DOI 10.31891/2307-5732-2023-321-3-308-313
УДК 681.3.05:004.056

РОЗЛОМІЙ ІННА
Черкаський національний університет імені Богдана Хмельницького
ORCID ID: 0000-0001-5065-9004
e-mail: inna-roz@ukr.net
НАУМЕНКО СЕРГІЙ
Черкаський національний університет імені Богдана Хмельницького
ORCID ID: 0000-0002-6337-1605
e-mail: naumenko.serhii1122@vu.cdu.edu.ua

ШИФРУВАННЯ ТА СТИСНЕННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ АВТОРСЬКИХ ШАБЛОНІВ, КЕРОВАНИХ МАТРИЦЕЮ

Стаття присвячена розробці нового підходу до побудови авторських шаблонів для задач шифрування та стиснення інформації. Використання авторських шаблонів забезпечує безпечний та ефективний спосіб шифрування та стиснення інформації, оскільки вони надають унікальний прототип шифрувального трафарету, який може використовуватись для широкого спектру застосувань.

Запропонований метод побудови авторських шаблонів базується на статистичному аналізі англомовних текстів та використанні модулярних криптографічних перетворень чисел з заданого діапазону. Побудований авторський шаблон є прототипом шифрувального трафарету. Авторський шаблон забезпечує безпечний спосіб шифрування та стиснення інформації, оскільки символи розподіляються випадковим способом, що ускладнює дешифрування та розпакування інформації неавторизованими користувачами.

Ключові слова: шифрувальний трафарет, авторський шаблон, решітка Кардано, шифрування, стиснення інформації, матричні криптографічні перетворення.

ROZLOMII INNA, NAUMENKO SERHII
Bohdan Khmelnytsky National University of Cherkasy

METHOD OF BUILDING PROPRIETARY TEMPLATES FOR INFORMATION ENCRYPTION AND COMPRESSION TASKS

The article presents a novel approach to building author's templates for encryption and compression tasks. The use of author's templates provides a secure and efficient way of encrypting and compressing information, as they offer a unique prototype for cipher templates that can be used for a wide range of applications. The proposed method for constructing author's templates is based on a statistical analysis of English language texts and the use of modular cryptographic transformation of numbers from a given range. The approach involves breaking down the text into smaller chunks and analyzing the frequency of occurrence of letters and combinations of letters within each chunk. The results of this analysis are then used to construct a matrix that determines the rules for distributing symbols in the author's template. The constructed author's template is a prototype of a cipher template and is similar to the Cardano's grid. The author's template provides a secure way of encrypting and compressing information, as the symbols are distributed in a random and unique way, making it difficult for unauthorized parties to decipher or decompress the information.

The proposed method allows for the creation of author's templates for a wide range of encryption and compression tasks. The input data for constructing author's templates are an English language text and a matrix that determines the rules for distributing symbols in the author's template. Changing the input data allows for the creation of new author's templates that can be tailored to specific applications or requirements.

In conclusion, the method presented in this article offers a unique and efficient way of constructing author's templates for encryption and compression tasks. The use of author's templates provides a secure and reliable way of encrypting and compressing information, making it an ideal solution for applications that require secure data transmission and storage.

Keywords: encryption stencil, author's template, Cardano's grid, encryption, information compression, matrix cryptographic transformations.

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

В сучасному світі інформація стала однією з найцінніших ресурсів, що відіграє важливу роль в різних сферах діяльності. Проте, з поширенням інтернету та швидким розвитком технологій, конфіденційність та цілісність інформації стали питаннями надзвичайної важливості. Необхідність забезпечення конфіденційності і цілісності інформації виникає в багатьох сферах діяльності, починаючи від банківської сфери і закінчуючи сферою медицини та науки. При передачі конфіденційної інформації, такої як фінансові дані, медичні записи чи дослідження, важливо забезпечити її конфіденційність та цілісність, щоб уникнути можливих наслідків, таких як крадіжка особистої інформації, порушення прав на інтелектуальну власність та інші [1–3].

