DOI 10.31891/2307-5732-2022-305-1-84-89
УДК 004.056

РОЗЛОМІЙ І. О.
https://orcid.org/0000-0001-5065-9004
e-mail: inna-roz@ukr.net
Черкаський національний університет ім. Б. Хмельницького

МЕТОД ПОБУДОВИ МАТРИЧНИХ РЕШІТОК КАРДАНО ДЛЯ СТИСНЕННЯ ІНФОРМАЦІЇ

Стаття присвячена методу побудови матричних решіток Кардано для стиснення та прихованої передачі даних. Розроблений метод грунтується на комплексному використанні існуючих підходів та методик захисту інформації. Зокрема, на класичному шифрі маршрутної перестановки – шифрувальної решітки Кардано. Шифрувальна решітка Кардано побудована на основі частотного аналізу англомовного тексту та застосування операцій матричного критографічного перетворення. В подальшому запропонований метод дозволить побудувати нові алгоритми шифрування інформації за аналогією шифрувальної решітки. Також, створені алгоритмічні моделі є базисом для побудови методу стиснення та прихованої передачі даних.

Ключові слова: частотний аналіз текстів, надлишковість, кодування, шифрувальна решітка, стиснення інформації, прихована передача даних.

INNA ROZLOMII
Bohdan Khmelnytsky National University of Cherkasy

METHOD OF CONSTRUCTION MATRIX CARDANO'S GRIDS FOR COMPRESSION OF INFORMATION

Due to the rapid development of computer technology and the information field, issues related to information security are becoming increasingly important. Knowledge of information security tools is required for the effective organization of the process of transmission and storage of classified information. The main means of information protection such as encryption, compression and covert transmission of information are present in the article . Information security techniques, including cryptographic data protection systems, play an important role in today's information-filled world. The means of cryptographic data protection, in particular encryption using the Cardano's encryption grid are list and analyze in the article. Existing mechanisms for reliable storage and transmission of information today do not provide adequate protection. The problem of lack of effective means of information protection is explained by rapid and systematic changes in information technology.

The article is devoted to the method of constructing Cardano matrix gratings for compression and hidden data transmission. The developed method is based on the integrated use of existing approaches and methods of information protection. In particular, on the classic cipher of the route permutation – Cardano's encryption grid. Cardano matrix lattice is based on frequency analysis of English text. The algorithm of frequency analysis of the text and its results are presented in the article. As a result of performing operations of matrix cryptographic transformation of numbers – the rules of distribution of symbols on a lattice are received.

In the future, the proposed method will build new algorithms for encrypting information by analogy with the encryption lattice. Also, the created algorithmic models are the basis for building a method of compression and covert data transmission. The methods of information protection considered in the article – encryption, compression and covert transmission, allow us to draw the general conclusion that only their integrated use will ensure an adequate level of protection.

Keywords: texts frequency analysis, redundancy, encoding, grille cipher, information compression, hidden data transmission.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Стрімкий розвиток інформаційних технологій неминуче призводить до необхідності забезпечення конфіденційності і цілісності інформації. Технології віртуально інфраструктури інтенсивно впроваджуються в сучасне життя. Експлуатація інформаційних систем (ІС) в контексті обробки даних стає звичним явищем, зручним та ефективним. Комплексне забезпечення інформаційної безпеки представляє собою безперервний процес, який постійно вимагає модифікації і, як результат, ускладнення ІС. Інфраструктура ІС передбачає впровадження технічних чи програмних компонентів, наявність яких призводить до збільшення можливостей несанкціонованого доступу до оброблюваної інформації.

Під інформаційною безпекою розуміють дії, спрямовані на запобігання від несанкціонованого доступу, умисного видалення, модифікації, перегляду, редагування та інших дій особами, які не мають на це прав. Загальновизнаними заходами щодо формування режиму інформаційної безпеки у комп'ютерних та телекомунікаційних системах є методи криптографії. До методів криптографічного перетворення інформації відносять: шифрування, кодування, стеганографію та стиснення.

