МЕТОДИ І АЛГОРИТМИ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.056.5:681.3.05

Ю. Грицюк[1], П. Грицюк[2],
[1] Національний університет "Львівська політехніка",
кафедра програмного забезпечення;
[2] Національний лісотехнічний університет України,
кафедра інформаційних технологій

ОСОБЛИВОСТІ ГЕНЕРУВАННЯ Q_p-МАТРИЦЬ ФІБОНАЧЧІ – КЛЮЧІВ ДЛЯ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Розглянуто особливості ефективного генерування Q_p-матриць Фібоначчі, які можуть використовуватися як ключі (де)шифрування для багатораундової матричної криптографічної системи перетворення інформації. З'ясовано, що у багатораундовій матричній афінній криптосистемі основна проблема полягає у генеруванні множини звичайних і обернених матриць – ключів (де)шифрування інформації, елементами яких мають бути цілі числа. Розроблено процедуру генерування множини Q_p-матриць Фібоначчі, яка за відомими значеннями степені матриці (n) та (p) і, як наслідок, p-чисел Фібоначчі дає змогу отримувати відповідну множину ключів (де)шифрування інформації, здійснювати розширення ключів для кожного раунду, що забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й створює зручність при передаванні каналами зв'язку.

Ключові слова: захист інформації, шифрування/дешифрування інформації, числа Фібоначчі, Q_p-матриці Фібоначчі, криптографічна система, матричні Афінні перетворення, багатораундова матрична криптографічна система.

The features of effective generation of the Fibonacci Q_p-matrix have been considered. Those matrices are used as decryption/encryption keys for the multi-round matrix cryptographic system of the information transformation. It was found that in multi-round affinity matrix cryptosystem the main problem is to generate a plurality of the conventional and inverse keys-matrices of the information encryption/decryption that must be integers. The procedure for generating a plurality of Fibonacci Q_p-matrix has been developed. This procedure relies on the known degree of matrix values (n) and p-numbers Fibonacci and lets us set of the appropriate information encryption/decryption keys, implement expansion keys for each round. This provides an efficient way of their formation and storage and creates the ease of transmitting channels.

Key words: information security, encryption/decryption information, Fibonacci numbers, Fibonacci Q_p-matrix, crypto-graphic system, matrix Affine transformation, matrix multi-rounds crypto-graphic system.

Вступ

Криптографічні перетворення даних з використанням ключів шифрування призначені для приховування змісту інформації, підтвердження її достовірності, цілісності, авторства, дати створення тощо. Порівняно з іншими методами захисту класична криптографія гарантує захист інформації тільки за умов, якщо використано ефективний криптографічний алгоритм, а також

дотримані умови секретності та цілісності ключів шифрування. У роботі [3] було розглянуто особливості побудови надійної криптосистеми захисту інформації, яка поєднує матричні афінні перетворення, багатораундові дії з різними ключами, а також перестановні алгоритми, що загалом значно підвищує її криптостійкість до брутальних атак. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової матричної афінної перестановної криптосистеми з різними ключами шифрування на кожному раунді. Також у цій роботі було зазначено, що, порівняно з іншими методами захисту, класична криптографія гарантує захист інформації тільки за умов, якщо використано ефективний криптографічний алгоритм, а також дотримані умови секретності та цілісності ключів шифрування.

Однак, у матричних афінних перетвореннях [3, розд. 1] основна проблема полягає у генеруванні множини матриць $\overline{\overline{A}} = [\overline{A}_i = [a_{ij},\ j = \overline{1,n}], i = \overline{1,n}]$ – ключів шифрування, елементами яких є спеціально підібрані цілі числами з діапазону $1 \le a_{ij} < m$ (де m – кількість символів алфавіту), а також НСД(a, m) = 1, де $a = \det(\overline{\overline{A}}) \bmod m$ – визначник матриці $\overline{\overline{A}}$ за модулем m. Є також деякі питання щодо генерування й стовпців $\overline{B} = [b_i, i = \overline{1,n}]$ – ключів додаткового коригування вже зашифрованого повідомлення, елементами яких є цілі числа з діапазону $1 \le b_i < m$. Водночас для отримання зворотних матриць $\overline{\overline{A}}' = [\overline{A}_i' = [a_{ij}',\ j = \overline{1,n}],\ i = \overline{1,n}]$ – ключів дешифрування та зворотних стовпців $\overline{B}' = [b_i', i = \overline{1,n}]$ – ключів коригування потрібно виконати деяку послідовність дій, які описано в зазначеній вище роботі.

Якщо ж використовувати багатораундову матричну афінну криптосистему [див. 3, розд. 3], то на кожному раунді криптографічних перетворень (кількість яких може бути від 4 до 16 чи 24) виникає потреба у різних матричних ключах, тобто потрібно вирішувати питання розширення ключів для кожного раунду. Оскільки розміри цих матриць (n) можуть бути різними (мінімальний 32×32, нормальний 128×128 чи 256×256, надмірний 1048×1048 та більше), а кількість раундів шифрування – великою (32, 48, 64, …), то виникає проблема не тільки їх збереження, але й передавання цих ключів каналами зв'язку з кожним повідомленням. А як відомо з [4, 9], розмір зашифрованого повідомлення не має істотно відрізнятися від вхідного повідомлення. Водночас передані з повідомленням ключі шифрування не мають викликати в криптоаналітиків підозри у цілісності зашифрованого повідомлення.

Отже, основна проблема багатораундової матричної афінної криптосистеми полягає у генеруванні множини звичайних і обернених матриць – ключів шифрування/дешифрування інформації, елементами яких мають бути цілі числа, розширенні ключів для кожного раунду, а також у ефективній системі їх зберігання та передавання каналами зв'язку. Для її вирішення пропонуємо використовувати Q_p-матриці, елементами яких є p-числа Фібоначчі [7, 8].

Об'єкт дослідження – матричні ключі (де)шифрування та їх розширення для багатораундової криптографічної системи перетворення інформації.

Предмет дослідження – методи і засоби генерування Q_p-матриць – ключів (де)шифрування та розширення їхньої множини для кожного раунду криптографічних перетворень, елементами яких є p-числа Фібоначчі.

Мета роботи полягає в розробленні методів і засобів генерування Q_p-матриць Фібоначчі – ключів (де)шифрування для багатораундової криптографічної системи перетворення інформації та розширення їхньої множини, що дасть змогу не тільки ефективно їх утворювати, але й зберігати та передавати каналами зв'язку.

Для реалізації зазначеної мети потрібно виконати такі основні завдання:

1) з'ясувати основні наслідки модифікування прямокутного трикутника Паскаля, результати якого мали б стати основою ключів (де)шифрування;

2) виявити основні особливості побудови матриць на основі p-чисел Фібоначчі, які значно полегшать процес їх генерування та розширення потрібної множини для кожного раунду криптографічних перетворень;

3) здійснити реалізацію багатораундової криптосистеми на основі Q_p-матриць Фібоначчі, яка значно підвищує криптостійкість алгоритму шифрування;

4) зробити відповідні теоретичні висновки та надати рекомендації щодо практичного використання.

