УДК 004.8 https://doi.org/10.35546/kntu2078-4481.2023.2.20

О. О. КУБАЙЧУК
кандидат фізико-математичних наук, доцент,
доцент кафедри математичного аналізу та теорії ймовірностей
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0002-5135-3688

ОГЛЯД ЗАСТОСУВАННЯ МЕТАЕВРИСТИЧНОГО ПІДХОДУ В КРИПТОАНАЛІЗІ

Криптографічний захист інформації є важливою складовою інформаційної безпеки. Розробка нових методів криптоаналізу допомагає зрозуміти межі стійкості наявних криптосистем. Сучасний криптоаналіз опирається на різні математичні дисципліни, зокрема, на теорію та методи оптимізації. Враховучи загальновизнані вимоги до стійкості шифрів, задача розшифрування може розглядатися як задача комбінаторної оптимізації.

Методи та алгоритми комбінаторної оптимізації сьогодні відіграють важливу роль у дослідженнях, пов'язаних з колом проблем, що безпосередньо впливають на інформаційну безпеку. Задача криптографічного захисту інформації вирішується створенням нових та вдосконаленням існуючих алгоритмів шифрування. З іншого боку, стрімко зростаючі можливості обчислювальної техніки відкривають практичні передумови впровадження технологій криптоаналізу, недоступних раніше. Зокрема, до актуальних технологій криптоаналізу можна віднести застосування оптимізаційних рандомізованих алгоритмів для інтелектуального дослідження простору пошуку з метою отримання прийнятного результату. Теоретично обгрунтовано, що такі алгоритми, за певних умов, дозволяють отримати розв'язок, коли ймовірність успіху дуже мала. Основним інструментом аналізу ефективності оптимізаційних рандомізованих алгоритмів є обчислювальний експеримент.

Аналіз можливості, особливостей та меж застосування метаевристичних алгоритмів криптоаналітиками вказує на перспективу використання метаевристичного підходу як універсального методу криптоаналізу.

В роботі обгрунтовується необхідність розвитку нових методів криптоаналізу із застосуванням метаевристик, міститься ретрспективний огляд публікацій за останній період в даній області. Число публікацій свідчить про актуальність напрямку досліджень.

Ключові слова: *криптоаналіз, криптографія, шифр, комбінаторна оптимізація, алгоритм, метаевристика.*

O. O. KUBAYCHUK
Candidate of Sciences in Mathematics (Ph.D.), Associate Professor,
Associate Professor at the Department of Mathematical Analysis
and Probability Theory
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"
ORCID: 0000-0002-5135-3688

REVIEW OF THE APPLICATIONS OF METAHEURISTIC APPROACH IN CRYPTANALYSIS

Cryptographic protection of information is an important component of information security. The development of new methods of cryptanalysis helps to understand the limits of stability of existing cryptosystems. Modern cryptanalysis relies on various mathematical disciplines, in particular, on the theory and methods of optimization. Taking into account the generally accepted requirements for the stability of ciphers, the decryption problem can be considered as a combinatorial optimization problem.

Methods and algorithms of combinatorial optimization today play an important role in research related to a range of problems directly affecting information security. The task of cryptographic protection of information is solved by creating new and improving existing encryption algorithms. On the other hand, the rapidly growing capabilities of computer technology open up practical prerequisites for the implementation of cryptanalysis technologies that were not available before. In particular, up-to-date cryptanalysis technologies include the use of optimization randomized algorithms for intelligent exploration of the search space in order to obtain an acceptable result. It is theoretically justified that such algorithms, under certain conditions, allow obtaining a solution when the probability of success is very small. The main tool for analyzing the effectiveness of optimization randomized algorithms is a computational experiment.

Analysis of the possibility, features and limits of the use of metaheuristic algorithms by cryptanalysts indicates the prospect of using the metaheuristic approach as a universal method of cryptanalysis.

The paper substantiates the need for the development of new methods of cryptanalysis using metaheuristics, contains a retrospective review of publications in the last period in this area. The number of publications indicates the relevance of the research direction.