Одним з ефективних способів вирішення проблеми захисту інформації є шифрування. Всі криптографічні алгоритми будуються на основі використання, так званих, криптографічних примітивів – простих операцій, комбінація яких дозволяє отримати алгоритм шифрування даних. Проте, часто потрібно не лише зашифрувати дані, але і зробити їх зберігання та передачу більш ефективною. В зв'язку з цим, разом з шифруванням доречним є використання методів стиснення та прихованої передачі даних. Стиснення – процес усунення надлишковості інформації. Стиснення даних до методів криптографічного перетворення інформації відноситься умовно і застосовується для зменшення об'єму інформації різними способами, наприклад, на основі використання правил скорочень, заміни та інших.

Аналіз досліджень та публікацій

В ряді випадків при організації збереження і передачі даних доводиться мати справу з текстовою інформацією. Як приклад, можуть служити різноманітні пошукові системи, системи збереження спеціалізованої текстової інформації та інші інформаційні системи. В таких випадках для підвищення ефективності зберігання та передачі великих об'ємів текстової інформації комп'ютерними мережами використовують її стиснення, методи прихованої передачі та шифрування. Багато публікацій присвячені розробці методів стиснення [1-3] та шифрування текстової інформації [4-8]. Особливої уваги заслуговує робота [9], в якій запропонована модель криптографічного стиснення даних. Особливістю алгоритму, що представлений в даній роботі є те, що він поєднує алгоритм стиснення та шифрування. В зв'язку з цим актуальною задачею є розробка нових ефективних методів стиснення, шифрування та прихованої передачі, які дозволять забезпечити цілісність інформації при її передачі та зберіганні.

Формулювання цілей статті

Мета роботи полягає у розробці методу формування матричних решіток Кардано для побудови нових методів криптографічного стиснення та прихованої передачі інформації відкритими каналами зв'язку.

Виклад основного матеріалу

Для побудови нових методів криптографічного стиснення та прихованої передачі інформації необхідно розробити прототип матричної решітки на основі класичної решітки Кардано. Формування матричних решіток Кардано передбачає використання операцій матричного криптографічного перетворення та виконання частотного аналізу тексту [10]. Алгоритм формування матричних решіток Кардано показаний на рис. 1 і описується наступною послідовністю кроків:

1) виконати частотний аналіз тексту – обчислити частоту входження кожної букви алфавіту;

2) задати матрицю та виконати матричне криптографічне перетворення чисел з діапазону 0…255;

3) визначити частоту входження кожної букви в решітку;

4) розставити букви в решітку.

На рис. 1 показана схема алгоритму формування матричної решітки Кардано.

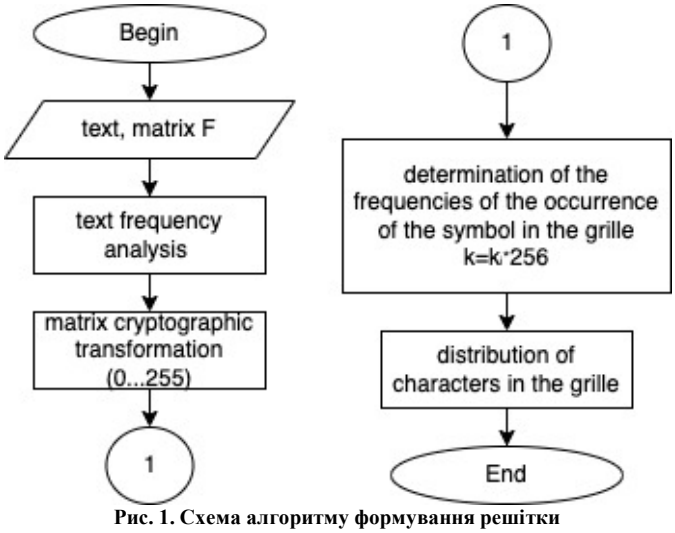

Рис. 1. Схема алгоритму формування решітки

Побудова матричних решіток Кардано базується на частотному аналізі тексту та операціях матричного криптографічного перетворення. Для побудови статистичної решітки Кардано було взято англомовний текст (рис.2).

