DOI: https://doi.org/10.36910/6775-2524-0560-2023-51-11
УДК 681.3.05:004.056
Розломій Інна Олександрівна, к.т.н., старш. викладач
https://orcid.org/0000-0001-5065-9004
Косенюк Григорій Володимирович, к.т.н., доцент
https://orcid.org/0000-0003-2103-3904
Науменко Сергій Васильович, аспірант
https://orcid.org/0000-0002-6337-1605
Черкаський національний університет імені Богдана Хмельницького, м. Черкаси, Україна

МЕТОД ВЕКТОРНОГО ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ АВТОРСЬКОГО ШАБЛОНУ

Розломій І.О., Косенюк Г.В., Науменко С.В. Метод векторного шифрування інформації на основі використання авторського шаблону. В зв'язку зі стрімким збільшенням обсягу даних, що обробляються сучасними інформаційними системами, виникає потреба в компактному та надійному зберіганні цих даних. У статті описано метод шифрування зі стисненням, який дозволяє не тільки захистити конфіденційну інформацію від зловмисного використання, але й зберегти простір для зберігання даних за рахунок їх стиснення. Цей метод шифрування відрізняється від інших існуючих методів тим, що дозволяє ефективно зменшити розмір даних, що зберігаються. Даний метод шифрування базується на авторському шаблоні, що є прототипом шифрувальної таблиці. Для побудови авторського шаблону використано статистичний аналіз тексту та матричні примітиви. Новий метод векторного шифрування текстової інформації для одночасної реалізації стиснення та шифрування з прийнятною довжиною ключа та не надмірними обчислювальними можливостями техніки, коли ключ легко розподіляється, зберігається та запам'ятовується. Метод полягає в розбитті вхідного тексту на вектори з вагами та пошуку їх позицій у авторському шаблоні. Застосування цього методу дозволяє не тільки захистити дані від несанкціонованого доступу, а й забезпечити оптимізоване зберігання даних. Як показали дослідження, отримана зашифрована послідовність менша за вхідний текст на 65%. Такий підхід є особливо важливим в умовах зростаючої кількості даних, коли ефективне зберігання та передача інформації стають ключовими факторами успіху в будь-якій інформаційній системі. Описаний метод шифрування може знайти широке застосування в багатьох сферах, включаючи фінансові послуги, медичну та наукову галузі, де потреба в надійному та компактному зберіганні даних є найважливішою.
Ключові слова: компресійне шифрування, матрична решітка, метод Кардано, шифрувальна решітка, матричне криптографічне перетворення, дешифрування, стиснення.

Rozlomii I., Kosenyuk H., Naumenko S. Vector's method of information encryption based on the author's template. In connection with the rapid increase in the amount of data processed by modern information systems, there is a need for compact and reliable storage of this data. Method of encryption with compression, which allows not only to protect confidential information from malicious use, but also to save storage space for data by the compression was describe in the article. This encryption method differs from other existing methods in that it effectively reduces the size of the data that is stored. This encryption method is based on the author's template, which is the prototype of the encryption table. Statistical text analysis and matrix primitives were used to build the author's template. A new method of using plaintext encryption to simultaneously implement compression and encryption with a long key and low hardware computing power, where the key is easily shared, stored and remembered. The method involves splitting the input text into vectors with weights and finding their positions in the author's template. Application of this method allows not only to protect data from unauthorized access, but also to ensure optimized data storage. Research has shown that the resulting encrypted sequence is 65% smaller than the input text. This approach is especially important in the conditions of the growing amount of data, when efficient storage and transfer of information become key success factors in any information system. The described encryption method can be widely used in many fields, including financial services, medical and scientific fields, where the need for reliable and compact data storage is the most important.
Key words: compression encryption, matrix grid, Cardano method, encryption grid, matrix cryptographic transformation, decryption, compression.

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями. У світі зростає обсяг інформації, яку потрібно зберігати та передавати. Шифрування і стиснення є двома основними методами зменшення розміру даних та забезпечення їх конфіденційності. Але часто вони використовуються окремо один від одного, збільшуючи час та зусилля, необхідні для обробки даних.

