



International Science Group

ISG-KONF.COM

VI

**INTERNATIONAL SCIENTIFIC
AND PRACTICAL CONFERENCE
"METHODICAL AND PRACTICAL METHODS OF
CREATING INVENTIONS"**

Sofia, Bulgaria

October 24 - 27, 2023

ISBN 979-8-89145-192-6

DOI 10.46299/ISG.2023.2.6

METHODICAL AND PRACTICAL METHODS OF CREATING INVENTIONS

Proceedings of the VI International Scientific and Practical Conference

Sofia, Bulgaria
October 24 – 27, 2023

UDC 01.1

The 6th International scientific and practical conference “Methodical and practical methods of creating inventions” (October 24 – 27, 2023) Sofia, Bulgaria. International Science Group. 2023. 282 p.

ISBN – 979-8-89145-192-6

DOI – 10.46299/ISG.2023.2.6

EDITORIAL BOARD

<u>Pluzhnik Elena</u>	Professor of the Department of Criminal Law and Criminology Odessa State University of Internal Affairs Candidate of Law, Associate Professor
<u>Liudmyla Polyvana</u>	Department of Accounting and Auditing Kharkiv National Technical University of Agriculture named after Petr Vasilenko, Ukraine
<u>Mushenyk Iryna</u>	Candidate of Economic Sciences, Associate Professor of Mathematical Disciplines, Informatics and Modeling. Podolsk State Agrarian Technical University
<u>Prudka Liudmyla</u>	Odessa State University of Internal Affairs, Associate Professor of Criminology and Psychology Department
<u>Marchenko Dmytro</u>	PhD, Associate Professor, Lecturer, Deputy Dean on Academic Affairs Faculty of Engineering and Energy
<u>Harchenko Roman</u>	Candidate of Technical Sciences, specialty 05.22.20 - operation and repair of vehicles.
<u>Belei Svitlana</u>	Ph.D., Associate Professor, Department of Economics and Security of Enterprise
<u>Lidiya Parashchuk</u>	PhD in specialty 05.17.11 "Technology of refractory non-metallic materials"
<u>Levon Mariia</u>	Candidate of Medical Sciences, Associate Professor, Scientific direction - morphology of the human digestive system
<u>Hubal Halyna Mykolaivna</u>	Ph.D. in Physical and Mathematical Sciences, Associate Professor

PSYCHOLOGY		
42.	Diachkova O., Barmina S. PECULIARITIES OF PSYCHOLOGICAL ASSISTANCE PROVIDING TO VICTIMS WHO HAVE SUFFERED FROM THE WAR	196
43.	Нечипорук К.О. СУЧАСНІ СТРАТЕГІЇ ПСИХОЛОГІЧНОЇ ТЕРАПІЇ ПТСР У ВІЙСЬКОВИХ ПІД ЧАС НАДАННЯ СПЕЦИФІЧНОЇ МЕДИЧНОЇ ДОПОМОГИ. ПОРІВНЯННЯ СВІТОВОГО ТА УКРАЇНСЬКОГО ДОСВІДІВ	199
44.	Ташматов В.А., Костів Л.А. МЕТОД "ЛАБІРИНТУ" У ЗООПСИХОЛОГІЇ	204
TECHNICAL SCIENCES		
45.	Akbarova S. ENHANCING THE ACCURACY OF COORDINATE MEASUREMENT RESULTS	206
46.	Melnykova N., Chereschchuk L. APPLICATION OF MACHINE LEARNING METHODS FOR PREDICTING THE RISK OF STROKE OCCURRENCE	210
47.	Melnykova N., Kukhar Y. RECOMMENDATION SYSTEM FOR SELECTION OF RECIPES BY USING ARTIFICIAL INTELLIGENCE	217
48.	Бганцов Є. ШИФРУВАННЯ ДАНИХ. ОПИС ТА СТРУКТУРА АЛГОРИТМУ СИМЕТРИЧНОГО ШИФРУВАННЯ AES	222
49.	Вовк О.Б., Бурцьо О.Ю. ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ РЕКОМЕНДАЦІЙ ЯК ЧАСТИНА ТАРГЕТОВАНОЇ РЕКЛАМИ ДЛЯ ПРОСУВАННЯ БІЗНЕСУ	226
50.	Головко В., Штофель О., Красиков І. ФРАКТАЛЬНІ ЗАМІРИ СТРУКТУРИ МЕТАЛУ ЗВАРНИХ ШВІВ. Ч.3*	230