Особливості модифікування прямокутного трикутника Паскаля та його основні наслідки

Як відомо **[**2**]**, існує багато різних форм подання трикутника Паскаля. В нашому дослідженні використаємо таблицю біноміальних коефіцієнтів (табл. 1), яку ще прийнято називати *прямокутним трикутником Паскаля* **[**7**]**. Така таблиця починається з нульового стовпця, який містить єдиний біноміальний коефіцієнт $C_0^0 = 1$, а також з нульового рядка, який містить біноміальні коефіцієнти: $C_0^0 = C_1^0 = C_2^0 = ... = C_n^0 = 1$. "Гіпотенуза" такого прямокутного трикутника складається з таких біноміальних коефіцієнтів: $C_0^0 = C_1^1 = C_2^2 = ... = C_n^n = 1$.

Таблиця 1

Початковий вигляд прямокутного трикутника Паскаля [7]

№ з/п	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1		**1**	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2			**1**	3	6	10	15	21	28	36	45	55	66	78	91	105	120	136	153	171	190
3				**1**	4	10	20	35	56	84	120	165	220	286	364	455	560	680	816	969	1140
4					**1**	5	15	35	70	126	210	330	495	715	1001	1365	1820	2380	3060	3876	4845
5						**1**	6	21	56	126	252	462	792	1287	2002	3003	4368	6188	8568	11628	15504
6							**1**	7	28	84	210	462	924	1716	3003	5005	8008	12376	18564	27132	38760
7								**1**	8	36	120	330	792	1716	3432	6435	11440	19448	31824	50388	77520
8									**1**	9	45	165	495	1287	3003	6435	12870	24310	43758	75582	125970
9										**1**	10	55	220	715	2002	5005	11440	24310	48620	92378	167960
10											**1**	11	66	286	1001	3003	8008	19448	43758	92378	184756
11												**1**	12	78	364	1365	4368	12376	31824	75582	167960
12													**1**	13	91	455	1820	6188	18564	50388	125970
13														**1**	14	105	560	2380	8568	27132	77520
14															**1**	15	120	680	3060	11628	38760
15																**1**	16	136	816	3876	15504
16																	**1**	17	153	969	4845
17																		**1**	18	171	1140
18																			**1**	19	190
19																				**1**	20
20																					**1**
Σ	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576
pF_0^n	1	2	4	8	16	32	64	128	256	512	1024	2048	4096	8192	16384	32768	65536	131072	262144	524288	1048576

Водночас, у *n*-му стовпці цієї таблиці згори донизу розміщені такі біноміальні коефіцієнти: C_n^0, C_n^1, C_n^2, …, C_n^j, …, C_n^n. При цьому всі клітини під "гіпотенузою" є порожніми, позаяк всі діагональні коефіцієнти типу C_n^m ($m>n$) тотожно дорівнюють нулю. Якщо ж просумувати значення біноміальних коефіцієнтів *n*-го стовпця прямокутного трикутника Паскаля, то отримаємо ряд чисел $C_n^0 + C_n^1 + ... + C_n^n = 2^n$, який називається двійковим. Отже, можна стверджувати, що трикутник Паскаля "генерує" двійковий ряд чисел, який можна реалізувати за допомогою такої формули: $pF_0^{n+1} = 2pF_0^n$ при $pF_0^0 = 1$.

Побудова 1-трикутника Паскаля. Спробуємо зсунути кожен рядок початкового трикутника Паскаля (табл. 1) на один стовпець праворуч відносно попереднього рядка. Внаслідок такого перетворення отримаємо деякий "деформований" трикутник Паскаля [7], який прийнято називати 1-трикутником Паскаля (табл. 2).

Якщо тепер просумувати значення біноміальних коефіцієнтів 1-го трикутника Паскаля в кожному стовпці, то отримаємо ряд чисел 1, 1, 2, 3, 5, 8, 13, …, pF_1^n, які називаються *числами Фібоначчі*. Задати їх можна за допомогою такого рекурентного співвідношення:

$$pF_1^{n+1} = pF_1^n + pF_1^{n-1} \text{ при } n > 1, pF_1^0 = pF_1^1 = 1. \quad (1)$$

Таблиця 2

Вигляд 1-трикутника Паскаля [7]

№\n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1			**1**	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2					**1**	3	6	10	15	21	28	36	45	55	66	78	91	105	120	136	153
3							**1**	4	10	20	35	56	84	120	165	220	286	364	455	560	680
4									**1**	5	15	35	70	126	210	330	495	715	1001	1365	1820
5											**1**	6	21	56	126	252	462	792	1287	2002	3003
6													**1**	7	28	84	210	462	924	1716	3003
7															**1**	8	36	120	330	792	1716
8																	**1**	9	45	165	495
9																			**1**	10	55
10																					**1**
Σ	**1**	**1**	**2**	**3**	**5**	**8**	**13**	**21**	**34**	**55**	**89**	**144**	**233**	**377**	**610**	**987**	**1597**	**2584**	**4181**	**6765**	**10946**
pF_1^n	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946

Побудова *p*-трикутника Паскаля. А тепер покажемо, що трикутник Паскаля є джерелом нових числових рядів **[7]**, які представляють інтерес для реалізації криптографічних перетворень. Для цього продовжимо наші "маніпуляції" з трикутником Паскаля. Якщо у початковому трикутнику (див. табл. 1) зсунути біномінальні коефіцієнти на p стовпців (p = 1, 2, 3, …) праворуч відносно попереднього рядка, то отримаємо p-й "деформований" трикутник, який прийнято називати p-трикутником Паскаля. Підсумовуючи значення біномінальних коефіцієнтів у p-трикутнику, отримаємо кожного разу новий числовий ряд, який можна задати таким рекурентним співвідношенням:

$$\begin{cases} pF_p^j = 1;\ j = \overline{0, p}; \\ pF_p^{n+1} = pF_p^n + pF_p^{n-p}, \end{cases} \forall n \geq p+1;\ p = 0,1,2,3,\ldots;\ n = 1,2,3,4,\ldots. \qquad (2)$$

Числові ряди, які задаються рекурентним співвідношенням (2), винайдено ще в 1977 р. [6] і названо їх p-числами Фібоначчі. У табл. 3 наведено найпоширеніші їхні числові значення. Також p-числа можна задати через біномінальні коефіцієнти, а саме:

$$pF_p^{n+1} = C_n^0 + C_{n-p}^1 + C_{n-2p}^2 + C_{n-3p}^2 + \ldots,\ p = \overline{0, n-1}. \qquad (3)$$

Таблиця 3

Найпоширеніші *p*-числа Фібоначчі для різних значень *n*

p\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
6	1	1	1	1	1	1	1	2	3	4	5	6	7	8	10	13	17	22	28	35	43
7	1	1	1	1	1	1	1	1	2	3	4	5	6	7	8	9	11	14	18	23	29
8	1	1	1	1	1	1	1	1	1	2	3	4	5	6	7	8	9	10	12	15	19
9	1	1	1	1	1	1	1	1	1	1	2	3	4	5	6	7	8	9	10	11	13
10	1	1	1	1	1	1	1	1	1	1	1	2	3	4	5	6	7	8	9	10	11

У роботі [7] автор стверджує, що існують два способи задавання p-чисел Фібоначчі: у вигляді рекурентного співвідношення (2) і у вигляді формули (3), яка їх виражає через біномінальні коефіцієнти. Однак, формула (3) не зручна для використання. Водночас рекурентне співвідношення (2) хоча і доволі зручне для використання, проте є одновимірним, тобто значення p-чисел Фібоначчі отримуються у вигляді одновимірного масиву. А у алгоритмах реалізації криптографічних перетворень з різних причин прийнято використовувати двовимірні таблиці числових даних [4].

