 -189 393	-189 393 460
	-6 -26 27	-26 27 72	27 72 -107	72 -107 -189	-107 -189 393
$\det \overline{\overline{G}}{}_2^{-n}(3)$	1	1	1	1	1

Загалом $\overline{\overline{G}}{}_2^n(\lambda)$-матриці можна записати так:

$$
\overline{\overline{G}}{}_2^n(\lambda) = \begin{bmatrix} \lambda F_2^{n+1} & \lambda F_2^{n} & \lambda F_2^{n-1} \\ \lambda F_2^{n-1} & \lambda F_2^{n-2} & \lambda F_2^{n-3} \\ \lambda F_2^{n} & \lambda F_2^{n-1} & \lambda F_2^{n-2} \end{bmatrix}, \quad \det \overline{\overline{G}}{}_2^n(\lambda) = (-1)^{2n}, \quad n = 2, 3, 4, \ldots, \tag{10}
$$

де λF_2^{n-1}, λF_2^{n}, λF_2^{n+1} – 2(λ)-числа Фібоначчі. Задавати $\overline{\overline{G}}{}_2^n(\lambda)$-матриці, піднесені до n-го степеня, доцільно за допомогою матричного виразу

$$
\overline{\overline{G}}{}_2^{n+1}(\lambda) = \overline{\overline{G}}{}_2^n(\lambda) \times \overline{\overline{G}}{}_2^1(\lambda), \quad n = 2, 3, 4, \ldots, \tag{11}
$$

основний недолік якого в тому, що для отримання $\overline{\overline{G}}{}_2^{n+1}(\lambda)$-матриці потрібно мати $\overline{\overline{G}}{}_2^n(\lambda)$-матрицю, а отже, усю послідовність матриць від першого до (n–1)-го степеня.

Для розуміння основних закономірностей побудови $\overline{\overline{G}}{}_p^n(\lambda)$-матриць розглянемо ще один приклад, коли p = 3 та λ = 5. Тоді набір $\overline{\overline{G}}{}_3^n(5)$-матриць (див.

нижче), піднесених до n-го степеня, має такі самі особливості побудови, як і $\bar{\bar{G}}_2^n(5)$-матриці, однак, елементами цих матриць вже є 3(5)-числа Фібоначчі. Звернемо увагу тільки на те, що матричний вираз (11) придатний також, щоб задавати $\bar{\bar{G}}_3^n(5)$-матрицю, піднесену до n-го степеня.

Послідовність $\bar{\bar{G}}_3^n(5)$-матриць Фібоначчі

$$\begin{array}{ccccccc}
n & 0 & 1 & 2 & 3 & 4 & 5 \\
\bar{\bar{G}}_3^n(5) & \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} & \begin{bmatrix}5&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix} & \begin{bmatrix}25&5&1&0\\0&0&0&1\\1&0&0&0\\5&1&0&0\end{bmatrix} & \begin{bmatrix}125&25&5&1\\1&0&0&0\\5&1&0&0\\25&5&1&0\end{bmatrix} & \begin{bmatrix}626&125&25&5\\5&1&0&0\\25&5&1&0\\125&25&5&1\end{bmatrix} & \begin{bmatrix}3135&626&125&25\\25&5&1&0\\125&25&5&1\\626&125&25&5\end{bmatrix} \\
\det\bar{\bar{G}}_3^n(5) & 1 & -1 & 1 & -1 & 1 & -1 \\
\bar{\bar{G}}_3^{-n}(5) & \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} & \begin{bmatrix}0&0&0&1\\1&0&0&-5\\0&1&0&0\\0&0&1&0\end{bmatrix} & \begin{bmatrix}0&0&1&0\\0&0&-5&1\\1&0&0&-5\\0&1&0&0\end{bmatrix} & \begin{bmatrix}0&1&0&0\\0&-5&1&0\\0&0&-5&1\\1&0&0&-5\end{bmatrix} & \begin{bmatrix}1&0&0&-5\\-5&1&0&25\\0&-5&1&0\\0&0&-5&1\end{bmatrix} & \begin{bmatrix}0&0&-5&1\\1&0&25&-10\\-5&1&0&25\\0&-5&1&0\end{bmatrix} \\
\det\bar{\bar{G}}_3^{-n}(5) & 1 & -1 & 1 & -1 & 1 & -1
\end{array}$$