ШИФРУВАННЯ ДАНИХ. ОПИС ТА СТРУКТУРА АЛГОРИТМУ СИМЕТРИЧНОГО ШИФРУВАННЯ AES

Бганцов Євгеній,
здобувач вищої освіти кафедри інформатики
Харківський національний університет радіоелектроніки

Шифрування є однією з ключових складових сучасного світу інформаційної безпеки. Воно використовується для захисту конфіденційності даних, забезпечення цілісності і перевірки автентичності інформації. У світі, де обмін даними відбувається нашвидкуруч та величезними обсягами, забезпечення безпеки цих даних стає надзвичайно важливим завданням. Шифрування – це основний інструмент, який допомагає нам досягнути цієї безпеки.

Розглянемо метод шифрування AES – абревіатура від Advanced Encryption Standard. Має нову архітектуру SQUARE, для якої характерно: представлення блоку, що шифрується, у вигляді двовимірного байтового масиву; шифрування за один раунд всього блоку даних (байт-орієнтована структура); виконання криптографічних перетворень як над окремими байтами масиву, так і над його рядками і стовпцями [1]. Це забезпечує дифузцію даних одночасно у двох напрямках - по рядках та по стовпцях.

Загальні характеристики AES:

- AES зашифровує та розшифровує 128-бітові блоки даних;
- AES дозволяє використовувати три різні ключі довжиною 128, 192 або 256 біт (залежно від довжини ключа версії шифру позначають AES-128, AES-192 або AES-256);
- від розміру ключа залежить кількість раундів шифрування: довжина 128 біт – 10 раундів; довжина 192 біта – 12 раундів; довжина 256 біт – 14 раундів;
- усі раунди, крім останнього, однакові [2, 3].

Як зазначалося, в версії алгоритму AES-128 ключ шифру складається з 128 бітів, поділених на 16 байтів $k_0, k_1, \dots, k_{15}$, і записується в стовпці матриці InputKey. Кожен стовпець матриці InputKey утворює слово, тобто. фактично ключ шифру – це чотири слова w_0, w_1, w_2, w_3 , де $w_0 = k_0 k_1 k_2 k_3$, $w_1 = k_4 k_5 k_6 k_7$ і т.д. [4].

Приклад матриці наведений на рисунку 1.

З цих слів за допомогою спеціального алгоритму утворюється послідовність із 44 слів: $w_0, w_1, w_2, \dots, w_{43}$ (кожне слово по 32 біти).

На кожен раунд шифрування подаються чотири слова цієї послідовності. Вони й відіграватимуть роль раундового ключа. Схема перетворення даних показана рисунку 2.