Особливості побудови матриць на основі чисел Фібоначчі

Поняття про *Q*-матрицю Фібоначчі. Як відомо з **[**10**]**, існує теорія матриць спеціального типу **[**1**]**, однією з яких є *Q*-матриця **[**8**]**. Найпростішою *Q*-матрицею є квадратна матриця розміром 2×2 такого вигляду:

$$\bar{\bar{Q}} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \det \bar{\bar{Q}} = -1 . \tag{4}$$

Однак, яке мають відношення *Q*-матриці до ряду чисел Фібоначчі? Для відповіді на це запитання достатньо піднести *Q*-матрицю до *n*-го степеня, внаслідок чого отримаємо такий набір матриць (звичайних і обернених, а також їхні визначники):

n	0	1	2	3	4	5	6	7	8	9	10
Q^n	1 0 0 1	1 1 1 0	2 1 1 1	3 2 2 1	5 3 3 2	8 5 5 3	13 8 8 5	21 13 13 8	34 21 21 13	55 34 34 21	89 55 55 34
p=1											
det Q^n	1	-1	1	-1	1	-1	1	-1	1	-1	1
Q^{-n}	1 0 0 1	0 1 1 -1	1 -1 -1 2	-1 2 2 -3	2 -3 -3 5	-3 5 5 -8	5 -8 -8 13	-8 13 13 -21	13 -21 -21 34	-21 34 34 -55	34 -55 -55 89
det Q^{-n}	1	-1	1	-1	1	-1	1	-1	1	-1	1

Отримані матриці можуть використовуватися як ключі шифрування (звичайні Q^n-матриці) та ключі дешифрування (обернені Q^{-n}-матриці) інформації для реалізації матричних афінних перетворень [3, розд. 1], а також як розширення ключів для реалізації багатораундової криптосистеми [3, розд. 3]. Особливості їхньої реалізації детально розглянуто у розд. 3 цього дослідження.

Розглянувши уважно наведені вище звичайні *Q*-матриці, можна побачити, що їхніми елементами є не що інше, як числа Фібоначчі. Водночас для певної Q^n-матриці, тобто піднесеної до *n*-го степеня, на головній діагоналі з трьох сусідніх чисел Фібоначчі знаходяться найбільше та найменше з них, а на побічній діагоналі – середнє число. Окрім цього, у звичайній та оберненій матрицях знаходяться одні і ті самі числа, тільки в оберненій матриці поміняні місцями числа на головній діагоналі та мають протилежний знак на побічній діагоналі. У загальному випадку *Q*-матриці, піднесені до *n*-го степеня, мають такий математичний запис [8]:

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

де F^{n-1}, F^n, F^{n+1} – числа Фібоначчі. Задавати *Q*-матриці *n*-го степеня можна за допомогою такого рекурентного співвідношення:

$$\bar{\bar{Q}}^{n+1} = \bar{\bar{Q}}^n + \bar{\bar{Q}}^{n-1}, \; n = 2,3,4,... \tag{6}$$

або за допомогою такого матричного виразу

$$\bar{\bar{Q}}^{n+1} = \bar{\bar{Q}}^n \times \bar{\bar{Q}}^1, \; n = 2,3,4,.... \tag{7}$$

Забігаючи наперед, зазначимо, що матричний вираз (7) є придатнішим для використання порівняно з рекурентним співвідношенням (6), позаяк має узагальнений характер розрахунку.

Узагальнена Q_p-матриця Фібоначчі. Спробуємо використати ідею побудови *Q*-матриці числами Фібоначчі для отримання узагальнених матриць Фібоначчі. В роботі [11] було введено квадратну матрицю спеціального типу, яку названо Q_p-матрицею:

$$\bar{\bar{Q}}_p = \left[\begin{array}{c|cccccc} \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{L} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & \mathbf{L} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{L} & 0 & 0 \\ \mathbf{L} & \mathbf{L} & \mathbf{L} & \mathbf{L} & \mathbf{L} & \mathbf{L} & \mathbf{L} \\ 0 & 0 & 0 & 0 & \mathbf{L} & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & \mathbf{L} & 0 & \mathbf{1} \\ \hline \mathbf{1} & 0 & 0 & 0 & \mathbf{L} & 0 & 0 \end{array}\right], \det \bar{\bar{Q}}_p = \pm 1, \; p = 0,1,2,3,.... \tag{8}$$

Особливістю будови Q_p-матриці 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 **1** 0 0 … 0 **1**. Для p = 0, 1, 2, 3 і 4 – відповідні матриці наведено нижче:

$$\bar{\bar{Q}}_0=[1],\ \det\bar{\bar{Q}}_1=1;\quad \bar{\bar{Q}}_1=\left[\begin{array}{c|c}1&1\\\hline 1&0\end{array}\right],\ \det\bar{\bar{Q}}_1=-1;\quad \bar{\bar{Q}}_2=\left[\begin{array}{c|cc}1&1&0\\\hline 0&0&1\\1&0&0\end{array}\right],\ \det\bar{\bar{Q}}_2=1;\quad \bar{\bar{Q}}_3=\left[\begin{array}{c|ccc}1&1&0&0\\\hline 0&0&1&0\\0&0&0&1\\1&0&0&0\end{array}\right],\ \det\bar{\bar{Q}}_3=-1;\quad \bar{\bar{Q}}_4=\left[\begin{array}{c|cccc}1&1&0&0&0\\\hline 0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\end{array}\right],\ \det\bar{\bar{Q}}_4=1. \tag{9}$$

Як не дивно, але Q_p-матриці також мають безпосереднє відношення до p-чисел Фібоначчі. Щоб це зрозуміти, достатньо піднести Q_p-матриці до n-го степеня, внаслідок чого для різних значень p отримаємо різні набори матриць з різними p-числами Фібоначчі. Наприклад, для p = 2 отримаємо набір $\bar{\bar{Q}}_2^n$-матриць, наведений нижче, елементами яких є 2-числа Фібоначчі (див. табл. 3).