Алгоритми стиснення дозволяють не тільки ефективно зберігати конфіденційні дані, а й значно зменшити розмір програми, яку за один прийом можна завантажити в пам'ять та виконати [1-2]. Існує велика кількість різних пакувальників файлів, деякі з них містять реалізації алгоритмів шифрування. Але в жодному з них алгоритм шифрування ніяк не пов'язаний з алгоритмом стиснення. Вони реалізовані як окремі алгоритми та використовуються окремо. Питання поєднання алгоритмів стиснення та шифрування стоїть давно.

Шифрування є важливою складовою сучасного світу, особливо в епоху цифрової технології і широкого використання Інтернету [3]. Захист конфіденційної інформації є важливою проблемою,

з якою стикаються усі галузі – від особистих комунікацій до фінансових установ і урядових органів. З огляду на все більшу кількість атак на мережеві системи та проникнення в приватні дані, відомі методи шифрування виявляються недостатньо ефективними. Тому виникає потреба в пошуку нових методів, які можуть допомогти вирішити ці проблеми.

Найбільшого поширення набули блочні симетричні шифри, так як вони забезпечують високий рівень захисту даних і відносно прості в реалізації. Ці шифри мають широке застосування в сучасних системах інформаційної безпеки, включаючи мережеву безпеку, електронну пошту, онлайн-банкінг, електронну комерцію та інші сфери. До блокових належать шифри перестановки та підстановки (заміни).

Одним з найвідоміших перестановочних методів шифрування є метод шифру маршрутної перестановки – метод, який використовується для перестановки символів в рядку повідомлення згідно з певними правилами, щоб отримати зашифрований текст [4-5]. Під час шифрування, символи повідомлення переставляються в рядки та стовпці шифрувальної таблиці, яка зазвичай має матричну форму та розмірність, задану ключем шифрування. Шифр маршрутної перестановки застосовується в багатьох сферах, включаючи комунікації в армії, поліції та інших силових органах, а також в криптографії.

Шифр маршрутної перестановки може бути відносно легко розшифрований, якщо не використовувати додаткові методи захисту, тому зазвичай використовується як частина складніших методів шифрування. Також, шифр маршрутної перестановки може бути вразливий до атак, які базуються на вивченні закономірностей розподілу символів у шифрованому тексті. Шифр маршрутної перестановки не є досконалим, але він може бути основою для побудови нового методу компресійного шифрування.

Аналіз останніх досліджень та публікацій. У сучасних умовах, коли цифрові технології стрімко розвиваються, а обсяги даних постійно зростають, важливість захисту інформації стає ще більшою. З цієї причини наукова спільнота сьогодні зосереджена на вирішенні проблем захисту даних, включаючи використання комплексних методів криптографії та стиснення даних. [6-7].

Багато публікацій присвячені шифрам перестановки, зокрема маршрутної перестановки, представником якої є шифрувальна таблиця [8-9]. Особливої уваги заслуговує робота [10], в якій запропоновано метод шифрування інформації за допомогою симетрично-поворотної решітки Кардано. Особливістю запропонованого методу є те, що ключі перестановки генеруються випадковим чином.

Щодо стиснення даних, варто відмітити роботу [11] в якій пропонується метод, який перетворює вихідні дані в компактну форму шляхом розпізнавання та використання шаблонів.

В статті [12] авторами пропонується комбінація найсучасніших методів стиснення та шифрування цифрових документів. Описується метод ефективного стиснення та шифрування даних, але ці два процеси розглядаються окремо один від одного.

В [13] описано забезпечення безпеки даних засобами криптографії та за допомогою стиснення. Авторами пропонується комплексний метод захисту, який передбачає стиснення даних з подальшим шифруванням.

Крім того, в роботі [14] запропоновано паралельний алгоритм стиснення та шифрування даних в мережах, оскільки через ці мережі регулярно проходить велика кількість інформації, яку, крім надійної передачі, необхідно ще й максимально компактно зберігати.

Огляд останніх досліджень підтвердив, що розробка нових методів криптографічного стиснення є перспективним напрямком. **Метою** статті є розробка методу векторного шифрування на основі використання прототипу шифрувальної таблиці для криптографічного стиснення даних.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Шифрувальні шаблони або трафарети – це інструменти, які використовуються для шифрування повідомлень та інформації [15]. Їх використання полягає в тому, що вони надають можливість шифрувати повідомлення, використовуючи певний набір символів або регулярних виразів. Шаблони можуть бути відкритими або закритими, тобто деякі символи можуть бути замінені знаками питання або іншими символами, які не вказують на конкретну букву або цифру.