А.С. Пушкин "Письмо Татьяны Онегину"

I love you, nothing else to say
I have, but also know you may
Surround me with your disdain.
But condoling my pitty way
You won't abandon me alone.
At first I wanted keep my senses,
You wouldn't hear what's right, what's wrong,
If I had any expectancies
To see you seldom, once a week
In our lands, to give you a quick,
Fond eye, to hear your voice and then,
Then think about "Where?", "When?"
My dear, we will meet again.
But people say that you're reserved
In our solitude you're bored,
And we're not brilliantly bright
But you are welcome days and nights.
Why have you visited that nook?
It was enough to have a look
At you to feel my poor heart
In love, if we had stood apart

My feelings would have come to end
And,I'd have met my future friend,
Who, maybe, I won't ever stand,
But I'd be able to become
A faithful wife and a kind mum.
Another man? Oh no, I'll never,
I'll never love another one!
It was determined in heaven,
And if you call me, I will come
To you. For me you're only one,
Who I've been waiting all my life.
I know exactly you're my Sun,
Which saves me from all the strikes.
I saw you even in my dreams,
You won my heart without seeing
Your queer stare took my being,
Your voice in soul was like scream
That time -No, I was not asleep!
I've noticed you're to it concerning
I was astonished, was I burning,
How I was dreaming of friendship!

I've heard you, dear, did you see?
How calm it was to speak to me,
When I was helping poor men
Or praying, were you near then
To make my soul just to be
In peace, this moment, precious sight,
You was the only man who might
Appear in the limpid night
Before my hoping face inclining.
Were not that you who shed in loving
Timbre hopeful light?
Can you pretend to save from evil
My innocence or you are devil?
My world was deeply got upset,
But maybe it is self-deception
Of soul lulled with loving thread?
And there won't be any action…
But I decided – I am yours
With tears asking for protection
Without you around the earth
There's only lonely direction.

No one of people round mine
Can matter out what possesses
My pour flagging crazy mind
Tossing in agony of death.
I wait for you and our date
Which'll be conclusive for my fate.

It's over! I became so pale,
I falter with a scaring heart
But till your honor is my bail
I put my faith in your conduct.

Рис. 2. Текст взятий за основу решітки

Над текстом з рис. 2 необхідно виконати його частотний аналіз за алгоритмом, який показаний на рис. 3. Частотний аналіз тексту розраховує частоту появи кожного символу в тексті [11-12].