Більшість існуючих методів шифрування та стискання інформації не завжди ефективні та безпечні та мають обмеження, які можуть бути використані для зламування шифрування, а також вони можуть не забезпечувати ефективного стискання даних. Методи стиснення даних можуть бути неефективними для великих файлів, і методи шифрування можуть бути піддані атакам з використанням потужних комп'ютерів. Також деякі методи можуть вимагати велику кількість ресурсів для розшифрування даних, що затримує роботу. Стиснення даних є не менш важливою проблемою в сучасному світі, оскільки кількість даних, що зберігається та передається, зростає з кожним роком. Стиснення даних дозволяє зменшити розмір файлів та зберігати більше даних на меншому просторі, що зменшує вартість зберігання та передачі даних.

Отже, постановка проблеми полягає в тому, що необхідно розробити новий метод шифрування та стиснення даних, який буде надійним та ефективним, тобто матиме високу стійкість до різноманітних атак, а також зменшувати обсяг даних без втрати інформації. Для вирішення цієї проблеми в статті запропоновано новий метод, який базується на розробці авторських шаблонів для задач шифрування та стискання інформації.

Аналіз досліджень та публікацій

Безпека та стиснення даних є загальною вимогою для більшості програм, пов'язаних із зберіганням і передачею інформації. З метою забезпечення надійного зберігання та безпеки інформації, необхідно використовувати методи шифрування та стиснення. Застосування цих методів дозволяє зменшити ризики крадіжки даних та втрати конфіденційної інформації. В [4] представлено метод вибіркового шифрування для шифрування текстових даних. Особливість даного методу полягає в його невизначеності – для процесу шифрування даних він вибирає лише важливі дані з усього повідомлення. Це, у свою чергу, зменшує витрати часу на шифрування та підвищує продуктивність. Частина шифрування виконується за допомогою алгоритму симетричного ключа. Для цього використовується алгоритм BLOWFISH.

Авторами [5] запропоновано гібридний алгоритм стиснення даних збільшує вхідні дані, які потрібно зашифрувати за допомогою методу криптографії RSA, щоб підвищити рівень безпеки. Цю техніку можна використовувати, щоб зменшити кількість переданих даних в умовах слабкого Інтернету чи недостатніх можливостях запам'ятовуючих пристроїв. Звичайний текст стискається за допомогою алгоритму кодування Хаффмана, молодший біт LSB використано для імплантації зашифрованих даних.

В [6] запропоновано варіант адаптивного арифметичного кодування, що додає криптографічні функції до цього класичного методу стиснення. Ідея полягає в тому, щоб виконувати оновлення частотних таблиць для символів основного алфавіту вибірково, відповідно до деякого випадково вибраного секретного ключа *K*. Натомість, автори [7] пропонують послідовне виконання етапів стиснення та шифрування інформації та проводять в своїй роботі порівняльний аналіз різних комбінацій технік стиснення та шифрування.

В [8] автори застосовують перетворення зашифрованого тексту для стиснення з метою використання в пристроях з обмеженими ресурсами, такими як IoT, смарт-карти та програми RFID. В статті запропонована техніка решітчастого стиснення зменшує розмір зашифрованого тексту більш ніж на 40%, а також забезпечує криптографію з відкритим ключем на раніше недоступних полегшених шифрах.

Особливої уваги заслуговує робота [9], в якій представлено новий метод багаторівневої безпеки та стиснення текстових даних із використанням бітової вставки та кодування Хаффмана. Запропонований метод містить різні модулі обробки для захисту та стиснення текстових даних за допомогою процесу шифрування. Середній відсоток скорочення або зменшення пам'яті становить 45,41%.

Формулювання цілей статті

Стиснення даних та їх шифрування – дві технології, які дозволяють ефективно зменшити витрати на зберігання та передачу інформації. Стиснення передбачає перетворення даних з джерела повідомлення до меншого формату – кодового слова, тим самим зменшуючи кількість бітів, які потрібно зберегти або передати. Зокрема, стиснення даних без втрат застосовується для стиснення будь-яких текстових даних, що дозволяє ефективно зменшити їх обсяг [10–13]. Шифрування, зі свого боку, захищає дані від підслуховування, перетворюючи відкритий текст у зашифрований за допомогою ключа шифрування. Однак, наразі методи стиснення та шифрування застосовуються окремо, що може призвести до певних проблем, таких як великий час обробки та вартість. Щоб подолати ці недоліки, використовують поєднання обох технологій в один процес.

Метою роботи є побудова авторського шаблону, який би дозволяв одночасно шифрувати та стискати інформацію. Для досягнення цієї мети пропонується використання решітки Кардано, але з рядом модифікацій.