та її продовження

$$\begin{array}{ccccc}
n & 6 & 7 & 8 & 9 \\
\bar{\bar{G}}_3^n(5) & \begin{bmatrix}15700&3135&626&125\\125&25&5&1\\626&125&25&5\\3135&626&125&25\end{bmatrix} & \begin{bmatrix}78625&15700&3135&626\\626&125&25&5\\3135&626&125&25\\15700&3135&626&125\end{bmatrix} & \begin{bmatrix}393751&78625&15700&3135\\3135&626&125&25\\15700&3135&626&125\\78625&15700&3135&626\end{bmatrix} & \begin{bmatrix}1971890&393751&78625&15700\\15700&3135&626&125\\78625&15700&3135&626\\393751&78625&15700&3135\end{bmatrix} \\
\det\bar{\bar{G}}_3^n(5) & 1 & -1 & 1 & -1 \\
\bar{\bar{G}}_3^{-n}(5) & \begin{bmatrix}0&-5&1&0\\0&25&-10&1\\1&0&25&-10\\-5&1&0&25\end{bmatrix} & \begin{bmatrix}-5&1&0&25\\25&-10&1&-125\\0&25&-10&1\\1&0&25&-10\end{bmatrix} & \begin{bmatrix}1&0&25&-10\\-10&1&-125&75\\25&-10&1&-125\\0&25&-10&1\end{bmatrix} & \begin{bmatrix}0&25&-10&1\\1&-125&75&-15\\-10&1&-125&75\\25&-10&1&-125\end{bmatrix} \\
\det\bar{\bar{G}}_3^{-n}(5) & -1 & -1 & 1 & -1
\end{array}$$

Отже, задавати $\bar{\bar{G}}_p^n(\lambda)$-матриці Фібоначчі, піднесені до n-го степеня, доцільно за таким узагальненим виразом:

$$\bar{\bar{G}}_p^{n+1}(\lambda) = \bar{\bar{G}}_p^n(\lambda) \times \bar{\bar{G}}_p^1(\lambda), \quad p = 1, 2, 3, \ldots; \; n = \pm 2, \pm 3, \pm 4, \ldots . \tag{12}$$

Варто зауважити, що λ-числа Фібоначчі можна згенерувати за рекурентним співвідношенням (4), однак, як згенерувати $p(\lambda)$-числами Фібоначчі, так і невідомо. Тому аналогічно, як і в рекурентному співвідношенні (2), призначеному для генерування p-чисел Фібоначчі, спробуємо також записати рекурентне співвідношення для генерування $p(\lambda)$-числа Фібоначчі для різних значень p, λ і n:

$$\begin{cases} \lambda F_p^j = \lambda^j, \; j = \overline{0, p}; \\ \lambda F_p^{n+1} = \lambda \cdot \lambda F_p^n + \lambda F_p^{n-p}, \end{cases} \quad \forall n \geq p+1; \quad p = 0, 1, 2, 3, \ldots; \quad n = 1, 2, 3, 4, \ldots . \tag{13}$$

У табл. 3 наведено деякі найуживаніші $p(\lambda)$-числа Фібоначчі для різних значень n. З таблиці видно, якщо ж задати $\lambda = 1$, то отримаємо найпоширеніші p-числа Фібоначчі для різних значень n (див. табл. 1). При $\lambda = 3$ та $p = 2$ маємо 2(3)-числа Фібоначчі, які було використано вище під час генерування послідовності $\bar{\bar{G}}_2^n(3)$-матриць Фібоначчі. Якщо ж задати $\lambda = 5$ та $p = 3$, то отримаємо 3(5)-числа Фібоначчі, які застосували вище під час генерування послідовності $\bar{\bar{G}}_3^n(5)$-матриць Фібоначчі.