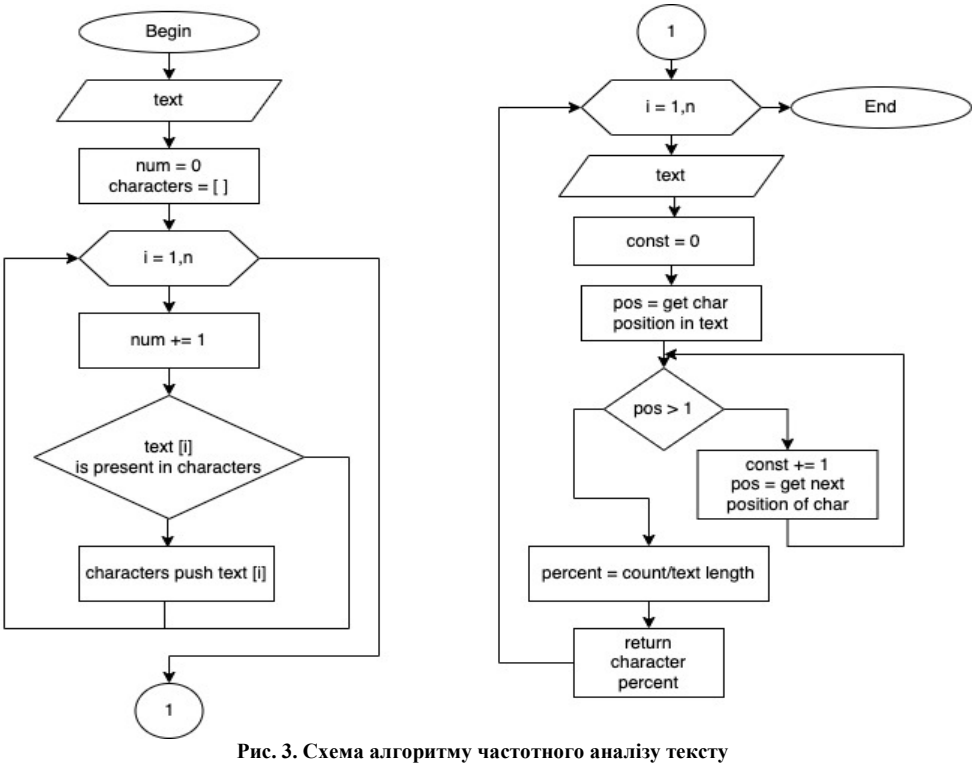

Рис. 3. Схема алгоритму частотного аналізу тексту

На рис. 4. Показані результати частотного аналізу тексту, а також статистичні дані частот літер англійської мови.

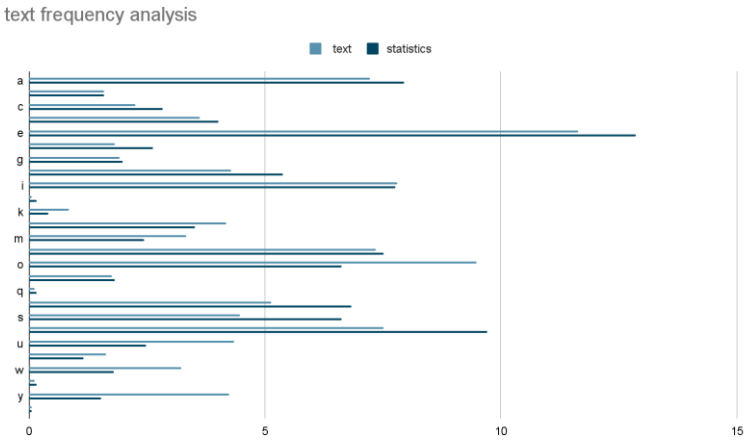

Рис. 4. Результат частотного аналізу англомовного тексту у відсотках

Наступним кроком алгоритму є визначення частоти входження кожної літери англійського алфавіту в решітку. Враховуючи, що решітка має 256 комірок, то частоту входження кожної літери обчислюємо amount=percent*256, де percent – результат частотного аналізу літери у відсотках (рис.3). Отримані результати обчислень показані на рис. 5. На рис. 5 показана частота входження кожної літери в решітку і діапазон, який займає кожна літера.

a = 18, [0-17]	g = 5, [71-75]	l = 11, [111-121]	q = 1, [177]	v = 4, [232-235]
b = 4, [18-21]	h = 11, [76-86]	m = 8, [122-129]	r = 13, [178-190]	w = 8, [236-243]
c = 6, [22-27]	i = 20 [87-107]	n = 19, [130-148]	s = 11, [191-201]	x = 1 [244]
d = 9, [28-36]	j = 1, [108]	o = 24, [149-172]	t = 19, [202-220]	y = 10, [245-254]
e = 30, [37-66]	k = 2, [109-110]	p = 4 [173-176]	u = 11, [221-231]	z = 1, [255]
f = 4, [67-70]				

Рис. 5. Результати визначення частоти входження кожної літери в решітку

Як зазначалося вище, для формування матричної решітки, крім частотного аналізу тексту, використовуються операції матричного криптографічного перетворення. Матричні алгоритми придатні для обернених перетворень, якщо при цьому виконуються такі умови:

1) відсутні нульові рядки і стовпці в матриці;

2) додавання рядків і стовпців матриці не дорівнюватиме нулю.