Використання шаблонів дає можливість шифрувати повідомлення за допомогою заміни символів або груп символів на інші символи або групи символів. Наприклад, шаблон може вказувати на заміну всіх голосних букв на певний символ, що використовується як ключ для розшифрування. Це може допомогти збільшити безпеку повідомлень та інформації, оскільки

шаблон може бути захищений паролем або іншими методами аутентифікації, що забезпечують доступ лише авторизованим користувачам.

Також використовуються спеціальні трафарети для шифрування інформації у вигляді матриць або таблиць, де кожному символу відповідає певна комбінація координат. Ці трафарети можуть бути використані для шифрування повідомлень та інформації за допомогою заміни символів на координати, які потім можуть бути перетворені у відповідні символи за допомогою таблиці дешифрування [16].

Загалом, шифрувальні шаблони та трафарети є ефективними інструментами для захисту повідомлень та інформації від небажаних доступу та зламу. Однак, варто пам'ятати, що жоден метод шифрування не є повністю безпечним, і його слід використовувати лише як один з елементів комплексної системи захисту даних. Крім того, ефективність шаблонів та трафаретів може залежати від їх складності та частоти використання, тому важливо розробляти нові та більш складні шаблони для збільшення безпеки.

У сучасному світі шифрувальні шаблони та трафарети використовуються в багатьох галузях, включаючи інформаційну безпеку, фінансові технології, медіа та інтернет-технології. Зокрема, шаблони використовуються в алгоритмах шифрування та підпису електронної пошти, в безпечному обміні інформацією через мережу Інтернет, а також в захисті фінансових операцій та транзакцій.

У підсумку, шифрувальні шаблони та трафарети є потужними інструментами для захисту інформації від небажаного доступу та зламу. Вони можуть бути використані в різних галузях та контекстах, але варто пам'ятати, що жоден метод шифрування не є повністю безпечним і їх слід використовувати лише як частину комплексної системи захисту даних.

Існуючі методи блокового шифрування дають у результаті зашифрований текст такого ж розміру, як і вхідний текст. Метод, який пропонується в статті, дозволяє отримати зашифровану послідовність, яка буде мати менший розмір, ніж вхідна. Метод векторного шифрування дозволяє виконувати шифрування зі стисненням. Поєднання шифрування та стиснення сприяє ефективнішому зберіганню та захисту інформації. Рисунок 1 демонструє схему шифрування, розроблену за допомогою діаграми IDEF.

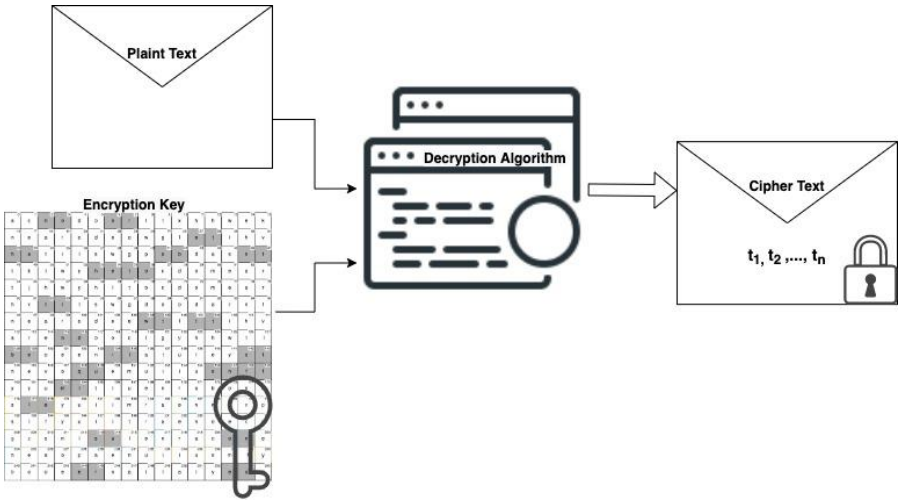

Рис. 1 – Шифрування, результатом якого є послідовність чисел (зсувів векторів)

Новий підхід для симетричного шифрування, в якому для шифрування відкритого тексту передбачає використання особливого ключа – авторського шаблону, який є прототипом шифрувальної решітки Кардано, але побудований за певними правилами, описаними в [17].

Правила побудови авторського шаблону, сформовані на основі статистичного аналізу тексту та матриці, наведені на рис. 2.