Таблиця 3. Найпоширеніші *p*(λ)-числа Фібоначчі для різних значень *n*

*p**n*	0	1	2	3	4	5	6	7	8	9	10	11	12
λ = 3													
0	1	4	16	64	256	1024	4096	16384	65536	262144	1048576	4194304	16777216
1	1	3	10	33	109	360	1189	3927	12970	42837	141481	467280	1543321
2	1	3	9	28	87	270	838	2601	8073	25057	77772	241389	749224
3	1	3	9	27	82	249	756	2295	6967	21150	64206	194913	591706
4	1	3	9	27	81	244	735	2214	6669	20088	60508	182259	548991
5	1	3	9	27	81	243	730	2193	6588	19791	59454	178605	536545
λ = 5													
0	1	6	36	216	1296	7776	46656	279936	1679616	10077696	60466176	362797056	2176782336
1	1	5	26	135	701	3640	18901	98145	509626	2646275	13741001	71351280	370497401
2	1	5	25	126	635	3200	16126	81265	409525	2063751	10400020	52409625	264111876
3	1	5	25	125	626	3135	15700	78625	393751	1971890	9875150	49454375	247665626
4	1	5	25	125	625	3126	15635	78200	391125	1956250	9784376	48937515	244765775
5	1	5	25	125	625	3125	15626	78135	390700	1953625	9768750	48846875	244250001

Процедура генерування $\bar{\bar{G}}_p^n(\lambda)$-матриць Фібоначчі. Загалом процедуру генерування $\bar{\bar{G}}_p^n(\lambda)$-матриці, піднесеної до *n*-го степеня, елементами якої будуть *p*(λ)-числа Фібоначчі за конкретних значень λ, можна записати так:

$$\bar{\bar{D}}_p^n = \left[d_{ij,p}^n = n-(p+1-i)-(j-1),\ i,j=\overline{1,p+1} \right];$$

$$\bar{\bar{M}}_p^k = \left[m_{ij,p}^k = \begin{cases} 1, \text{ якщо } (i+k-j)\operatorname{mod}(p+1)=0; \\ 0 - \text{в іншому випадку}, \end{cases} \quad i,j=\overline{1,p+1} \right];$$

$$\bar{\bar{U}}_p^n = \left[u_{ij,p}^n = \sum_{l=1}^{p+1} m_{il,p}^{-n} \cdot d_{lj,p}^n,\ i,j=\overline{1,p+1} \right]; \qquad (14)$$

$$\bar{\bar{G}}_p^n(\lambda) = \left[g_{ij,p}^n(\lambda) = \lambda F_p^{u_{ij,p}^n},\ i,j=\overline{1,p+1} \right], \quad p=1,2,3,\ldots;\ \ n=2,3,4,\ldots;$$

$$k=-1,-2,\ldots,-p.$$

Тут основною особливістю є те, що для отримання $\bar{\bar{G}}_p^{n+1}(\lambda)$-матриці не потрібна $\bar{\bar{G}}_p^n(\lambda)$-матриця, тобто зникає необхідність і в будь-яких попередніх матрицях. Потрібні тільки наперед згенеровані *p*(λ)-числа Фібоначчі для конкретного значення λ за різних значень *n* (див. табл. 3).

Продемонструємо особливості використання процедури генерування $\bar{\bar{G}}_p^n(\lambda)$-матриці Фібоначчі, піднесеної до *n*-го степеня, значеннями елементів якої будуть *p*(λ)-числа Фібоначчі, на конкретному прикладі за таких вхідних даних: λ = 3, *p* = 4, *n* = 10 та *k* = 2. Тоді, згідно з табл. 3, матимемо справу з такими 4(3)-числа Фібоначчі: 1, 3, 9, 27, 81, 244, 735, 2214, 6669, 20088, 60508, 182259, 548991, 1653642, 4981014. Після математичної процедури (14) отримаємо такі результати розрахунку:

$\overline{\overline{D}}_4^{10}$, $k = 2$; $\overline{\overline{M}}_4^{2}$; $\overline{\overline{U}}_4^{10}$; $\overline{\overline{G}}_4^{10}(3)$; $\overline{\overline{G}}_4^{-10}(3)$

10	1	2	3	4	5																					
1	6	5	4	3	2	0	0	0	**1**	0	9	8	7	6	5	20088	6669	2214	735	244	-6	1	0	-0	9
2	7	6	5	4	3	0	0	0	0	**1**	10	9	8	7	6	60508	20088	6669	2214	735	27	-6	1	0	-27
3	8	7	6	5	4	**1**	0	0	0	0	6	5	4	3	2	735	244	81	27	9	-27	9	-6	1	-0
4	9	8	7	6	5	0	**1**	0	0	0	7	6	5	4	3	2214	735	244	81	27	-0	0	9	-6	1
5	10	9	8	7	6	0	0	**1**	0	0	8	7	6	5	4	6669	2214	735	244	81	1	0	-0	9	-6

$\det \overline{\overline{G}}_4^{10}(3) =$ 1 $\qquad \det \overline{\overline{G}}_4^{-10}(3) =$ 1

Використання $\overline{\overline{G}}_p^n(\lambda)$-матриць Фібоначчі для шифрування інформації. Виявляється [12], що $\overline{\overline{G}}_p^n(\lambda)$-матриці Фібоначчі (12) також можна успішно застосовувати для реалізації матричної криптографічної системи, як і Афінну криптосистему. Суть методу шифрування, який ґрунтується на цих матрицях, полягає у поданні початкового повідомлення у вигляді матриці $\overline{\overline{T}}$ розміром $(p+1)\times q$ і реалізації таких матричних дій:

– шифрування $$\overline{\overline{G}}_p^n(\lambda)\underset{m}{\otimes}\overline{\overline{T}}\underset{m}{\oplus}\overline{B}=\overline{\overline{K}}\,; \tag{15}$$

– дешифрування $$\overline{\overline{G}}_p^{-n}(\lambda)\underset{m}{\otimes}(\overline{\overline{K}}-\overline{B})=\overline{\overline{T}}\,, \tag{16}$$

де q – кількість стовпців матриці $\overline{\overline{T}}$, $q \geq 1$; p, n, λ – додаткові ключі шифрування.

Продемонструємо особливості застосування описаного методу шифрування інформації з використанням $\overline{\overline{G}}_p^n(\lambda)$-матриць Фібоначчі на конкретному прикладі. Тут для p = 3, n = 5 та λ = 5 взято $\overline{\overline{G}}_3^5(5)$-матрицю, елементами якої є 3(5)-числа Фібоначчі.

Шифрування вхідного повідомлення:

$\overline{\overline{G}}_3^5(5)$ × $\overline{\overline{T}}$ + $\overline{B}$ = $(\overline{\overline{G}}_3^5(5)\times\overline{\overline{T}}+\overline{B})\bmod 256=\overline{\overline{K}}$

3135	626	125	25		219	185	202	183	204	213	97		232		60	246	183	22	123	20	217
25	5	1	0	×	93	64	155	59	103	136	151	+	175	=	146	247	222	174	233	99	185
125	25	5	1		175	247	110	249	75	63	158		108		61	32	60	65	192	142	124
626	125	25	5		98	76	229	218	50	158	222		186		170	247	148	154	42	57	107

Дешифрування зашифрованої інформації:

$\overline{\overline{G}}_3^{-5}(5)$ × ($\overline{\overline{K}}$ – $\overline{B}$) = $(\overline{\overline{G}}_3^{-5}(5)\times(\overline{\overline{K}}-\overline{B}))\bmod 256=\overline{\overline{T}}$