Виходячи з цього можна говорити, що при додаванні рядків і стовпців матриці, матриця буде не виродженою [13]. Візьмемо це з основу.

В загальному вигляді операції криптографічного перетворення, побудовані на основі додавання за модулем два, описуються такою моделлю (1) [13-14]:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \oplus b_2 \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \oplus b_n \end{pmatrix}, \tag{2}$$

де $a_{ij} \in [0,1]; b_i \in [0,1]; x_1 ... x_n$ – операнди-розряди відповідно; $\oplus$ – операція «сума за mod 2» [16].

Для того, щоб вказати, як розташувати букви в комірки решітки виконаємо матричні криптографічні перетворення чисел від 0 до 255. Нехай операція матричного криптографічного перетворення задана матрицею:

$$\vec{F}_k = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

для знаходження результату перетворення необхідно підставити значення відповідних інформаційних бітів в систему

$$F = \begin{cases} x_2 \oplus x_4 \oplus x_5 = y_1 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_7 \oplus x_8 = y_2 \\ x_2 \oplus x_4 \oplus x_5 \oplus x_8 = y_3 \\ x_2 \oplus x_6 \oplus x_8 = y_4 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_7 = y_5 \\ x_1 \oplus x_2 \oplus x_5 \oplus x_7 = y_6 \\ x_3 \oplus x_3 \oplus x_6 \oplus x_7 = y_7 \\ x_5 = y_8 \end{cases},$$

де $x_1,...,x_8$ – вихідний байт, $y_1,...,y_8$ – байт, отриманий в результаті матричного перетворення.

Для обчислення значень матричних криптографічних перетворень чисел із заданого діапазону було розроблено програмне забезпечення, результати якого показані на рис. 6.

Для побудови матричних решіток Кардано скористаємось даними отриманими в результаті частотного аналізу тексту та результатом виконання матричного криптографічного перетворення чисел. З рис. 5 відома кількість кожної літери, яка має входити в решітку. Далі необхідно заповнити 256 комірок решітки літерами. Номери комірок в які буде розміщуватись та чи інша літера візьмемо з результатів, представлених на рис. 6. Наприклад, з рис. 5 відомо, що літера «а» займає діапазон [0–17]. З рис. 6 потрібно взяти результати матричного криптографічного перетворення чисел цього діапазону [0–17]. Відповідно, результати вкажуть на комірки, в яких буде записана літера «а». Аналогічним чином необхідно заповнити всі комірки решітки літерами в тій кількості в якій заначено на рис. 6.