Key words: *cryptanalysis, cryptography, cipher, combinatorial optimization, algorithm, metaheuristics.*

Постановка проблеми

Задачі комбінаторної оптимізації виникають у багатьох областях застосування обчислювальних методів, зокрема, таких як дослідження операцій, біоінформатика, маршрутизація, розподіл ресурсів і у криптоаналізі. Більшість практично важливих задач комбінаторної оптимізації належать до числа NP-важких, що, враховуючи можливі похибки у вхідних даних та можливість існування багатьох локальних екстремумів цільової функції, робить недоцільним використання точних алгоритмів розв'язання. Ці та інші аспекти, разом з прогресом обчислювальної техніки обумовили інтенсивний розвиток класу наближених методів, названих метаевристичними. Метаевристичні методи в силу своєї структури і гнучкості дозволяють конструювати на базі єдиної обчислювальної схеми наближені алгоритми розв'язання доволі широкого класу задач за прийнятний час. Такі алгоритми називають метаевристиками. Метаевристика є стратегією, яка повинна ефективно управляти дослідженням простору пошуку з метою отримання (суб)оптимального розв'язку. Дослідження простору пошуку здійснюється, зокрема, на основі евристик – процедур (функцій), які не вимагають строгого теоретичного обгрунтування. Ефективність тих чи інших евристик встановлюють емпіричним шляхом.

Метаевристика не є проблемно-орієнтованою, але вона може використовувати знання з певної предметної області у формі евристик. В результаті пошуку накопичуться нові знання, які автоматично враховуються на наступних етапах, тобто відбувається направлений інтелектуальний пошук. Результати інтелектуального пошуку можна перевіряти в рамках конкретної практичної задачі криптоаналізу.

В основі метаевристичних методів часто лежать висновки з результатів спостережень над процесами, які відбуваються у живій та неживій природі. Ці процеси характеризуються, зокрема, повторюваністю та випадковістю, а їх результати (оптимальність) оцінюються самою природою. Частину метаевристичних алгоритмів складає клас популяційних алгоритмів, – алгоритмів, у яких, на відміну від траекторних, на кожній ітерації опрацьовується не один, а одразу декілька варіантів розв'язку. Можливість розпаралелювання обчислень позитивно впливає на результати криптоаналізу.

Формулювання мети дослідження

На даний момент накопичено значний досвід (як позитивний так і негативний) застосування метаевристичних методів до аналізу симетричних і несиметричних шифрів. Огляд сучасного стану та оцінка перспектив застосування метаевристичного підходу до вирішення практичних задач криптоаналізу є основною метою даного дослідження.

Викладення основного матеріалу дослідження

Результати сучасних досліджень із розробки й упровадження прикладних методів комбінаторної оптимізації, питання класифікації, підходи до розв'язування та оцінки обчислювальної складності задач комбінаторної оптимізації представлено Гуляницьким Л. Ф. та Мулесою О. Ю. в [1]. Застосування метаевристичних методів комбінаторної оптимізації дозволяє автоматизувати процес розв'язання задачі криптоаналізу, сформульованої як задача оптимізації. Класичні шифри першими потрапили під приціл даної технології криптоаналізу. Серед робіт у цьому напрямку важливе місце займає робота Кларка та Доусона [2], що присвячена криптоаналізу класичних шифрів з використанням генетичного алгоритму, імітації відпалу та пошуку табу. До цієї ж задачі Кларк разом з Расселом та Степні розглядають застосування алгоритму ACO в [3]. Дімовські та Глігорські в [4], Тоймех і Арамахем у [5] продовжили дослідження Кларка, експериментуючи з різними параметрами оптимізаційної евристики з [2]. Юддін та Юсуф у [6] реалізують атаку на шифр простої підстановки застосовуючи ACO, аналогічно до [3]. Приблизно у той же період Сонг та ін. в [7] фокусуються на диференціальному криптоаналізі шифру DES4, застосовуючи генетичний алгоритм. Герг у [8] доводить переваги міметичного алгоритму перед генетичним у випадку атаки на SDES (Simplified DES). Для атаки блокового шифру TEA, Вей Ху в [9] застосовує підхід, що поєднує квантові і еволюційні обчислення, а саме, використовує алгоритм QGA. Була показана ефективність QGA у випадку TEA4 і TEA5 у той час, як звичайний GA виявився неспроможним.