Набір $\bar{\bar{Q}}_2^n$-матриць Фібоначчі

$n=$	0	1	2	3	4	5	6
$\bar{\bar{Q}}_2^n$	1 0 0 0 1 0 0 0 1	1 1 0 0 0 1 1 0 0	1 1 1 1 0 0 1 1 0	2 1 1 1 1 0 1 1 1	3 2 1 1 1 1 2 1 1	4 3 2 2 1 1 3 2 1	6 4 3 3 2 1 4 3 2
$\det\bar{\bar{Q}}_2^n$	1	1	1	1	1	1	1
$\bar{\bar{Q}}_2^{-n}$	1 0 0 0 1 0 0 0 1	0 0 1 1 0 -1 0 1 0	0 1 0 0 -1 1 1 0 -1	1 0 -1 -1 1 1 0 -1 1	0 -1 1 1 1 -2 -1 1 1	-1 1 1 1 -2 0 1 1 -2	1 1 -2 -2 0 3 1 -2 0
$\det\bar{\bar{Q}}_2^{-n}$	1	1	1	1	1	1	1

Продовження набору $\bar{\bar{Q}}_2^n$-матриць Фібоначчі

$n=$	7	8	9	10	11	12	13
$\bar{\bar{Q}}_2^n$	9 6 4 4 3 2 6 4 3	13 9 6 6 4 3 9 6 4	19 13 9 9 6 4 13 9 6	28 19 13 13 9 6 19 13 9	41 28 19 19 13 9 28 19 13	60 41 28 28 19 13 41 28 19	88 60 41 41 28 19 60 41 28
$\det\bar{\bar{Q}}_2^n$	1	1	1	1	1	1	1
$\bar{\bar{Q}}_2^{-n}$	1 -2 0 0 3 -2 -2 0 3	-2 0 3 3 -2 -3 0 3 -2	0 3 -2 -2 -3 5 3 -2 -3	3 -2 -3 -3 5 1 -2 -3 5	-2 -3 5 5 1 -8 -3 5 1	-3 5 1 1 -8 4 5 1 -8	5 1 -8 -8 4 9 1 -8 4
$\det\bar{\bar{Q}}_2^{-n}$	1	1	1	1	1	1	1

Розглянувши уважно звичайні та обернені матриці, можна побачити, що у звичайних матрицях значення елементів набувають тільки додатні 2-числа Фібоначчі, а в обернених – як додатні, так і від'ємні, можливо, й числа Фібоначчі, однак далеко не з цього самого набору. Водночас, $\bar{\bar{Q}}_2^n$-матриці при n = ±1 та ±2 є бінарними, а вже при n = ±3, ±4, ..., ±13 значення елементів набувають наступні 2-числа Фібоначчі. В обернених матрицях більшість значень елементів не відповідають їхнім значенням у звичайних матрицях.

У загальному випадку $\bar{\bar{Q}}_2^n$-матриці мають такий математичний запис:

$$\bar{\bar{Q}}_2^n=\begin{bmatrix} pF_2^{n+1} & pF_2^{n} & pF_2^{n-1}\\ pF_2^{n-1} & pF_2^{n-2} & pF_2^{n-3}\\ pF_2^{n} & pF_2^{n-1} & pF_2^{n-2}\end{bmatrix},\ \det\bar{\bar{Q}}_2^n=(-1)^{2\cdot n},\ n=2,3,4,\ldots, \tag{10}$$

де pF_2^{n-1}, pF_2^{n}, pF_2^{n+1} – 2-числа Фібоначчі. Задавати $\bar{\bar{Q}}_2^n$-матриці n-го степеня можна за допомогою такого матричного виразу:

$$\bar{\bar{Q}}_2^{n+1}=\bar{\bar{Q}}_2^n\times\bar{\bar{Q}}_2^1,\ n=2,3,4,\ldots. \tag{11}$$

Основний недолік цього виразу в тому, що для отримання $\bar{\bar{Q}}_2^{n+1}$-матриці Фібоначчі потрібно мати при цьому $\bar{\bar{Q}}_2^n$-матрицю, а це означає, що мають бути й усі попередні матриці від 2-го до (n-1)-го степеня.

Для розуміння основних закономірностей процесу побудови $\bar{\bar{Q}}_p^n$-матриць Фібоначчі розглянемо ще один приклад для p = 3. Тоді отриманий набір $\bar{\bar{Q}}_3^n$-матриць (див. нижче), піднесених до n-го степеня, має аналогічні особливості побудови, як і $\bar{\bar{Q}}_2^n$-матриці, однак елементами цих матриць вже є 3-числа Фібоначчі (див. табл. 3). Звернемо увагу тільки на те, що матрична формула (11) є також придатною для задавання $\bar{\bar{Q}}_3^n$-матриці, піднесеної до n-го степеня.

Набір $\bar{\bar{Q}}_3^n$-матриць Фібоначчі

$n=$	0	1	2	3	4	5
$\bar{\bar{Q}}_3^n$	1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1	1 1 0 0 0 0 1 0 0 0 0 1 1 0 0 0	1 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0	1 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0	2 1 1 1 1 1 0 0 1 1 1 0 1 1 1 1	3 2 1 1 1 1 1 0 1 1 1 1 2 1 1 1
$\det \bar{\bar{Q}}_3^n$	1	-1	1	-1	1	-1
$\bar{\bar{Q}}_3^{-n}$	1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1	0 0 0 1 1 0 0 -1 0 1 0 0 0 0 1 0	0 0 1 0 0 0 -1 1 1 0 0 -1 0 1 0 0	0 1 0 0 0 -1 1 0 0 0 -1 1 1 0 0 -1	1 0 0 -1 -1 1 0 1 0 -1 1 0 0 0 -1 1	0 0 -1 1 1 0 1 -2 -1 1 0 1 0 -1 1 0
$\det \bar{\bar{Q}}_3^{-n}$	1	-1	1	-1	1	-1

Продовження набору $\bar{\bar{Q}}_3^n$-матриць Фібоначчі

$n=$	6	7	8	9	10	11
$\bar{\bar{Q}}_3^n$	4 3 2 1 1 1 1 1 2 1 1 1 3 2 1 1	5 4 3 2 2 1 1 1 3 2 1 1 4 3 2 1	7 5 4 3 3 2 1 1 4 3 2 1 5 4 3 2	10 7 5 4 4 3 2 1 5 4 3 2 7 5 4 3	14 10 7 5 5 4 3 2 7 5 4 3 10 7 5 4	19 14 10 7 7 5 4 3 10 7 5 4 14 10 7 5
$\det \bar{\bar{Q}}_3^n$	1	-1	1	-1	1	-1
$\bar{\bar{Q}}_3^{-n}$	0 -1 1 0 0 1 -2 1 1 0 1 -2 -1 1 0 1	-1 1 0 1 1 -2 1 -1 0 1 -2 1 1 0 1 -2	1 0 1 -2 -2 1 -1 3 1 -2 1 -1 0 1 -2 1	0 1 -2 1 1 -1 3 -3 -2 1 -1 3 1 -2 1 -1	1 -2 1 -1 -1 3 -3 2 1 -1 3 -3 -2 1 -1 3	-2 1 -1 3 3 -3 2 -4 -1 3 -3 2 1 -1 3 -3
$\det \bar{\bar{Q}}_3^{-n}$	1	-1	1	-1	1	-1