0 => 0	1 => 112	2 => 78	3 => 62	4 => 18	5 => 98	6 => 92	7 => 44	8 => 229	9 => 149	10 => 171
11 => 219	12 => 247	13 => 135	14 => 185	15 => 201	16 => 226	17 => 146	18 => 172	19 => 220	20 => 240	21 => 128
22 => 190	23 => 206	24 => 7	25 => 119	26 => 73	27 => 57	28 => 21	29 => 101	30 => 91	31 => 43	32 => 74
33 => 58	34 => 4	35 => 116	36 => 88	37 => 40	38 => 22	39 => 102	40 => 175	41 => 223	42 => 225	43 => 145
44 => 189	45 => 205	46 => 243	47 => 131	48 => 168	49 => 216	50 => 230	51 => 150	52 => 186	53 => 202	54 => 244
55 => 132	56 => 77	57 => 61	58 => 3	59 => 115	60 => 95	61 => 47	62 => 17	63 => 97	64 => 252	65 => 140
66 => 178	67 => 194	68 => 238	69 => 158	70 => 160	71 => 208	72 => 25	73 => 105	74 => 87	75 => 39	76 => 11
77 => 123	78 => 69	79 => 53	80 => 30	81 => 110	82 => 80	83 => 32	84 => 12	85 => 124	86 => 66	87 => 50
88 => 251	89 => 139	90 => 181	91 => 197	92 => 233	93 => 153	94 => 167	95 => 215	96 => 182	97 => 198	98 => 248
99 => 136	100 => 164	101 => 212	102 => 234	103 => 154	104 => 83	105 => 35	106 => 29	107 => 109	108 => 65	109 => 49
110 => 15	111 => 127	112 => 84	113 => 36	114 => 26	115 => 106	116 => 70	117 => 54	118 => 8	119 => 120	120 => 177
121 => 193	122 => 255	123 => 143	124 => 163	125 => 211	126 => 237	127 => 157	128 => 76	129 => 60	130 => 2	131 => 114
132 => 94	133 => 46	134 => 16	135 => 96	136 => 169	137 => 217	138 => 231	139 => 151	140 => 187	141 => 203	142 => 245
143 => 133	144 => 174	145 => 222	146 => 224	147 => 144	148 => 188	149 => 204	150 => 242	151 => 130	152 => 75	153 => 59
154 => 5	155 => 117	156 => 89	157 => 41	158 => 23	159 => 103	160 => 6	161 => 118	162 => 72	163 => 56	164 => 20
165 => 100	166 => 90	167 => 42	168 => 227	169 => 147	170 => 173	171 => 221	172 => 241	173 => 129	174 => 191	175 => 207
176 => 228	177 => 148	178 => 170	179 => 218	180 => 246	181 => 134	182 => 184	183 => 200	184 => 1	185 => 113	186 => 79
187 => 63	188 => 19	189 => 99	190 => 93	191 => 45	192 => 176	193 => 192	194 => 254	195 => 142	196 => 162	197 => 210
198 => 236	199 => 156	200 => 85	201 => 37	202 => 27	203 => 107	204 => 71	205 => 55	206 => 9	207 => 121	208 => 82
209 => 34	210 => 28	211 => 108	212 => 64	213 => 48	214 => 14	215 => 126	216 => 183	217 => 199	218 => 249	219 => 137
220 => 165	221 => 213	222 => 235	223 => 155	224 => 250	225 => 138	226 => 180	227 => 196	228 => 232	229 => 152	230 => 166
231 => 214	232 => 31	233 => 111	234 => 81	235 => 33	236 => 13	237 => 125	238 => 67	239 => 51	240 => 24	241 => 104
242 => 86	243 => 38	244 => 10	245 => 122	246 => 68	247 => 52	248 => 253	249 => 141	250 => 179	251 => 195	252 => 239
253 => 159	254 => 161	255 => 209								

Рис. 6. Результат матричного криптографічного перетворення чисел

В результаті отримано матричну решітку (рис.7), яка служить основою для подальшої розробки методів шифрування, стиснення та прихованої передачі даних. Даний підхід до формування решітки дозволяє отримувати різні варіанти решіток шляхом зміни вхідних даних. Зокрема, якщо взяти інший текст для частотного аналізу – буде інший результат частоти входження кожної літери в решітку. Також зміна матриці для виконання операцій матричного криптографічного перетворення сформує інакші правила розподіл усимволів по комірках решітки.