Виклад основного матеріалу

З огляду на швидкий розвиток технологій та інформаційної сфери, питання, пов'язані з інформаційною безпекою, стають все актуальнішими. Знання засобів захисту інформації є необхідними для ефективної організації процесу передачі та зберігання конфіденційної інформації. Перестановочні шифри з шифрувальними решітками є одним з методів шифрування, що застосовуються для збереження конфіденційності даних [14–17]. Цей метод полягає у переставленні символів відкритого тексту у певному порядку, що визначається шифрувальною решіткою. Результатом цього процесу є шифртекст, який може бути розшифрований лише за наявності відповідної шифрувальної решітки.

Шифрувальна решітка – трафарет з вирізаними комірками, який використовувався для шифрування відкритого тексту наприкінці шістнадцятого століття. Найвідомішою шифрувальною решіткою є решітка Кардано [18]. Вона представляє собою прямокутний трафарет з вирізаними комірками, в які записувались окремі букви, склади, слова. Фрагменти записаного в комірки відкритого тексту додатково маскувались буквами, складами, якими заповнювали порожні проміжки між текстом, який потрібно було зашифрувати. Принцип шифрування простою решіткою Кардано показаний на рис. 1.

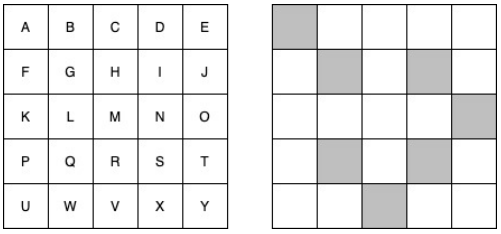

Рис. 1. Шифр перестановки на основі простої решітки Кардано

Решітка Кардано може бути простою, як показано на рис. 1, або симетрично-поворотною – рис. 2. На відміну від простої решітки, яка є прямокутною, симетрично-поворотна решітка – квадратна. Таку решітку-трафарет можна застосовувати декілька разів, повертаючи трафарет навколо центру. Симетрично-поворотна решітка Кардано дозволяє записати текст масивом символів так, що результат виглядатиме цілком незрозуміло для читання, тому такий варіант решітки володіє більшою криптографічною стійкістю ніж проста решітка Кардано.

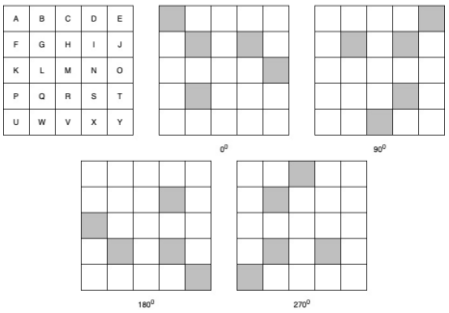

Рис. 2. Шифр перестановки на основі симетрично-поворотної решітки Кардано

В більш пізніх варіантах решітки Кардано виникають проблеми, які є загальними для всіх транспозиційних шифрів. Для всіх шифрів маршрутної перестановки характерною є невисока криптостійкість. Оскільки інформація заноситься в комірки-отвори решітки, важливим є розміщення цих комірок. Розміщення комірок-отворів отримаємо за допомогою застосування операцій матричного криптографічного перетворення.

Запропонований метод базується на принципах шифрувальної решітки Кардано. Основна ідея полягає в тому, що шифрувальний трафарет використовується для зміни порядку букв у тексті, а також для стиснення даних. Таким чином, обсяг даних може бути зменшений без втрати інформації. Крім того, розроблений метод може бути використаний для побудови надійних систем шифрування та стиснення даних. Для побудови решітки був використаний статистичний аналіз текстів, що дозволяє визначити кількість повторень кожної букви в тексті, а також їхній розподіл. Це дає змогу оптимізувати розмір шифрованого тексту та забезпечити стійкість до різноманітних атак. Для опису алгоритму формування авторського шаблону було визначено наступну послідовність дій:

1. Провести частотний аналіз англомовного тексту та обчислити кількість входжень кожної букви в шаблон, рис. 3.