Зрозуміло, що для $\bar{\bar{Q}}_3^n$-матриць Фібоначчі можна вивести й узагальнений математичний запис так, як це показано у виразі (10). Однак основним результатом роботи [11] є наведення для $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-го степеня, такого виразу:

$$\bar{\bar{Q}}_p^n = \begin{bmatrix} pF_p^{n+1} & pF_p^n & \mathbf{L} & pF_p^{n-p+2} & pF_p^{n-p+1} \\ pF_p^{n-p+1} & pF_p^{n-p} & \mathbf{L} & pF_p^{n-2p+2} & pF_p^{n-2p+1} \\ \mathbf{L} & \mathbf{L} & \mathbf{L} & \mathbf{L} & \mathbf{L} \\ pF_p^{n-1} & pF_p^{n-2} & \mathbf{L} & pF_p^{n-p} & pF_p^{n-p-1} \\ pF_p^n & pF_p^{n-1} & \mathbf{L} & pF_p^{n-p+1} & pF_p^{n-p} \end{bmatrix}, \qquad (12)$$

$$\det \bar{\bar{Q}}_p^n = (-1)^{p \cdot n}, \; p = 1, 2, 3, \ldots; \; n = \pm 2, \pm 3, \pm 4, \ldots.$$

Елементами цієї $\bar{\bar{Q}}_p^n$-матриці є p-числа Фібоначчі, які можна задати рекурентним співвідношенням (2). Зауважимо, що $\bar{\bar{Q}}_p^n$-матриці Фібоначчі для всіх $n \le p$ є бінарними, а при $n > p$ значення елементів набувають наступні p-числа Фібоначчі. Заради святих наукових ідей звернемо увагу й на те, що у виразі (12), як на перший погляд, слабко спостерігається закономірність процесу

формування $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-го степеня, елементами якої є p-числа Фібоначчі. Проте нижче спробуємо виявити таку закономірність, а також замість матричного виразу (11) використаємо дещо іншу математичну процедуру побудови $\bar{\bar{Q}}_p^n$-матриць Фібоначчі.

Отже, внаслідок проведеного дослідження встановлено, що існує теорія побудови квадратних матриць спеціального типу [8], які володіють унікальною математичною властивістю, придатною для виконання криптографічних перетворень: наведено алгоритм формування $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-го степеня, елементами якої є p-числа Фібоначчі; згідно з (12) визначник будь-якої $\bar{\bar{Q}}_p^n$-матриці завжди дорівнює одиниці за абсолютною величиною, а її знак залежить від добутку двох цілих чисел $p \cdot n$ (p = 1, 2, 3, ...; n = ±2, ±3, ±4, ...). Якщо цей добуток є парним, то визначник матриці (12) дорівнює +1, інакше – дорівнює –1. Отримані матриці можуть використовуватися як ключі шифрування (звичайні $\bar{\bar{Q}}_p^n$-матриці) та ключі дешифрування (обернені $\bar{\bar{Q}}_p^{-n}$-матриці) інформації для реалізації матричних криптографічних перетворень, а також як розширення ключів для реалізації багатораундової криптосистеми [3]. Особливості їхньої реалізації детально розглянуто у розд. 3 цього дослідження.

Процедура генерування $\bar{\bar{Q}}_p^n$-матриць Фібоначчі. Для виявлення основних закономірностей процедури генерування $\bar{\bar{Q}}_p^n$-матриці, піднесеної до n-го степеня, елементами якої є p-числа Фібоначчі, розглянемо такий приклад. За основу візьмемо $\bar{\bar{Q}}_3^n$-матрицю, піднесену до n = ±11, ±12, ..., ±16 степеня, внаслідок чого отримаємо їхній набір (див. нижче), елементами яких є 3-числа Фібоначчі (див. табл. 3). Спочатку розглянемо елементи $\bar{\bar{Q}}_3^{11}$-матриці, випишемо порядкові номери $u_{ij,3}^{11}$ її елементів і занесемо у відповідну матрицю $\bar{\bar{U}}_3^{11}$. Ці номери, згідно з даними табл. 3, відповідають номерам її стовпців, тобто маємо таку послідовність: $u_{1,1,3}^{11} = 11$, $u_{1,2,3}^{11} = u_{4,1,3}^{11} = 10$, $u_{1,3,3}^{11} = u_{3,1,3}^{11} = u_{4,2,3}^{11} = 9$ і т.д.

Продовження набору $\bar{\bar{Q}}_3^n$-матриць Фібоначчі

n	11	12	13	14	15	16
$\bar{\bar{Q}}_3^n$	19 14 10 7 7 5 4 3 10 7 5 4 14 10 7 5	26 19 14 10 10 7 5 4 14 10 7 5 19 14 10 7	36 26 19 14 14 10 7 5 19 14 10 7 26 19 14 10	50 36 26 19 19 14 10 7 26 19 14 10 36 26 19 14	69 50 36 26 26 19 14 10 36 26 19 14 50 36 26 19	95 69 50 36 36 26 19 14 50 36 26 19 69 50 36 26
$\det \bar{\bar{Q}}_3^n$	-1	1	-1	1	-1	1
$\bar{\bar{Q}}_3^{-n}$	-2 1 -1 3 3 -3 2 -4 -1 3 -3 2 1 -1 3 -3	1 -1 3 -3 -3 2 -4 6 3 -3 2 -4 -1 3 -3 2	-1 3 -3 2 2 -4 6 -5 -3 2 -4 6 3 -3 2 -4	3 -3 2 -4 -4 6 -5 6 2 -4 6 -5 -3 2 -4 6	-3 2 -4 6 6 -5 6 -10 -4 6 -5 6 2 -4 6 -5	2 -4 6 -5 -5 6 -10 11 6 -5 6 -10 -4 6 -5 6
$\det \bar{\bar{Q}}_3^{-n}$	-1	1	-1	1	-1	1
$\bar{\bar{U}}_3^n$	11 10 9 8 8 7 6 5 9 8 7 6 10 9 8 7	12 11 10 9 9 8 7 6 10 9 8 7 11 10 9 8	13 12 11 10 10 9 8 7 11 10 9 8 12 11 10 9	14 13 12 11 11 10 9 8 12 11 10 9 13 12 11 10	15 14 13 12 12 11 10 9 13 12 11 10 14 13 12 11	16 15 14 13 13 12 11 10 14 13 12 11 15 14 13 12

n = 11	1 2 3 4	12	1 2 3 4	13	1 2 3 4	14	1 2 3 4	15	1 2 3 4	16	1 2 3 4
$\bar{\bar{D}}_3^n$	1 8 7 6 5 2 9 8 7 6 3 10 9 8 7 4 11 10 9 8	1	1 9 8 7 6 2 10 9 8 7 3 11 10 9 8 4 12 11 10 9	1	1 10 9 8 7 2 11 10 9 8 3 12 11 10 9 4 13 12 11 10	1	1 11 10 9 8 2 12 11 10 9 3 13 12 11 10 4 14 13 12 11	1	1 12 11 10 9 2 13 12 11 10 3 14 13 12 11 4 15 14 13 12	1	1 13 12 11 10 2 14 13 12 11 3 15 14 13 12 4 16 15 14 13

Проаналізувавши значення елементів матриці $\bar{\bar{U}}_3^{11}$, бачимо, що перший рядок так і "проситься" перенести його донизу матриці, а всі решта рядки потрібно зсунути догори на одну позицію. Внаслідок такого зсуву рядків матриці $\bar{\bar{U}}_3^{11}$ на одну позицію догори отримаємо нову матрицю $\bar{\bar{U}}_3'^{11}$. Такі дії можна реалізувати за допомогою такого матричного виразу:

$$\bar{\bar{M}}_3^{+1} \times \bar{\bar{U}}_3^{11} = \bar{\bar{U}}_3'^{11}, \tag{13}$$

де $\bar{\bar{M}}_3^{+1}$ – матриця зсуву рядків матриці на одну позицію догори. Ця матриця є бінарною, а її елементи формуються так, як це показано нижче. Як виявиться згодом, нам доведеться зсувати рядки матриці на одну позицію не догори, а донизу, при цьому матриця зсуву $\bar{\bar{M}}_3^{-1}$ матиме дещо інший порядок розташування елементів (див. нижче). Зрозуміло, що зсув рядків матриці можна організувати не на одну, а на *k*-ту кількість позицій і, як виявиться потім, це значно вплине на якість виконання криптографічних перетворень, тобто підвищить їхню криптографічну стійкість.