0	0	-5	1		60	246	183	22	123	20	217		192		219	185	202	183	204	213	97
1	0	25	-10	×	146	247	222	174	233	99	185	–	57	=	93	64	155	59	103	136	151
-5	1	0	25		61	32	60	65	192	142	124		59		175	247	110	249	75	63	158
0	-5	1	0		170	247	148	154	42	57	107		187		98	76	229	218	50	158	222

Використання $\overline{\overline{G}}_p^n(\lambda)$-матриць Фібоначчі для багатораундової криптосистеми. За матричним виразом (15) можна шифрувати повідомлення $\overline{\overline{T}}$, застосовуючи R-раундову процедуру шифрування і кожного разу з новими ключами, тобто $\overline{\overline{G}}_p^n(\lambda)$-матрицями Фібоначчі за різних значень n. Водночас дешифрування інформації за виразом (16) також повторюватиметься R разів. У цьому випадку узагальнені вирази для прямого та зворотного криптографічного перетворення даних матимуть вигляд

$$\overline{\overline{K}}=\underbrace{\overline{\overline{G}}_p^{R+k}(\lambda)\underset{m}{\otimes}\ldots\left(\overline{\overline{G}}_p^{2+k}(\lambda)\underset{m}{\otimes}\left(\overline{\overline{G}}_p^{1+k}(\lambda)\underset{m}{\otimes}\overline{\overline{T}}\underset{m}{\oplus}\overline{B}_1\right)\underset{m}{\oplus}\overline{B}_2\right)\ldots\underset{m}{\oplus}\overline{B}_R}_{R\text{ раундів}}\,; \tag{17}$$

$$\bar{\bar{T}} = \underbrace{\bar{\bar{G}}_p^{-(1+k)}(\lambda) \underset{m}{\otimes} \left(...\bar{\bar{G}}_p^{-(R-1+k)}(\lambda) \underset{m}{\otimes} \left(\bar{\bar{G}}_p^{-(R+k)}(\lambda) \underset{m}{\otimes} \left(\bar{\bar{K}} - \bar{B}_R \right) - \bar{B}_{R-1} \right) ... - \bar{B}_1 \right)}_{R \text{ раундів}}, \quad (18)$$

де k – коефіцієнт уточнення степеня піднесення $\bar{\bar{G}}_p^n(\lambda)$-матриці Фібоначчі; $n = r + k$ – додатковий ключ шифрування.

Матрична криптосистема (17) і (18) разом з матричними перестановними алгоритмами [1] утворюють багатораундову матричну перестановну криптосистему перетворення даних, яку загалом подамо у вигляді такого багатораундового (де)шифрування інформації:

$$\bar{\bar{K}}_{\text{рс}}^{\text{п}} = \underbrace{\bar{\bar{G}}_p^{R+k}(\lambda) \underset{m}{\otimes} ... \left(\bar{\bar{G}}_p^{2+k}(\lambda) \underset{m}{\otimes} \left(\bar{\bar{G}}_p^{1+k}(\lambda) \underset{m}{\otimes} \left(\bar{\bar{P}}_{\text{р}}^{\text{п}} \times \bar{\bar{T}} \times \bar{\bar{P}}_{\text{с}}^{\text{п}} \right) \underset{m}{\oplus} \bar{B}_1 \right) \underset{m}{\oplus} \bar{B}_2 \right) ... \underset{m}{\oplus} \bar{B}_R}_{R \text{ раундів}}; \quad (19)$$

$$\bar{\bar{T}}_{\text{ср}}^{\text{п}} = \bar{\bar{P}}_{\text{р}}'^{\text{п}} \times$$

$$\times \left(\underbrace{\bar{\bar{G}}_p^{-(1+k)}(\lambda) \underset{m}{\otimes} \left(...\bar{\bar{G}}_p^{-(R-1+k)}(\lambda) \underset{m}{\otimes} \left(\bar{\bar{G}}_p^{-(R+k)}(\lambda) \underset{m}{\otimes} \left(\bar{\bar{K}}_{\text{рс}}^{\text{п}} - \bar{B}_R \right) - \bar{B}_{R-1} \right) ... - \bar{B}_1 \right)}_{R \text{ раундів}} \times \bar{\bar{P}}_{\text{с}}'^{\text{п}} \right), \quad (20)$$