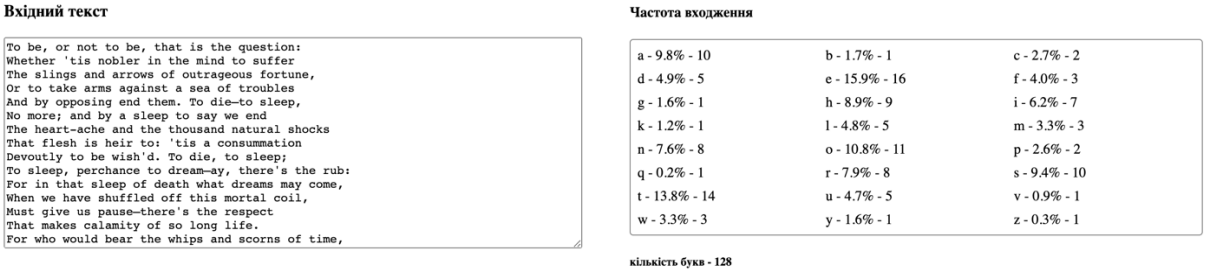

Рис. 3. Результат частотного аналізу англомовного тексту

2. Згенерувати випадковим чином матрицю та виконати матричні криптографічні перетворення [19] для чисел у діапазоні від 0 до 128.

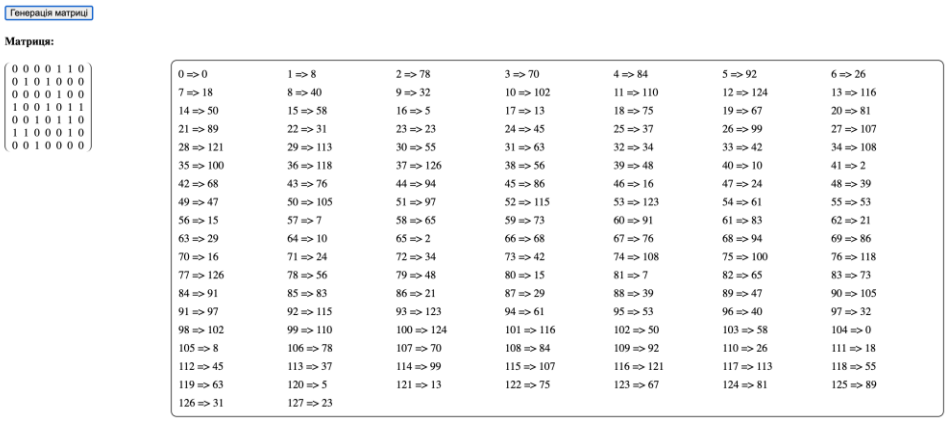

Рис. 4. Результати матричних криптографічних перетворень чисел

3. За результатами матричного криптографічного перетворення чисел 0…128 заповнити комірки авторського шаблону, відповідно до кількості входжень кожної літери, рис. 5.

t 0	n 2	u 5	o 7	t 8	n 10	u 13	o 15
n 16	t 18	r 21	z 23	o 24	t 26	r 29	y 31
s 32	o 34	t 37	r 39	s 40	o 42	t 45	r 47
o 48	s 50	s 53	u 55	o 56	t 58	s 61	u 63
p 65	w 67	n 68	t 70	p 73	v 75	n 76	t 78
w 81	r 83	t 84	n 86	w 89	q 91	t 92	n 94
r 97	t 99	o 100	s 102	r 105	t 107	o 108	s 110
u 113	r 115	s 116	o 118	t 121	s 123	s 124	o 126

Рис. 5. Заповнений авторський шаблон

Авторський шаблон є керованим матрицею, оскільки саме матриця визначає правила розташування літер. Це означає, що кожна матриця, що генерується випадковим чином, надає унікальний авторський шаблон.

За допомогою матриці, можна створити безліч різних авторських шаблонів, які будуть відрізнятися один від одного розташуванням літер в решітці.

На рис. 5 показано принцип шифрування текстової інформації із застосуванням авторського шаблону. Результатом шифрування є послідовність пар чисел, що складаються з зсуву та кількості літер, що повторюються в авторському шаблоні.