Атаку на DES з використанням методу оптимізації роєм частинок (PSO) описано Елмонімом та ін. в [10]. Інший приклад застосування роєвого інтелекту – криптоаналіз класичних шифрів методом оптимізації колонією мурах представлено Мехазні Т. та ін. у [11].

Боричка та ін. в [12] на прикладі класичних шифрів показують, що застосування еволюційних алгоритмів є доцільним для розв'язання задач криптоаналізу. Можливість атаки на DES4 за фрагментом шифротексту вивчають Дадліч та ін.у [13]. При цьому, для обчислення оптимального ключа використовуються роєві алгоритми оптимізації. Садехзадеш і Тагербахал, здійснюючи криптоаналіз шифрів перестановок, у [14] порівнюють ефективність використання детермінованого і стохастичного локального пошуку для прискорення роботи генетичного алгоритму. Критичні зауваження щодо можливості застосування еволюційних алгоритмів для криптоаналізу блокового шифру SDES можна знайти у Тейтауда і Фонлапта [15].

Алгоритм пошуку, що імітує політ зозулі (Cuckoo Search) для обчислення ключа шифру Віженера, застосовано Ашоком та ін. [16]. Тахар у [17] дослідив можливість криптоаналізу шифрів SDES, DES4, DES за допомогою популяційного алгоритму оптимізації, що імітує полювання кажанів у повній темряві – алгоритму BAT.

Дворак і Боричка у [18] описують диференціальний криптоаналіз блокового шифру FEAL4 (Four-rounded Fast Data Encipherment Algorithm) з використанням еволюційного алгоритму. У [19] вони ж разом із Налєпою та Кавулком показують атаку на SDES із застосуванням генетичного алгоритму і експериментально доводять ефективність міметичного підходу, який дозволяє суттєво скорочувати час роботи алгоритму за рахунок використання процедури детермінованого локального пошуку. Пізніше, у [20], Дворак і Боричка використовують генетичний алгоритм, як знаряддя для диференціального аналізу, атакуючи уже DES6.

Амік та ін. у [21] застосовують технологію роєвого інтелекту, що базується на поведінці колонії світляків (Binary Firefly Algorithm) до атаки на DES, а у [22] ці ж автори досліджують можливості метаевристики, що імітує поведінку домашньої кішки (Binary Cat Swarm Optimization (BCSO)) до задач криптоаналізу.

До відкритого доступу потрапляє мало публікацій присвячених криптоаналізу актуальної криптосистеми з відкритим ключем RSA. Одним з перспективних напрямків у пошуках підходу до вирішення задачі факторизації є застосування методів комбінаторної оптимізації. Кандра, Ракшмаваті та ін. у [23] провели серію обчислювальних експериментів, які показали, що табуйований пошук можна застосовувати, але цей метод не є ефективним для розв'язання проблеми факторизації.

Прикладом успішної атаки на ранцеву криптосистему Меркля-Хеллмана є застосування Грері та ін. у [24] алгоритму MH-ACO, що є незначною модифікацією ACO. Згодом, той же колектив авторів описав можливість застосування ACO до криптоаналізу шифрів підстановки та блокових шифрів SDES і SAES у [25], [26] і [27].

Джейн та ін. у [28] порівнювали Cuckoo Search та GA, досліджуючи атаки на шифри підстановки. Алгоритм, що імітує стратегію зграї дельфінів під час полювання, застосовували Амік та ін. до шифру DES у [29].

Ракшмаваті та ін. [30] продовжили спроби вирішення проблеми факторизації, застосовуючи метаевристичний підхід. Цього разу в якості інструменту криптоаналізу було обрано генетичний алгоритм. Обчислювальні експерименти довели спроможність GA до атак на RSA, причому було показано, що підбір параметрів генетичного алгоритму має істотний вплив на швидкість отримання результату.