де $\bar{\bar{P}}_{\text{р}}^{\text{п}}$, $\bar{\bar{P}}_{\text{р}}'^{\text{п}}$ та $\bar{\bar{P}}_{\text{с}}^{\text{п}}$, $\bar{\bar{P}}_{\text{с}}'^{\text{п}}$ – квадратні перестановні матриці відповідно рядків і стовпців вхідної матриці $\bar{\bar{T}}$ для прямого і зворотного ходів відповідно.

Можливі ще й такі матричні вирази для реалізації цієї процедури:

$$\bar{\bar{K}}_{\text{рс}}^{\text{п}} = \bar{\bar{P}}_{\text{р}}^{\text{п}} \times \underbrace{\bar{\bar{G}}_p^{R+k}(\lambda) \underset{m}{\otimes} ... \left(\bar{\bar{G}}_p^{2+k}(\lambda) \underset{m}{\otimes} \left(\bar{\bar{G}}_p^{1+k}(\lambda) \underset{m}{\otimes} \bar{\bar{T}} \underset{m}{\oplus} \bar{B}_1 \right) \underset{m}{\oplus} \bar{B}_2 \right) ... \underset{m}{\oplus} \bar{B}_R}_{R \text{ раундів}} \times \bar{\bar{P}}_{\text{с}}^{\text{п}}; \quad (21)$$

$$\bar{\bar{T}}_{\text{ср}}^{\text{п}} =$$

$$= \underbrace{\bar{\bar{G}}_p^{-(1+k)}(\lambda) \underset{m}{\otimes} \left(...\bar{\bar{G}}_p^{-(R-1+k)}(\lambda) \underset{m}{\otimes} \left(\bar{\bar{G}}_p^{-(R+k)}(\lambda) \underset{m}{\otimes} \left(\bar{\bar{P}}_{\text{р}}'^{\text{п}} \times \left(\bar{\bar{K}}_{\text{рс}}^{\text{п}} \times \bar{\bar{P}}_{\text{с}}'^{\text{п}} \right) - \bar{B}_R \right) - \bar{B}_{R-1} \right) ... - \bar{B}_1 \right)}_{R \text{ раундів}}. \quad (22)$$

Отже, з'ясовано, що $\bar{\bar{G}}_p^n(\lambda)$-матриці, піднесені до n-го степеня, значеннями елементів яких є $p(\lambda)$-числа Фібоначчі для конкретного значення λ, ефективні для криптографічного перетворення даних. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової матричної звичайної та перестановної криптосистеми з різними ключами шифрування на кожному раунді. Запропонована структура реалізації цього алгоритму значно підвищує його криптостійкість до різних атак зловмисників.

ВИСНОВКИ

З'ясовано, що основна проблема багатораундової матричної Афінної криптосистеми полягає у генеруванні множини звичайних і обернених матриць – ключів (де)шифрування інформації, елементами яких мають бути цілі числа, у розширенні ключів для кожного раунду, а також у ефективній формі їх зберігання та передавання каналами зв'язку. Для її вирішення використано $\bar{\bar{G}}_p^n(\lambda)$-матрицю Фібоначчі, піднесену до n-го степеня. Наведено алгоритм формування такої матриці, елементами якої є $p(\lambda)$-числа Фібоначчі за конкретного значення λ. Отримані матриці можна використовувати як ключі шифрування (звичайні $\overline{\overline{G}}_p^n(\lambda)$ -матриці) та ключі дешифрування (обернені $\overline{\overline{G}}_p^{-n}(\lambda)$ -матриці) інформації для реалізації матричних криптографічних перетворень, а також як розширення ключів для реалізації багатораундової криптосистеми. Розроблено математичну процедуру генерування множини $\overline{\overline{G}}_p^n(\lambda)$ -матриць Фібоначчі, яка за відомими значеннями степеня матриці (n) для конкретних значень p і λ та, як наслідок, $p(\lambda)$-чисел Фібоначчі дає змогу отримувати відповідні матриці – ключі (де)шифрування, розширювати їх для кожного раунду, що забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й зручність під час передавання каналами зв'язку. З'ясовано, що $\overline{\overline{G}}_p^n(\lambda)$ -матриці Фібоначчі придатні для криптографічного перетворення даних. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової матричної звичайної та перестановної криптосистем з різними ключами шифрування на кожному раунді. Програмна реалізація алгоритму значно підвищує його криптостійкість до різних атак зловмисників.