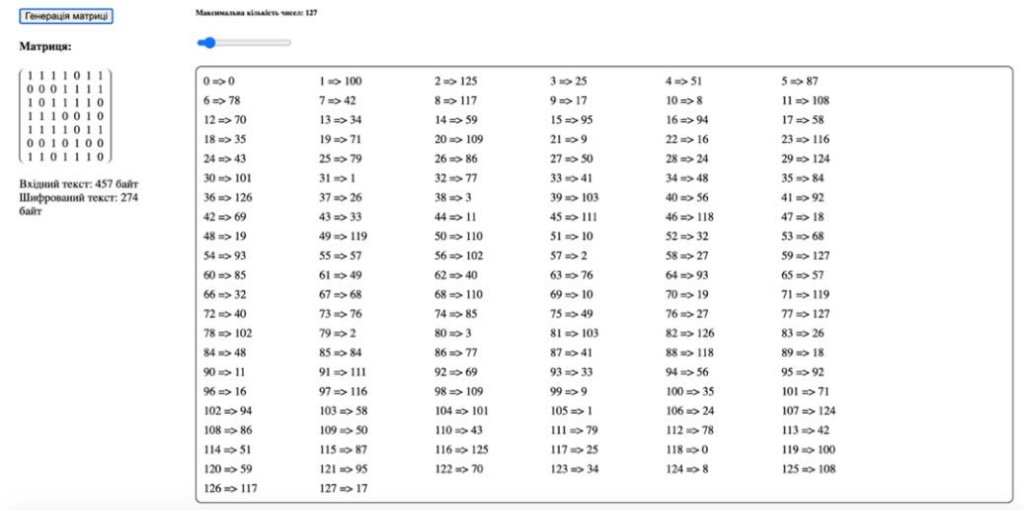

Рис. 2 – Правила побудови авторського шаблону

На рис. 2 показана матриця, згенерована випадковим чином, на основі якої побудовані правила перетворень чисел з заданого діапазону. В даному випадку перетворення здійснювалось над числами в діапазоні від 0 до 127, тобто авторський шаблон містить 128 комірок. Також, на рис. 2 показані результати матричних перетворень чисел з указаного діапазону, які вказують на номери комірок в авторському шаблоні. Авторський шаблон заповнюється на основі статистичного аналізу англомовного тексту. Кількість входжень тієї чи іншої літери в шаблон визначається частотою входження літери в текст. Наприклад, в англомовних текстах найчастіше зустрічається літера «e», відповідно в шаблоні кількість літер «e» буде найбільшою. Такий підхід до статистичного аналізу тексту часто використовують для створення шаблонів шифрування. Зміна матриці та нового тексту для статистичного аналізу дасть змогу отримувати нові варіанти авторських шаблонів, з іншим розміщенням літер.

В результаті обчислень, маємо авторський шаблон, який показаний на рис. 3.

a 0	s 1	u 2	e 3	r 4	i 5	h 6	o 7
g 8	n 9	s 10	l 11	t 12	e 13	a 14	t 15
t 16	e 17	c 18	t 19	h 20	n 21	s 22	l 23
r 24	i 25	h 26	o 27	a 28	s 29	w 30	e 31
e 32	w 33	s 34	a 35	o 36	h 37	i 38	o 39
m 40	r 41	n 42	e 43	t 44	c 45	d 46	t 47
t 48	d 49	e 50	u 51	n 52	r 53	o 54	f 55
o 56	h 57	l 58	p 59	e 60	z 61	s 62	a 63
t 64	d 65	d 66	u 67	m 68	r 69	n 70	e 71
o 72	h 73	i 74	o 75	e 76	w 77	s 78	a 79
e 80	y 81	s 82	a 83	o 84	h 85	k 86	p 87
m 88	r 89	n 90	f 91	t 92	d 93	e 94	u 95
t 96	e 97	a 98	t 99	f 100	n 101	r 102	l 103
q 104	i 105	h 106	o 107	a 108	s 109	u 110	e 111
a 112	t 113	v 114	e 115	r 116	i 117	i 118	o 119
h 120	n 121	s 122	l 123	t 124	e 125	b 126	t 127

Рис. 3 – Авторський шаблон для шифрування інформації

Метод шифрування, який описується, базується на використанні авторських шаблонів, які представляють собою решітки з числовими значеннями. Цей метод шифрування полягає в тому, що на кожному етапі шифрування знаходиться вектор у шаблоні, після чого його позиція та вага зберігаються. В результаті шифрування отримується послідовність пар чисел – вага вектора та зсув вектора, рис. 4.