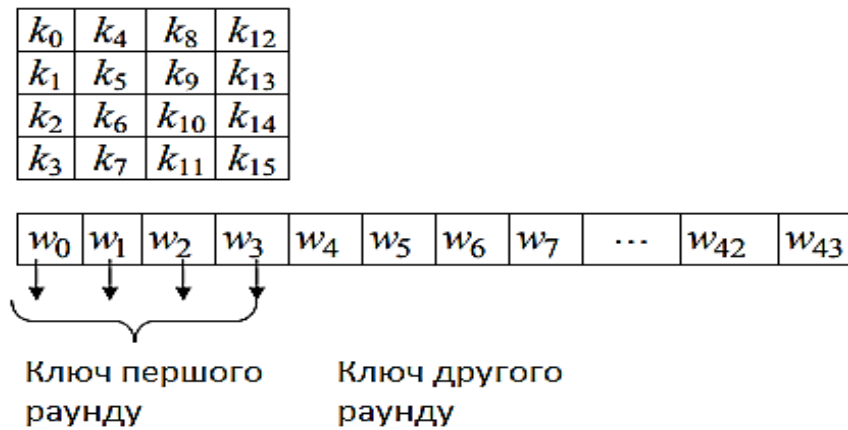


Рисунок 1 – Матриця InputKey

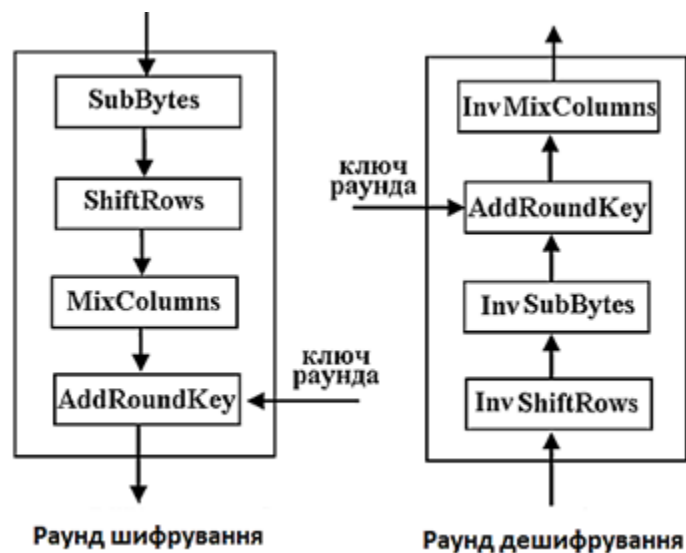


Рисунок 2 – Схема перетворення даних

Перед першим раундом виконується операція AddRoundKey (підсумовування за модулем 2 з початковим ключем шифру). Перетворення, виконані одному раунді, позначають Round(State, RoundKey), де змінна State – матриця, що описує дані на вході раунду і його виході після шифрування; змінна RoundKey – матриця, яка містить раундовий ключ.

Раунд складається з 4 різних перетворень: SubBytes – побайтова підстановка у S-боксі з фіксованою таблицею заміन; ShiftRows – побайтове зсув рядків матриці State на різну кількість байт; MixColumns – перемішування байт у стовпцях; AddRoundKey – додавання з раундовим ключем (операція XOR).

Останній раунд дещо відрізняється від попередніх тим, що не використовує функцію MixColumns. Приклад операції AddRoundKey наведений на рисунку 3.

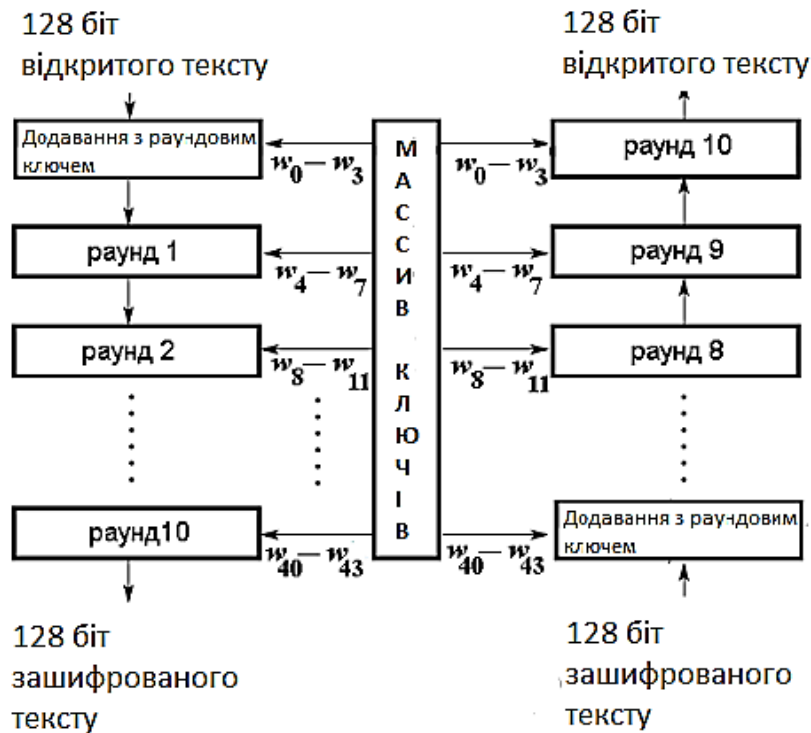


Рисунок 3 – Операція AddRoundKey

При дешифруванні в кожному раунді виконуються зворотні операції: InvShiftRows, InvSubBytes, AddRoundKey та InvMixColumns (у позначках перед назвою функції з'являється приставка Inv). Порядок виконання операцій при шифруванні та дешифруванні різний, причини чого будуть зрозумілі після детального розгляду кожного перетворення [5].