Перспективи подальших досліджень. Обґрунтовані особливості ефективного генерування $\overline{\overline{G}}_p^n(\lambda)$ -матриць Фібоначчі, які можна використовувати як ключі (де)шифрування інформації, надалі реалізуємо у криптографічних перетвореннях $\overline{\overline{T}} \underset{m}{\otimes} \overline{\overline{G}}_p^n(\lambda) \underset{m}{\oplus} \overline{B} = \overline{\overline{K}}$ та $\overline{\overline{G}}_p^n(\lambda) \underset{m}{\otimes} \overline{\overline{T}} \underset{m}{\otimes} \overline{\overline{G}}_{p'}^{n'}(\lambda') \underset{m}{\oplus} \overline{B} = \overline{\overline{K}}$. Розглядатимемо можливість застосування повороту $\overline{\overline{G}}_p^n(\lambda)$ -матриць Фібоначчі для збільшення їх допустимої множини, а також можливість циклічного зсуву елементів стовпців і рядків $\overline{\overline{G}}_p^n(\lambda)$ -матриці Фібоначчі для підвищення стійкості криптографічних перетворень до брутальних атак.

1. *Грицюк П. Ю., Грицюк Ю. І.* Особливості реалізації матричної Афінної криптосистеми захисту інформації // Наук. вісник НЛТУ України. – 2015. – Вип. 25.5. – С. 346–356.
2. *Красиленко В. Г., Грабовляк С. К.* Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень // Системи обробки інформації. – 2012. – **2**, вип. 3 (101). – С. 53–61.
3. *Ємець В., Мельник А., Попович Р.* Сучасна криптографія: Основні поняття. – Львів: Вид-во БаК, 2003. – 144 с.
4. *Хорошко В. О., Четков А. О.* Методи та засоби захисту інформації: Навч. посібн. – К.: Юніор, 2003. – 502 с.
5. *Стахов А. П.* Гармония Мироздания и Золотое Сечение: древнейшая научная парадигма и ее роль в современной науке, математике и образовании: в 2-х ч. – Ч. 1: Доступный с http://www. obretenie.info/txt/stahov/harmoni1.htm
6. *Стахов А. П.* Гармония Мироздания и Золотое Сечение: древнейшая научная парадигма и ее роль в современной науке, математике и образовании: в 2-х ч. – Ч. 2: Доступный с http://www. obretenie.info/txt/stahov/harmoni2.htm
7. *Стахов А. П.* Введение в алгоритмическую теорию измерения. – М.: Сов. радио, 1977. – 246 с.
8. *Hoggat V. E.* Fibonacci and Lucas Numbers. – California: Houghton-Mifflin, Palo Alto, 1969. – 168 p.
9. *Гантмахер Ф. Р.* Теория матриц. – М.: Физматлит, 2010. – 560 с.
10. *Голуб Дж., ван Лоун Ч.* Матричные вычисления. – М.: Мир, 1999. – 548 с.
11. *Stakhov A. P.* Brousentsov's ternary principle, Bergman's number system and ternary mirror-symmetrical arithmetic // The Computer J. – 2002. – **45**, № 2. – P. 222–236.
12. *Stakhov A. P., Massingua V., Sluchenkova A. A.* Introduction into Fibonacci Coding and Cryptography. – Харьков: Основа, 1999. – 236 p.

Одержано 15.10.2015