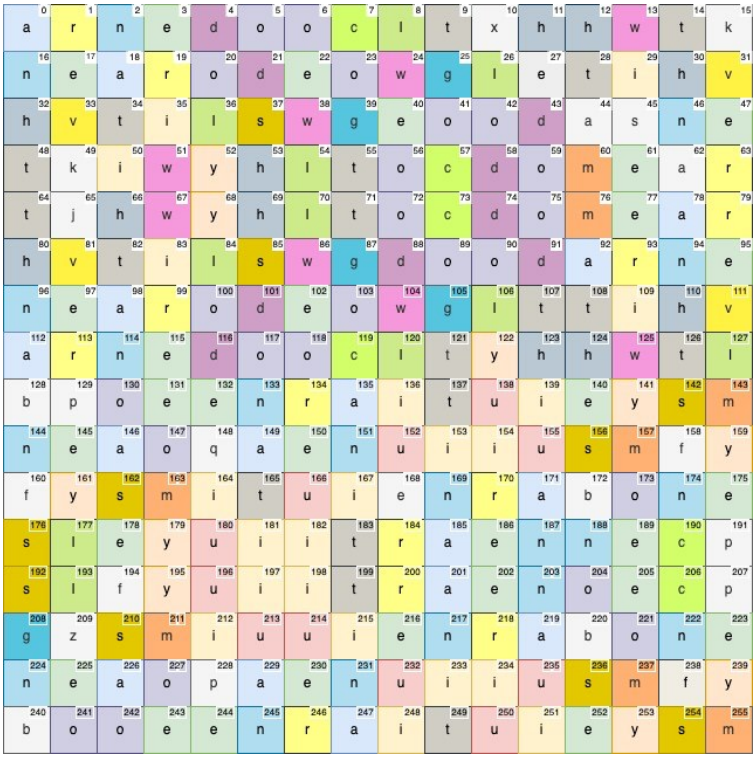

Рис. 7. Матрична решітка

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Методи захисту інформації, зокрема системи криптографічного захисту даних, відіграють важливу роль у сучасному, наповненому інформацією світі. Уявлення про засоби захисту потрібні для нормального функціонування передачі та зберігання секретної інформації. Таким чином, слід зазначити, що існуючі механізми надійного зберігання та передачі інформації сьогодні не забезпечують належного захисту. Проте, проблема відсутності ефективних засобів захисту інформації пояснюється швидкими і систематичними змінами інформаційних технологій. Розглянуті в статті методи захисту інформації – шифрування, стиснення та прихована передача, дозволяють зробити загальний висновок про те, що лише комплексне їх використання дозволить забезпечити належний рівень захисту. Тому, в статті було запропоновано метод формування матричної решітки, яка служить базисом для розробки нових методів шифрування, стиснення та прихованої передачі інформації.

Література

1. Потемкин В.Г., Корсунов Н.И. (2009) Алгоритм сжатия информации с адаптацией для криптосистем. Научные ведомости. 7 (62). 101–107.

2. Серебровский В.В., Ефремова И.Н., Ефремов В.В., Емельянова Н.А. (2019) Исследование эффективности объединения процессов поиска и сжатия символьной информации. Научные ведомости. 2(46). 284–295.

3. Кудина В.А., Нэй Лин (2019) Использование метода сжатия информации в семантическом информационном поиске. Научные ведомости. 1(161). Т. 46. 161–172.

4. Бабаш А.В., Баранова Е.К., Лютина А.А., Мурзакова А.А., Мурзакова Е.А., Рябова Д.М., Семис Е.С. (2020) О границах зашумления текстов при сохранении их содержания. Приложение к криптографии. Вопросы кибербезопасности. 1(35). 74 – 86.

5. Encryption: practical guide. Jean-Philippe Aumasson. San Francisco: no starch press, 2017. 312p.

6. Запечников С.В. Криптографические методы защиты информации: учебное пособие. М.: Юрайт, 2017. 309 с.

7. Васильева И.Н. Криптографические методы защиты информации: учебное пособие. М.: Юрайт, 2016. 64 с.

8. Жданов О.Н., Золотарев В.В. Методы и средства криптографической защиты информации: учебное пособие. Красноярск: Сиб. ГАУ, 2007. 217 с.