Метод симетричного шифрування AES представляє приклад сучасної криптографії, який надійно захищає конфіденційність та цілісність інформації. Цей стандарт шифрування, прийнятий у всьому світі, забезпечує високий рівень безпеки і оптимізовану швидкість обробки даних [6-17], що робить його ідеальним вибором для багатьох застосувань.

Список літератури:

1. Christof Paar and Jan Pelzl (2009). Understanding Cryptography: A Textbook for Students and Practitioners.
2. Lars R. Knudsen (2011). The Block Cipher Companion.
3. Bernard Menezes (2018). Cryptography and Network Security: Principles and Practice.
4. Yakymenko I., Kasyanchuk M., Nykolajchuk Y. (2010) Matrix algorithms of processing of the information flow in computer systems based on theoretical and numerical Krestenson's basis. *Proceedings of the X-th International Conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET-2010)*. Lviv-Slavske. p. 241.
5. Yang L. L., Hanzo L. (2001) Minimum-distance decoding of redundant residue number system codes. *Proc. IEEE ICC '2001. Helsinki (Finland)*. pp. 2975-2979.

6. Gorokhovatskiy, V.A. (2011) Compression of Descriptions in the Structural Image Recognition, *Telecommunications and Radio Engineering*, Vol. 70, No. 15, pp. 1363–1371.
7. Gorokhovatsky V.A. Putyatin Y. P. (2009) Image Likelihood Measures of the Basis of the Set of Conformities. *Telecommunications and Radio Engineering*, 68 (9), p. 763–778.
8. Gorokhovatskyi, V., Vlasenko, N. (2021) Редукція опису зображення у складі множини дескрипторів на основі метричного критерію інформативності. *Advanced Information Systems*, 5(4), pp. 10–16.
9. Gadetska, S. V., Gorokhovatskyi, V. O. (2018) Statistical measures for computation of the image relevance of visual objects in the structural image classification methods. *Telecommunications and Radio Engineering*, 77(12), pp. 1041–1053.
10. Pomazan V., Tvoroshenko I., and Gorokhovatskyi V. (2023) Handwritten character recognition models based on convolutional neural networks, *International Journal of Academic Engineering Research*, 7(9), pp. 64–72.
11. Gorokhovatskyi, V., Tvoroshenko, I., Kobylin, O., Vlasenko, N. (2023) Search for Visual Objects by Request in the Form of a Cluster Representation for the Structural Image Description. *Advances in Electrical and Electronic Engineering*, 21(1), pp. 19–27.
12. Гороховатский В.А. Структурный анализ и интеллектуальная обработка данных в компьютерном зрении: монография, Комп. СМИТ, 2014. 316 с.
13. Гороховатський В., Творошенко І., Сидоренко Д. (2021) Класифікація зображень із використанням кластерного подання, Міжнародний науковий симпозіум «Інтелектуальні рішення-С». Обчислювальний інтелект (результати, проблеми, перспективи). Теорія прийняття рішень: праці міжн. наук. симпозіуму (Вересень 29, 2021). Київ – Ужгород, С. 44–45.
14. Gorokhovatskyi, V., Peredrii, O., Tvoroshenko, I., Markov, T. (2023) Матриця відстаней для множини компонентів структурного опису як інструмент для створення класифікатора зображень. *Advanced Information Systems*, 7(1), С. 5–13.
15. Pomazan V., Tvoroshenko I., and Gorokhovatskyi V. (2023) Development of an application for recognizing emotions using convolutional neural networks, *International Journal of Academic Information Systems Research*, 7(7), pp. 25–36.
16. Gorokhovatskyi V., Tvoroshenko I. (2020) Image Classification Based on the Kohonen Network and the Data Space Modification. In *CEUR Workshop Proc.: Computer Modeling and Intelligent Systems (CMIS-2020)*, 2608, pp. 1013–1026.
17. Tvoroshenko I., Gorokhovatskyi V., Kobylin O., and Tvoroshenko A. (2023) Application of deep learning methods for recognizing and classifying culinary dishes in images, *International Journal of Academic and Applied Research*, 7(9), pp. 57–70.