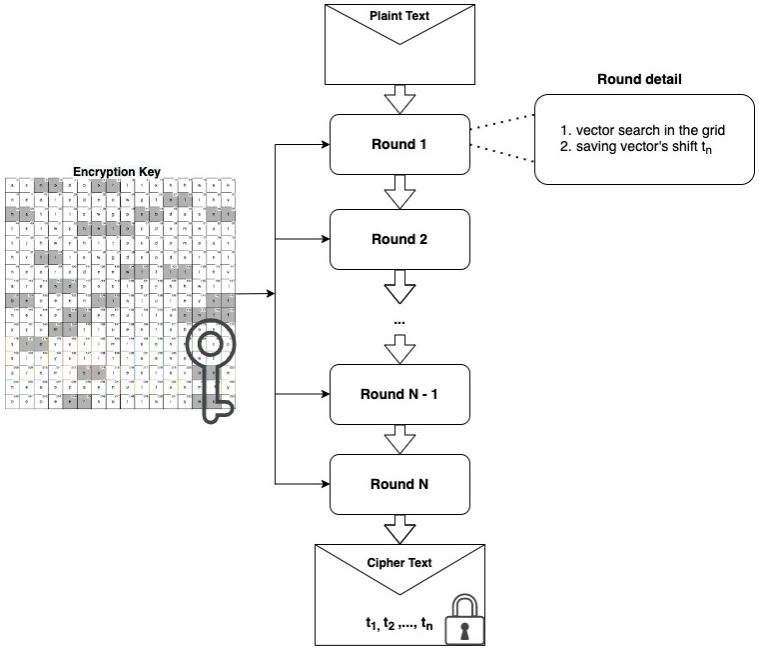

Рис. 4 – Схема методу векторного шифрування

Опис процесу шифрування даного методу можна розбити на кілька етапів:

1) створення авторського шаблону розміром nxn, комірки котрого заповнені літерами англійського алфавіту;

2) розбиття вихідного тексту на вектори – блоки фіксованої довжини, які можуть бути оброблені окремо;

3) застосування авторського шаблону до кожного вектора. Для кожного елемента шаблону знаходиться вектор, що представляє його значення в бінарній формі;

4) для кожного вектора в шаблоні знаходиться його позиція та вага, і ці значення зберігаються в результаті шифрування;

5) послідовність пар чисел – вага вектора та зсув вектора складається в одну послідовність, яка є результатом щифрування.

Результат шифрування запропонованим методом показаний на рис. 5 і представляє собою послідовносіть пар чисел – вага вектора та зсув вектора в авторському шаблоні.

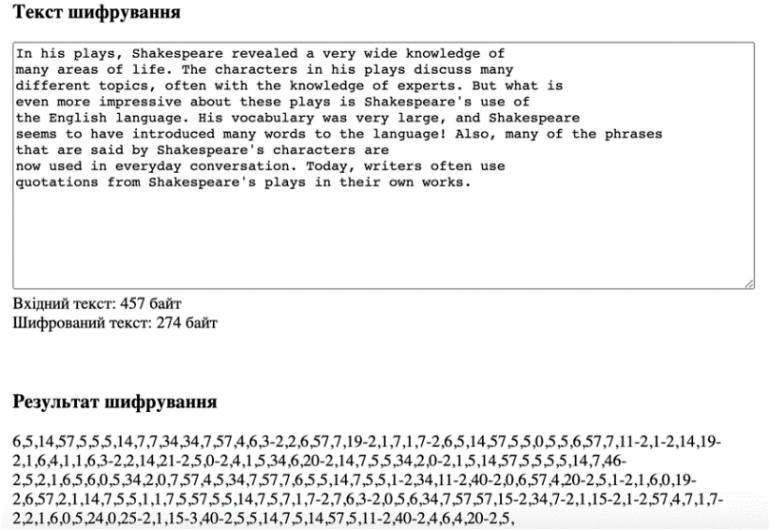

Рис. 5 – Результат шифрування

Як видно з рис. 5, вхідні дані мали розмір 457 байт в результаті шифрування отримали 274 байти, що на 65% менше вхідного тексту.