Зсув рядків матриці догори на 1 позицію

$\bar{\bar{M}}_3^{+1}$

	1	2	3	4
1	0	**1**	0	0
2	0	0	**1**	0
3	0	0	0	**1**
4	**1**	0	0	0

$\times$ $\bar{\bar{U}}_3^{11}$

11	10	9	8
8	7	6	5
9	8	7	6
10	9	8	7

$=$ $\bar{\bar{U}}_3'^{11}$

8	7	6	5
9	8	7	6
10	9	8	7
11	10	9	8

Зсув рядків матриці вниз на 1 позицію

$\bar{\bar{M}}_3^{-1}$

	1	2	3	4
1	0	0	0	**1**
2	**1**	0	0	0
3	0	**1**	0	0
4	0	0	**1**	0

$\times$ $\bar{\bar{D}}_3^{11}$

8	7	6	5
9	8	7	6
10	9	8	7
11	10	9	8

$=$ $\bar{\bar{U}}_3^{11}$

11	10	9	8
8	7	6	5
9	8	7	6
10	9	8	7

Для формування елементів матриці зсуву $\bar{\bar{M}}_p^k$ використовується такий логічний вираз

$$\bar{\bar{M}}_p^k = \left[m_{ij,p}^k = \begin{cases} 1, \text{ якщо } (i+k-j) \bmod (p+1) = 0; \\ 0 - \text{у іншому випадку,} \end{cases} i, j = \overline{1, p+1} \right], \; k \le p, \tag{14}$$

де: $(p+1)$ – розмір бінарної матриці зсуву; k – кількість позицій зсуву ($\pm k$ – зсув догори/донизу).

Отже, з новоутвореної матриці $\bar{\bar{U}}_3'^{11}$ видно, що її елементи мають чітке впорядкування: відбувається зменшення їхніх значень з нижнього лівого кута матриці у бік її верхнього правого кута. Для формування елементів такої матриці (назвемо її $\bar{\bar{D}}_p^n$-матрицею), значення яких залежатимуть від *p*-чисел Фібоначчі та степеня *n* (до якого потрібно піднести матрицю), використаємо таку формулу

$$\bar{\bar{D}}_p^n = \left[d_{ij,p}^n = n - (p+1-i) - (j-1), \; i, j = \overline{1, p+1} \right]. \tag{15}$$

Ця формула є придатною для формування елементів матриці, якщо нумерація її рядків і стовпців починається з одиниці. Для інших випадків потрібні незначні корективи. Приклади генерування $\bar{\bar{D}}_3^n$-матриць для *n* = 12, 13, ..., 16 показано вище.

Повертаючись до нашого набору $\bar{\bar{Q}}_3^n$-матриць Фібоначчі для *n* = 11, 12, ..., 16 (див. вище), бачимо, що, сформувавши $\bar{\bar{D}}_3^{11}$-матрицю, потрібно здійснити зсув її рядків на одну позицію донизу, внаслідок чого отримаємо

$$\bar{\bar{M}}_3^{-1} \times \bar{\bar{D}}_3^{11} = \bar{\bar{U}}_3^{11}. \tag{16}$$

Тепер за елементами матриці $\bar{\bar{U}}_3^{11}$ можна відновити елементи $\bar{\bar{Q}}_3^{11}$-матриці, значеннями яких будуть 3-числа Фібоначчі (див. табл. 3).

Загалом процедура генерування $\bar{\bar{Q}}_p^n$-матриці, піднесеної до *n*-го степеня, значеннями елементів яких будуть *p*-числа Фібоначчі, матиме такий математичний запис:

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

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

$$\bar{\bar{U}}_p^n = \left[u_{ij,p}^n = \sum_{l=1}^{p+1} m_{il,p}^{-n} \cdot d_{lj,p}^n,\ i,j=\overline{1,p+1} \right]; \qquad (17)$$

$$\bar{\bar{Q}}_p^n = \left[q_{ij,p}^n = pF_p^{u_{ij,p}^n},\ i,j=\overline{1,p+1} \right],\ p=1,2,3,\ldots;\ n=2,3,4,\ldots;\ k=-1,-2,\ldots-p.$$

Основною перевагою цієї процедури над матричним виразом (11) є те, що для отримання $\bar{\bar{Q}}_p^{n+1}$–матриці зовсім не потрібно мати $\bar{\bar{Q}}_p^n$-матрицю, а це означає, що немає потреби і в будь-яких попередніх матрицях. Єдине, що потрібно мати, так це наперед згенеровані *p*-числа Фібоначчі для різних значень *n* (див. табл. 3). Зазначимо також, що наведені вище $\bar{\bar{Q}}_3^n$-матриці для *n* = 12, 13, ..., 16 сформовано за допомогою наведеної процедури (17), уникнувши при цьому матричного виразу (11). При цьому обернені до них матриці отримано звичайним способом, хоча не виключено, що їх також можна отримати дещо простішим способом. Однак для цього потрібно провести ще додаткове дослідження з виявлення закономірностей їх побудови.

Продемонструємо використання процедури генерування $\bar{\bar{Q}}_p^n$-матриці Фібоначчі на конкретному прикладі при таких вхідних значеннях: *p* = 4, *n* = 16 та *k* = 2. У цьому випадку, згідно з табл. 3, маємо справу з такими 4-числа Фібоначчі: 1, 1, 1, 1, 1, 2, 3, 4, 5, 6, 8, 11, 15, 20, 26, 34, 45. Внаслідок виконання математичної процедури (17) отримаємо такі результати розрахунку:

$\bar{\bar{D}}_4^{16}$

16	1	2	3	4	5
1	12	11	10	9	8
2	13	12	11	10	9
3	14	13	12	11	10
4	15	14	13	12	11
5	16	15	14	13	12

$\bar{\bar{M}}_4^2$

k=	2			
0	0	0	1	0
0	0	0	0	1
1	0	0	0	0
0	1	0	0	0
0	0	1	0	0

$\bar{\bar{U}}_4^{16}$

15	14	13	12	11
16	15	14	13	12
12	11	10	9	8
13	12	11	10	9
14	13	12	11	10

$\bar{\bar{Q}}_4^{16}$

34	26	20	15	11
45	34	26	20	15
15	11	8	6	5
20	15	11	8	6
26	20	15	11	8

$\bar{\bar{Q}}_4^{-16}$

1	0	-1	3	-3
-4	1	1	-4	6
6	-3	1	1	-4
-4	3	-3	1	1
1	-1	3	-3	1

$\det \bar{\bar{Q}}_4^{16} = 1$ $\quad \det \bar{\bar{Q}}_4^{-16} = 1$

Отже, внаслідок проведеного дослідження розроблено процедуру генерування множини $\bar{\bar{Q}}_p^n$–матриць Фібоначчі, яка за відомими значеннями степеня матриці (*n*) та *p*-чисел Фібоначчі дає змогу отримувати відповідні матриці – ключі (де)шифрування, здійснювати їхнє розширення для кожного раунду, що забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й створює зручність при передаванні каналами зв'язку.