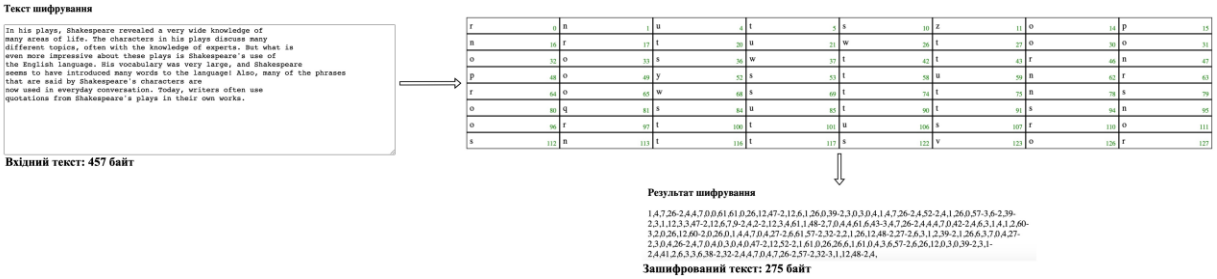

Рис. 6. Принцип шифрування текстової інформації із застосуванням авторського шаблону

Стаття пропонує новий метод шифрування та стиснення даних, який базується на розробці авторських шаблонів. Ідея створення авторського шаблону була заснована на концепції шифрувальної решітки Кардано. Використання цієї ідеї дозволило створити надійний та ефективний авторський шаблон. Запропонований метод використовує трафарет шифрування, що був розроблений на основі статистичного аналізу тексту. Крім шифрування запропонований метод дозволяє стискати дані. Як видно з рис. 6, результат шифрування на 65: менший за вихідний текст. Згідно з результатами досліджень, запропонований метод шифрування та стиснення даних має кілька переваг порівняно з іншими методами. Зокрема, він ефективно працює з текстовими даними та вимагає меншої кількості ресурсів для шифрування та розшифрування.

Висновки та перспективи подальшого дослідження. Таким чином, запропонований метод побудови авторських шаблонів є ефективним та перспективним інструментом для задач шифрування та стиснення інформації. Використання цього методу дозволяє зберігати конфіденційність та цілісність даних, що є особливо важливим в сучасному світі, де обмін інформацією здійснюється в масштабах, небачених раніше.

У загальному, стаття пропонує новий метод шифрування та стискання інформації, який має потенціал для використання в різних галузях, включаючи безпеку даних, зберігання та передачу інформації.

Результати дослідження можуть бути корисні для вдосконалення технологій шифрування та стискання даних у майбутньому. Також метод побудови авторських шаблонів може знайти застосування в інших галузях, де важливо зберігати конфіденційність та цілісність даних. Наприклад, його можна використовувати в системах безпеки інформації, в банківській сфері, в телекомунікаційних мережах тощо.

Література

1. Yassein M. B., Aljawarneh S., Qawasmeh E., Mardini W., Khamayseh Y. (2017). Comprehensive study of symmetric key and asymmetric key encryption algorithms. In 2017 international conference on engineering and technology, 1–7.

2. Koko S. O. F. M., Babiker A. (2015). Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication. IOSR Journal of Computer Engineering (IOSR-JCE), 17(1), 62–69.

3. Teng L., Li H., Yin S., Sun Y. (2020). A Modified Advanced Encryption Standard for Data Security. Int. J. Netw. Secur., 22(1), 112–117.

4. Kushwaha A., Sharma H. R., Ambhaikar A. (2016). A novel selective encryption method for securing text over mobile ad hoc network. Procedia Computer Science, 79, 16–23.

5. Wahab O. F. A., Khalaf A. A., Hussein A. I., Hamed H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. IEEE access, 9, 31805-31815.

6. Klein S. T., Shapira D. (2021). Integrated encryption in dynamic arithmetic compression. Information and Computation, 279, 104617.

7. Sharma R., Bollavarapu S. (2015). Data security using compression and cryptography techniques. International Journal of Computer Applications, 117(14).

8. Saarinen M. J. O. (2017, April). Ring-LWE ciphertext compression and error correction: Tools for lightweight post-quantum cryptography. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, 15-22.

9. Kodabagi M. M., Jerabandi M. V., Gadagin N. (2015). Multilevel security and compression of text data using bit stuffing and huffman coding. In 2015 International Conference on Applied and Theoretical Computing and Communication Technology, 800–804.

10. Лебіга М.М., Пасічник О.А., Скрипник Т.К., Медвчедчук В.В. (2019). Комбінований алгоритм стиснення даних, представлених в текстовому форматі. Вісник ХНУ. Технічні науки. 6(279), 131–133.