Для дешифрування використовується збережена послідовність значень – ваги та позиції векторів. Кожен вектор відновлюється з використанням авторського шаблону, а зсув вектора відновлюється з використанням збереженого зсуву.

Для дешифрування зашифрованої послідовності пар чисел необхідно використовувати той самий авторський шаблон, що був використаний при шифруванні. На кожному етапі дешифрування необхідно знайти вектор, відповідний ваговий коефіцієнт та зсув зі шифртексту, і відновити відповідний блок даних.

Крім того, необхідно використовувати обернену матрицю, щоб відновити вихідний блок даних. Якщо використовувати той самий авторський шаблон та обернену матрицю, то можна гарантувати точність відновлення вихідних даних. Процес дешифрування полягає в пошуку відповідного вектора за його вагою та зсувом в авторському шаблоні.

Описаний метод шифрування дозволяє досягти високого рівня інформаційної безпеки за рахунок використання авторських шаблонів зі стійкими криптографічними властивостями. Крім того, використання цього методу дозволяє ефективно стискувати вхідні дані, що є важливим фактором при передачі даних в обмежених умовах, наприклад, при використанні мобільних мереж.

Висновки та перспективи подальшого дослідження. У статті описується новий метод, який поєднує функції шифрування та стиснення, і дозволяє зменшити розмір даних, які необхідно передавати, забезпечуючи їх конфіденційність в одній операції. Застосування цього методу може спростити процес передачі та збереження великих обсягів даних, таких як відео чи аудіофайли, знижуючи час та зусилля, необхідні для їх обробки.

Запропонований метод векторного шифрування із стисненням, що описаний у статті, дозволяє захистити дані від несанкціонованого доступу, зберігаючи при цьому їх цілісність та зменшуючи обсяг пам'яті, необхідної для зберігання даних. Автори статті показують, що за допомогою використання авторського шаблону для знаходження позицій векторів, які утворюють вхідний текст, можна досягти ефективнішого стискання даних та забезпечити їх інформаційну безпеку. Отримана послідовність пар чисел, яка є результатом шифрування, може бути легко розкодована з використанням зворотного процесу, що дозволяє відновити вихідний текст.

Цей метод може знайти своє застосування у багатьох сферах, де зберігаються великі об'єми даних та важлива їх конфіденційність. Він може бути особливо корисним для захисту фінансових даних, медичної інформації та інших важливих даних, що потребують ефективного захисту.

Список бібліографічного опису

1. Baig, M. W., Khan, M. F., and M. A. Raza (2015) Compression-Based Cryptography for Secure Wireless Sensor Networks. Wireless Personal Communications, 4(84), 2559-2572.
2. Ma, Z., Bai, G., and Z. Wang (2018) A Hybrid Compression-Encryption Method for Big Data in Cloud Storage. IEEE Access, 6, 29002-29013.
3. Raigoza, J., & Jituri, K. (2016) Evaluating performance of symmetric encryption algorithms. International conference on computational science and computational intelligence, 1378-1379.
4. Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.
5. Saleem, K., Derhab, A., Orgun, M. A., Al-Muhtadi, J., Rodrigues, J. J., Khalil, M. S., & Ali Ahmed, A. (2016). Cost-effective encryption-based autonomous routing protocol for efficient and secure wireless sensor networks. Sensors, 16(4), 460.
6. Demertzis, I., Talapatra, R., & Papamanthou, C. (2018). Efficient searchable encryption through compression. Proceedings of the VLDB Endowment, 11(11), 1729-1741.
7. Wang, C., Ni, J., & Huang, Q. (2015). A new encryption-then-compression algorithm using the rate–distortion optimization. Signal Processing: Image Communication, 39, 141-150.
8. Kansal, S., & Mittal, M. (2014). Performance evaluation of various symmetric encryption algorithms. International conference on parallel, distributed and grid computing, 105-109.
9. Biswas, M. H., Ali, M. A., Rahman, M., & Sohel, M. M. K. (2019). A systematic study on classical cryptographic cypher in order to design a smallest cipher. Int. J. Sci. Res. Publ, 9(12), 507-511.
10. Грицюк, Ю. І., Грицюк, П. Ю. (2015). Математичні основи процесу генерації ключів перестановки з використанням шифру Кардано. Науковий вісник НЛТУ України, 25(10), 311-323.
11. Jayasankar, U., Thirumal, V., & Ponnurangam, D. (2021). A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications. Journal of King Saud University-Computer and Information Sciences, 33(2), 119-140.
12. Carpentieri, B. (2018). Efficient compression and encryption for digital data transmission. Security and Communication Networks, 112-118.
13. Sharma, R., & Bollavarapu, S. (2015). Data security using compression and cryptography techniques. International Journal of Computer Applications, 117(14).
14. Jiancheng, Q., Yiqin, L., & Yu, Z. (2017). Parallel algorithm for wireless data compression and encryption. Journal of Sensors, 219-230.
15. Kim, S. J., Park, H. J., and Kim, H. J. (2016) A New Encryption Method Using Huffman Coding and One-Time Pad. Journal of Information Processing Systems, 4(12), 627-638.
16. Liu, J., Zhou, T., Zhang, Z., Ke, Y., Lei, Y., & Zhang, M. (2018, December). Digital cardan grille: A modern