3. Використання узагальнених матриць Фібоначчі для криптографічних перетворень інформації

Виявляється [12], що $\bar{\bar{Q}}_p^n$-матриці Фібоначчі (12) можна з успіхом використовувати для реалізації матричної криптосистеми аналогічно афінній. Суть методу шифрування, який ґрунтується на використанні цих матриць, полягає у поданні початкового повідомлення у вигляді матриці $\bar{\bar{T}}$ розміром (*p*+1)×*q* і реалізації таких матричних дій:

шифрування $$\bar{\bar{Q}}_p^n \underset{m}{\otimes} \bar{\bar{T}} \underset{m}{\oplus} \bar{B} = \bar{\bar{K}}; \qquad (18)$$

дешифрування $$\bar{\bar{Q}}_p^{-n} \underset{m}{\otimes} \left(\bar{\bar{K}} - \bar{B} \right) = \bar{\bar{T}}, \qquad (19)$$

де *q* – кількість стовпців матриці $\bar{\bar{T}}$, $q \geq 1$; $\bar{B} = [b_i, i=\overline{1,p+1}]$ – стовпець (ключ) коригування, елементами якого є цілі числа з діапазону $1 \leq b_i < m$; У виразах (18) і (19) символами $\underset{m}{\otimes}$ і $\underset{m}{\oplus}$ позначено відповідно множення та додавання елементів матриць за модулем *m*.

Продемонструємо особливості застосування розглянутого вище методу (де)шифрування інформації з використанням узагальнених матриць Фібоначчі на конкретному прикладі (див. нижче). У цьому прикладі використано $\bar{\bar{Q}}_p^n$-матрицю для p = 3, n = 5, елементами якої є 3-числа Фібоначчі.

Шифрування вхідного повідомлення

$\bar{\bar{Q}}_3^5$

3	2	1	1
1	1	1	0
1	1	1	1
2	1	1	1

$\times$

$\bar{\bar{T}}$

219	185	202	183	204	213	97
93	64	155	59	103	136	151
175	247	110	249	75	63	158
98	76	229	218	50	158	222

$+$

$\bar{B}$

232
175
108
186

$=$

$(\bar{\bar{Q}}_3^5 \times \bar{\bar{T}} + \bar{B}) \bmod 256 = \bar{\bar{K}}$

68	214	207	86	151	84	181
150	159	130	154	45	75	69
181	168	36	49	28	166	224
222	175	60	54	54	201	143

Дешифрування зашифрованої інформації

$\bar{\bar{Q}}_3^{-5}$

0	0	-1	1
1	0	1	-2
-1	1	0	1
0	-1	1	0

$\times$

$\left(\right.$ $\bar{\bar{K}}$

68	214	207	86	151	84	181
150	159	130	154	45	75	69
181	168	36	49	28	166	224
222	175	60	54	54	201	143

$-$

$\bar{B}$

232
175
108
186

$\left.\right)$ $=$

$(\bar{\bar{Q}}_3^{-5} \times (\bar{\bar{K}} - \bar{B})) \bmod 256 = \bar{\bar{T}}$

219	185	202	183	204	213	97
93	64	155	59	103	136	151
175	247	110	249	75	63	158
98	76	229	218	50	158	222

Використання $\bar{\bar{Q}}_p^n$-матриці Фібоначчі для реалізації багатораундової матричної криптосистеми. Виявляється, що до матричного виразу (18), який дає змогу зашифрувати повідомлення $\bar{\bar{T}}$, можна застосувати R-раундову процедуру шифрування, при цьому кожного разу з новими ключами, тобто $\bar{\bar{Q}}_p^n$-матрицями Фібоначчі для $n = r = 1, 2, ..., R$. Водночас процес дешифрування інформації за виразом (19) також повторюватиметься R разів. У цьому випадку узагальнені вирази для реалізації прямого та зворотного криптографічних перетворень матимуть такий вигляд:

$$\bar{\bar{K}} = \underbrace{\bar{\bar{Q}}_p^R \otimes ... \left(\bar{\bar{Q}}_p^2 \otimes \left(\bar{\bar{Q}}_p^1 \otimes \bar{\bar{T}} \oplus \bar{B}_1 \right) \oplus \bar{B}_2 \right) ... \oplus \bar{B}_R}_{R \text{ раундів}}; \tag{20}$$

$$\bar{\bar{T}} = \underbrace{\bar{\bar{Q}}_p^{-1} \otimes \left(... \bar{\bar{Q}}_p^{-(R-1)} \otimes \left(\bar{\bar{Q}}_p^{-R} \otimes \left(\bar{\bar{K}} - \bar{B}_R \right) - \bar{B}_{R-1} \right) ... - \bar{B}_1 \right)}_{R \text{ раундів}}. \tag{21}$$

Поєднання матричної криптосистеми (20) і (21) з матричними перестановними алгоритмами [3, розд. 3] дає змогу побудувати багатораундову матричну перестановну криптосистему для захисту інформації, яку загалом можна подавати у вигляді процедури багатораундового (де)шифрування на основі таких матричних виразів:

$$\bar{\bar{K}}_{\text{рс}}^{\text{п}} = \underbrace{\bar{\bar{Q}}_p^R \otimes ... \left(\bar{\bar{Q}}_p^2 \otimes \left(\bar{\bar{Q}}_p^1 \otimes \left(\bar{\bar{P}}_{\text{р}}^{\text{п}} \times \bar{\bar{T}} \times \bar{\bar{P}}_{\text{с}}^{\text{п}} \right) \oplus \bar{B}_1 \right) \oplus \bar{B}_2 \right) ... \oplus \bar{B}_R}_{R \text{ раундів}}; \tag{22}$$

$$\bar{\bar{T}}_{\text{ср}}^{\text{п}} = \bar{\bar{P}}_{\text{р}}'^{\text{п}} \times \left(\underbrace{\bar{\bar{Q}}_p^{-1} \otimes \left(... \bar{\bar{Q}}_p^{-(R-1)} \otimes \left(\bar{\bar{Q}}_p^{-R} \otimes \left(\bar{\bar{K}}_{\text{рс}}^{\text{п}} - \bar{B}_R \right) - \bar{B}_{R-1} \right) ... - \bar{B}_1 \right)}_{R \text{ раундів}} \times \bar{\bar{P}}_{\text{с}}'^{\text{п}} \right), \tag{23}$$