9. Кожевникова И. С., Ананьин Е. В., Датская Л. В. (2015) Формализированная модель криптографического сжатия данных. Евразийский Союз Ученых. 5 (14). 78–80.

10. Головань О. В. (2008) Частотный анализ как первый шаг а построении интеллектуальной системы исследования текста. Ползуновский альманах. 2. 153 – 155.

11. Ворончихина Е. Н., Жигалко Е. Ф., Калинина П. С., Привалов Н. А., Пашнина Н. В., Пахнушева М. Ю. (2010) Частотные характеристики символов чертежных текстов. Известия ПГУПС. 1. 10–18.

12. Осочкин А.А., Фомин В.В., Флегонтов А.В. (2017) Метод частотно-морфологической классификацыи текстов. Программные продукты и системы. Software & Systems 3 (30). 478 – 486.

13. Розломій І.О. Методи обчислення хеш-функції електронного документу на основі матричних криптографічних перетворень. Вісник ЧДТУ. Технічні науки. 2016. № 4. С. 88–94.

14. Розломій І.О., Косенюк Г.В. Виявлення порушень цілісності електронного документу шляхом перехресного хешування. Вісник Хмнльницького національного університету. Радіотехніка, електроніка та телекомунікації. 2018. № 5 (265). С. 32–35.

References

1. Potemkin V.G., Korsunov N.I. (2009) Algorithm of compression of the alphabetic information with adaptation for cryptosystems. Scientific statements. 7 (62). 101–107.

2. Serebrovsky V.V., Efremova I.N., Efremov V.V., Emelianova N.A. (2019), Assessment of the efficiency of unification pf search processes and compression of symbol information. Scientific statements. 2(46). 284–295.

3. Kudinov V.A., Nay Lin (2019) Using the method of information compression in a semantic retrieval. Scientific statements. 1(161). T. 46. 161–172.

4. Babash A.V., Baranova E.K., Lyutina A.A., Murzakova A.A., Murzakova E.A., Ryabova D.M., Semis E.S. About text noise borders with the text content saving. Applications to cryptography. Cybersecurity issues. 1(35). 74–86.

5. Encryption: practical guide. Jean-Philippe Aumasson. San Francisco: no starch press, 2017. 312p.

6. Zapechnikov S.V. Information protecting cryptographic methods: a tutorial. M.: Yurayt, 2017. 309 p.

7. Vasilyeva I.N. Information protecting cryptographic methods: a tutorial. M.: Yurayt, 2016. 64 p.

8. Zhdanov O.N., Zolotarev V.V. Cryptographic information protection methods and means: educational manual. Krasnoyarsk: Sib. GAU, 2007. 217 p.

9. Kozhevnikova I.S., Ananin E.V., Datskaya L.V. (2015) Formalized model of cryptographic data compression. Eurasian Union of Scientists. 5 (14). 78–80.

10. Golovan O.V. (2008) Frequency analysis as the first step in the construction of an intellectual system for text research. Polzunovsky almanac 2. 153–155.

11. Voronchikhina E. N., Zhigalko E. F., Kalinina PS, Privalov N. A., Pashnina N. V., Pakhnusheva M. Yu. (2010) Frequency characteristics of symbols of drawing texts. Izvestia PGUPS. 1. 10–18.

12. Osochkin A.A., Fomin V.V., Flegontov A.V. (2017) Method of frequency-morphological classification of texts. Software & Systems 3 (30). 478–486.

13. Rozlomii I.O. (2016) Methods for calculating the hash function of an electronic document based on matrix cryptographic conversions. Visnik ChDTU. Technical sciences. 4. 88–94.

14. Rozlomii I.O., Kosenyuk H.V. (2018) Revealing the deterioration of the integrity of the electronic document by the way of perekhresny kheshuvannya. Herald of Khmelnytskyi National University. 5 (265). 32–35.

Рецензія/Peer review : 13.01.2022 р. Надрукована/Printed : 27.02.2022 р.