approach for information hiding. In Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence, 441-446.
17. Розломій І.О. (2022) Метод побудови матричних решіток Кардано для стиснення інформації. Вісник ХНУ. Технічні науки, 1(305), 85-90.

References

1. Baig, M. W., Khan, M. F., and M. A. Raza (2015) Compression-Based Cryptography for Secure Wireless Sensor Networks. Wireless Personal Communications, 4(84), 2559-2572.
2. Ma, Z., Bai, G., and Z. Wang (2018) A Hybrid Compression-Encryption Method for Big Data in Cloud Storage. IEEE Access, 6, 29002-29013.
3. Raigoza, J., & Jituri, K. (2016) Evaluating performance of symmetric encryption algorithms. International conference on computational science and computational intelligence, 1378-1379.
4. Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.
5. Saleem, K., Derhab, A., Orgun, M. A., Al-Muhtadi, J., Rodrigues, J. J., Khalil, M. S., & Ali Ahmed, A. (2016). Cost-effective encryption-based autonomous routing protocol for efficient and secure wireless sensor networks. Sensors, 16(4), 460.
6. Demertzis, I., Talapatra, R., & Papamanthou, C. (2018). Efficient searchable encryption through compression. Proceedings of the VLDB Endowment, 11(11), 1729-1741.
7. Wang, C., Ni, J., & Huang, Q. (2015). A new encryption-then-compression algorithm using the rate–distortion optimization. Signal Processing: Image Communication, 39, 141-150.
8. Kansal, S., & Mittal, M. (2014). Performance evaluation of various symmetric encryption algorithms. International conference on parallel, distributed and grid computing, 105-109.
9. Biswas, M. H., Ali, M. A., Rahman, M., & Sohel, M. M. K. (2019). A systematic study on classical cryptographic cypher in order to design a smallest cipher. Int. J. Sci. Res. Publ, 9(12), 507-511.
10. Gryciuk Yu.I. & Grytsyuk P.Yu. (2015) Mathematical Foundations of the generation of keys using a permutation cipher Cardano. Scientific Bulletin of UNFU, 25(10), 311-323.
11. Jayasankar, U., Thirumal, V., & Ponnurangam, D. (2021). A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications. Journal of King Saud University-Computer and Information Sciences, 33(2), 119-140.
12. Carpentieri, B. (2018). Efficient compression and encryption for digital data transmission. Security and Communication Networks, 112-118.
13. Sharma, R., & Bollavarapu, S. (2015). Data security using compression and cryptography techniques. International Journal of Computer Applications, 117(14).
14. Jiancheng, Q., Yiqin, L., & Yu, Z. (2017). Parallel algorithm for wireless data compression and encryption. Journal of Sensors, 219-230.
15. Kim, S. J., Park, H. J., and Kim, H. J. (2016) A New Encryption Method Using Huffman Coding and One-Time Pad. Journal of Information Processing Systems, 4(12), 627-638.
16. Liu, J., Zhou, T., Zhang, Z., Ke, Y., Lei, Y., & Zhang, M. (2018, December). Digital cardan grille: A modern approach for information hiding. In Proceedings of the 2018 2nd International Conference on Computer Science and Artificial Intelligence, 441-446.
17. Rozlomii, I.O. (2022) Method of construction matrix Cardano's grids for compression of information. KHNU Bulletin: Technical Sciences, 1(305), 85-90.