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. Основу матричних виразів (22) і (23) становлять перестановні матриці $\bar{\bar{P}}^{\text{п}}$, в яких у кожному стовпці та в кожному рядку є тільки один елемент, який дорівнює **1**, а всі інші – 0. Наприклад, нехай задана така перестановка $\Pi = \{p_j,\ j = \overline{1,n}\} \Rightarrow \begin{Bmatrix} 1 & 2 & 3 & 4 & 5 \\ \mathbf{4} & \mathbf{3} & \mathbf{5} & \mathbf{1} & \mathbf{2} \end{Bmatrix}$. Тоді перестановна матриця шифрування матиме такий вигляд:

$$\bar{\bar{P}}^{\text{п}} = \left[\bar{P}_i^{\text{п}} = \left[p_{ij}^{\text{п}} = \begin{cases} \mathbf{1}, \text{ якщо } p_j = i; \\ 0, \text{ якщо } p_j \neq i, \end{cases} j = \overline{1,n} \right], i = \overline{1,n} \right] =$$

	4	**3**	**5**	**1**	**2**
1	0	0	0	**1**	0
2	0	0	0	0	**1**
3	0	**1**	0	0	0
4	**1**	0	0	0	0
5	0	0	**1**	0	0

. (24)

Водночас зворотна перестановна матриця дешифрування матиме такий вигляд:

$$\bar{\bar{P}}'^{\text{п}} = \left[\bar{P}_i'^{\text{п}} = \left[p_{ij}'^{\text{п}} = \begin{cases} \mathbf{1}, \text{ якщо } p_i = j; \\ 0, \text{ якщо } p_i \neq j, \end{cases} j = \overline{1,n} \right], i = \overline{1,n} \right] =$$

	1	2	3	4	5
4	0	0	0	**1**	0
3	0	0	**1**	0	0
5	0	0	0	0	**1**
1	**1**	0	0	0	0
2	0	**1**	0	0	0

. (25)

Окрім матричних виразів (22) і (23) можливі ще й такі вирази для реалізації процедури багатораундового (де)шифрування інформації:

$$\bar{\bar{K}}_{\text{рс}}^{\text{п}} = \bar{\bar{P}}_{\text{р}}^{\text{п}} \times \underbrace{\bar{\bar{Q}}_p^R \otimes \ldots \left(\bar{\bar{Q}}_p^2 \otimes \left(\bar{\bar{Q}}_p^1 \otimes \bar{\bar{T}} \oplus \bar{B}_1 \right) \oplus \bar{B}_2 \right) \ldots \oplus \bar{B}_R}_{R \text{ раундів}} \times \bar{\bar{P}}_{\text{с}}^{\text{п}}; \tag{26}$$

$$\bar{\bar{T}}_{\text{ср}}^{\text{п}} = \underbrace{\bar{\bar{Q}}_p^{-1} \otimes \left(\ldots \bar{\bar{Q}}_p^{-(R-1)} \otimes \left(\bar{\bar{Q}}_p^{-R} \otimes \left(\bar{\bar{P}}_{\text{р}}'^{\text{п}} \times \left(\bar{\bar{K}}_{\text{рс}}^{\text{п}} \times \bar{\bar{P}}_{\text{с}}'^{\text{п}} \right) - \bar{B}_R \right) - \bar{B}_{R-1} \right) \ldots - \bar{B}_1 \right)}_{R \text{ раундів}}; \tag{27}$$

Отже, внаслідок проведеного дослідження з'ясовано, що $\bar{\bar{Q}}_p^n$-матриці, піднесені до n-го степеня, значеннями елементів яких є p-числа Фібоначчі, можуть ефективно використовуватися для виконання криптографічних перетворень інформації. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової матричної звичайної та перестановної криптосистеми з різними ключами шифрування на кожному раунді, реалізація якого значно підвищує його криптостійкість до брутальних атак.

Висновки

1. 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, розширенні ключів для кожного раунду, а також у ефективній системі їх зберігання та передавання каналами зв'язку. Для її вирішення прийнято рішення використовувати Q_p-матриці Фібоначчі.

2. Наведено алгоритм формування $\bar{\bar{Q}}_p^n$-матриці Фібоначчі, піднесеної до n-го степеня, елементами якої є p-числа Фібоначчі. Отримані матриці можуть використовуватися як ключі шифрування (звичайні $\bar{\bar{Q}}_p^n$-матриці) та ключі дешифрування (обернені $\bar{\bar{Q}}_p^{-n}$-матриці) інформації для реалізації матричних перетворень, а також як розширення ключів для реалізації багатораундової криптосистеми.

3. Розроблено процедуру генерування множини $\bar{\bar{Q}}_p^n$-матриці Фібоначчі, яка за відомими значеннями степені матриці (n) та p-чисел Фібоначчі дає змогу отримувати відповідні матриці – ключі (де)шифрування, здійснювати їхнє розширення для кожного раунду, що забезпечує не тільки ефективний спосіб їх утворення та зберігання, але й створює зручність при передаванні каналами зв'язку.

4. З'ясовано, що $\bar{\bar{Q}}_p^n$-матриці Фібоначчі можуть ефективно використовуватися для виконання криптографічних перетворень інформації. Математично описано алгоритм (де)шифрування інформації за допомогою багатораундової матричної звичайної та перестановної криптосистеми з різними ключами шифрування на кожному раунді, реалізація якого значно підвищує його криптостійкість до брутальних атак.

Перспективи подальших досліджень

Обґрунтовано теоретичні особливості ефективного генерування Q_p-матриць Фібоначчі, які можуть використовуватися як ключі (де)шифрування інформації у подальших дослідженнях щодо розроблення алгоритму формування $\bar{\bar{G}}_p^n(\lambda)$-матриць Фібоначчі, піднесених до n-го степеня, елементами яких будуть l-числа Фібоначчі. Отримані матриці можуть використовуватися як ключі шифрування (звичайні $\bar{\bar{G}}_p^n(\lambda)$-матриці) та ключі дешифрування (обернені $\bar{\bar{G}}_p^n(\lambda)$-матриці) інформації для реалізації криптографічних перетворень, а також як розширення ключів для реалізації багатораундових криптосистем. Окрім наведеної вище схеми перетворення $\bar{\bar{G}}_p^n(\lambda) \underset{m}{\otimes} \bar{\bar{T}} \underset{m}{\oplus} \bar{B} = \bar{\bar{K}}$, будуть залучені ще й додаткові криптографічні схеми, такі як $\bar{\bar{T}} \underset{m}{\otimes} \bar{\bar{G}}_p^n(\lambda) \underset{m}{\oplus} \bar{B} = \bar{\bar{K}}$ та $\bar{\bar{G}}_p^n(\lambda) \underset{m}{\otimes} \bar{\bar{T}} \underset{m}{\otimes} \bar{\bar{G}}_p^{n'}(\lambda') \underset{m}{\oplus} \bar{B} = \bar{\bar{K}}$. Буде також розглянуто можливість використання повороту матриць Фібоначчі для збільшення їх допустимої множини, а також можливість циклічного зсуву елементів стовпців і рядків $\bar{\bar{G}}_p^n(\lambda)$-матриці Фібоначчі для підвищення стійкості криптографічних перетворень до брутальних атак.

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