Сабончі і Акай у [31] в рамках диференціального криптоаналізу наводять можливості застосування еволюційного підходу та алгоритмів роєвого інтелекту до атак на класичні шифри. Вони ж у [32] до шифру Віженера, застосовують гібридизацію алгоритму оптимізації колонією бджіл, додаючи операцію біноміального кросоверу. В оглядовій статті [33] Сабончі та Акай підсумовують результати застосування різноманітних метаевристик до криптоаналізу класичних шифрів.

Серед останніх публікацій – роботи Грері та ін. [34], Дворак і Боричка [35] які продовжили свої дослідження щодо застосування метаевристик у криптоаналізі. Зокрема, у [34] для атаки шифру Меркля Хеллмана розглядається алгоритми MH-BACO (binary ant colony optimization) та MH-MACO, який є гібридизацією алгоритмів MH-BACO та MH-ACO з [24]. Есперементально показано, що гібридний алгоритм MH-MACO має переваги. Також доведено, що цей алгоритм має переваги і перед генетичним алгоритмом, і перед PSO. У [35] Дворак і Боричка узагальнюють свої результати, здобуті у [18], [19], [20]. Для диференціального криптоаналізу DES6 вони модифікують міметичний алгоритм, застосовуючи імітаційний відпал замість процедури детермінованого локального пошуку.

Опубліковані приклади застосування метаевристичного підходу до вирішення проблем криптоаналізу доводять спроможність даного підходу.

Висновки

Метаевристичні підходи до розв'язання задач комбінаторної оптимізації дозволяють отримувати прийнятні результати. Їхня вага значно зростає у випадках, коли застосування інших методів ускладнене. Задачею криптографічного захисту інформації якраз і є максимальне ускладнення можливостей для успішного криптоаналізу. Рандомізовані алгоритми, за певних умов, дозволяють знаходити розв'язок навіть тоді, коли ймовірність успіху дуже мала. Метаевристики, які використовують властивості рандомізованих процедур пошуку, стають потужним знаряддям криптоаналіу. Кожна з публікацій, наведених вище є реалізацією метаевристичного підходу до криптоаналізу. Спектр атакованих шифрів, від класичних до сучасних шифрів з відкритим ключем, доводить універсальність методу.

Список використаної літератури

1. Гуляницький Л. Ф., Мулеса О.Ю. Прикладні методи комбінаторної оптимізації. Київ: ВПЦ «Київський університет». 2016. 142 с.

2. Andrew Clark, Ed Dawson, Optimisation Heuristics for the Automated Cryptanalysis of Classical Ciphers. *Journal of Combinatorial Mathematics and Combinatorial Computing.* Vol. 28. 1998. pp. 63–86.

3. M. D. Russell, J. A. Clark and S. Stepney. Making the most of two heuristics: breaking transposition ciphers with ants. *The 2003 Congress on Evolutionary Computation, 2003. CEC '03*., Canberra, ACT, Australia Vol. 4. 2003. pp. 2653–2658. https://doi.org/10.1109/CEC.2003.1299423

4. Dimovski A., Gligoroski D. Attacks on the Transposition Ciphers Using Optimization Heuristics. *International Scientific Conference on Information, Communication Energy Systems,Technologies.* ICEST 2003.

5. Toemeh R., Arumugam S. Breaking Transposition Cipher with Genetic Algorithm. *Elektronika Ir Elektrotechnika.* 79(7). 2007. pp. 75–78. https://eejournal.ktu.lt/index.php/elt/article/view/10844

6. Uddin M. F., Youssef A. M. An artificial life technique for the cryptanalysis of simple substitution ciphers. *Canadian Conference on Electrical and Computer Engineering. IEEE.* 2006. pp. 1582–1585. http://dx.doi.org/10.1109%2FCCECE.2006.277769

7. Song J., Zhang H., Meng Q., Zhangyi W. Cryptanalysis of Four-Round DES Based on Genetic Algorithm. *Wirel. Commun. Netw. Mob. Comput. IEEE*, 2007, 10. pp. 2326–2329. https://doi.org/10.1109/WICOM.2007.580