11. Кулібаба С.О., Курченко О.А. (2022). Криптографічний метод шифрування даних Pattern reverse multiplication. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 216–223.

12. Kaur A. (2017). A Review on Symmetric Key Cryptography Algorithms. International Journal of Advanced Research in Computer Science, 8(4).

13. Jha D. P., Kohli R., Gupta A. (2016). Proposed encryption algorithm for data security using matrix properties. In 2016 International conference on innovation and challenges in cyber security, 86-90.

14. Sajay K. R., Babu S. S., Vijayalakshmi Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. Journal of Ambient Intelligence and Humanized Computing, 1–10.

15. Gupta H., Sharma V. K. (2013). Multiphase encryption: A new concept in modern cryptography. International Journal of Computer Theory and Engineering, 5(4), 638.

16. 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.

17. Mushtaque M. A., Dhiman H., Hussain S. (2014). A hybrid approach and implementation of a new encryption algorithm for data security in cloud computing. International Research Publication House, 7, 669–675.

18. 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.

19. Розломій І.О. (2022). Метод побудови матричних решіток Кардано для стиснення інформації. Вісник ХНУ. Технічні науки, 1(305), 85–90.

References

1. Yassein M. B., Aljawarneh S., Qawasmeh E., Mardini W., Khamayseh Y. (2017). Comprehensive study of symmetric key and asymmetric key encryption algorithms. In 2017 international conference on engineering and technology, 1–7.

2. Koko S. O. F. M., Babiker A. (2015). Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication. IOSR Journal of Computer Engineering (IOSR-JCE), 17(1), 62–69.

3. Teng L., Li H., Yin S., Sun Y. (2020). A Modified Advanced Encryption Standard for Data Security. Int. J. Netw. Secur., 22(1), 112–117.

4. Kushwaha A., Sharma H. R., Ambhaikar A. (2016). A novel selective encryption method for securing text over mobile ad hoc network. Procedia Computer Science, 79, 16–23.

5. Wahab O. F. A., Khalaf A. A., Hussein A. I., Hamed H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. IEEE access, 9, 31805-31815.

6. Klein S. T., Shapira D. (2021). Integrated encryption in dynamic arithmetic compression. Information and Computation, 279, 104617.

7. Sharma R., Bollavarapu S. (2015). Data security using compression and cryptography techniques. International Journal of Computer Applications, 117(14).

8. Saarinen M. J. O. (2017, April). Ring-LWE ciphertext compression and error correction: Tools for lightweight post-quantum cryptography. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, 15-22.

9. Kodabagi M. M., Jerabandi M. V., Gadagin N. (2015). Multilevel security and compression of text data using bit stuffing and huffman coding. In 2015 International Conference on Applied and Theoretical Computing and Communication Technology, 800–804.

10. Lebiga M., Pasichnyk T., Skrypnyk T., Medvedchuk, V. (2019). Combided text data compression algorithm. Herald of Khmelnytskyi national university, 6 (279), 131–133.

11. Kulibaba S., Kurchenko O. (2022). Cryptography data encryption method Pattern reverse multiplication. Electronic professional scientific publication «Cybersecurity: education, science, technology», 3(15), 216–223.

12. Kaur A. (2017). A Review on Symmetric Key Cryptography Algorithms. International Journal of Advanced Research in Computer Science, 8(4).

13. Jha D. P., Kohli R., Gupta A. (2016). Proposed encryption algorithm for data security using matrix properties. In 2016 International conference on innovation and challenges in cyber security, 86–90.

14. Sajay K. R., Babu S. S., Vijayalakshmi Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. Journal of Ambient Intelligence and Humanized Computing, 1–10.

15. Gupta H., Sharma V. K. (2013). Multiphase encryption: A new concept in modern cryptography. International Journal of Computer Theory and Engineering, 5(4), 638.

16. 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.

17. Mushtaque M. A., Dhiman H., Hussain S. (2014). A hybrid approach and implementation of a new encryption algorithm for data security in cloud computing. International Research Publication House, 7, 669–675.

18. Gryciuk Y., Grytsyuk P. (2016). Implementation details for the cipher key generation Cardano permutation. In 2016 13th international conference on modern problems of radio engineering, telecommunications and computer science, 498–502.

19. Rozlomii I.O. (2022) Method of construction matrix Cardano's grids for compression of information. KHNU Bulletin: Technical Sciences, 1(305), 85–90.