8. Garg P. A. Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm. *Int. J. Netw. Secur. Its Appl. (IJNSA).* 1. 2009. pp. 34–42. https://doi.org/10.48550/arXiv.1004.0574

9. Hu W. Cryptanalysis of TEA using quantum-inspired genetic algorithms. J. *Softw. Eng. Appl.* 3. 2010. pp. 50–57. http://dx.doi.org/10.4236/jsea.2010.31006

10. Abd-Elmonim W.G., Ghali N.I., Hassanien A.E., Abraham. A. Known-Plaintext Attack of DES16 Using Particle Swarm Optimization. *In Proceedings of the Third IEEE World Congress on Nature and Biologically Inspired Computing. Salamanca.* Spain. 2011. pp. 12–16. https://doi.org/10.1109/NaBIC.2011.6089410

11. Mekhaznia T., Menai M. Cryptanalysis of classical ciphers with ant algorithms. *International Journal of Metaheuristics*. 3(3). 2014. pp. 175–198. https://doi.org/10.1504/IJMHEUR.2014.065159

12. Boryczka U., Dworak K. Genetic Transformation Techniques in Cryptanalysis. In: Nguyen, N.T., Attachoo, B., Trawiński, B., Somboonviwat, K. (eds) *Intelligent Information and Database Systems. ACIIDS 2014. Lecture Notes in Computer Science*. vol. 8398. 2014. Springer, Cham. https://doi.org/10.1007/978-3-319-05458-2_16

13. Dadhich A., Gupta A., Yadav S. Swarm Intelligence based linear cryptanalysis of four-round Data Encryption Standard algorithm. *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),* 2014, pp. 378–383. http://dx.doi.org/10.1109%2FICICICT.2014.6781312

14. Sadeghzadeh M, Taherbaghal M. A new method for decoding an encrypted text by genetic algorithms and its comparison with tabu search and simulated annealing. *Management Science Letters.* 4(2). 2014. pp. 213–220. https://doi.org/10.5267/j.msl.2013.12.037

15. Teytaud F., Fonlupt, C. A. Critical Reassessment of Evolutionary Algorithms on the cryptanalysis of the simplified data encryption standard algorithm. 2014. ArXiv, abs/1407.1993. https://doi.org/10.5121/IJCIS.2014.4201

16. Ashok K. Bhateja, Aditi Bhateja, Santanu Chaudhury, P.K. Saxena. Cryptanalysis of Vigenere cipher using Cuckoo Search. *Applied Soft Computing,* Vol. 26. 2015. pp. 315–324. https://doi.org/10.1016/j.asoc.2014.10.004

17. Tahar, M. BAT algorithm for Cryptanalysis of Feistel cryptosystems. 3(2). 2015. pp. 82–85. https://doi.org/10.18201/ijisae.82426

18. Dworak K., Boryczka U. Differential Cryptanalysis of FEAL4 Using Evolutionary Algorithm. In: Nguyen, N., Iliadis, L., Manolopoulos, Y., Trawiński, B. (eds) *Computational Collective Intelligence. ICCCI 2016. Lecture Notes in Computer Science.* 2016. vol. 9876. Springer. Cham. https://doi.org/10.1007/978-3-319-45246-3_10

19. Dworak, K., Nalepa, J., Boryczka, U., Kawulok, M. Cryptanalysis of SDES Using Genetic and Memetic Algorithms. In: Król, D., Madeyski, L., Nguyen, N. (eds) *Recent Developments in Intelligent Information and Database Systems. Studies in Computational Intelligence.* vol 642. 2016. Springer. Cham. https://doi.org/10.1007/978-3-319-31277-4_1

20. Dworak, K., Boryczka, U. Genetic Algorithm as Optimization Tool for Differential Cryptanalysis of DES6. In: Nguyen, N., Papadopoulos, G., Jędrzejowicz, P., Trawiński, B., Vossen, G. (eds) *Computational Collective Intelligence. ICCCI* 2017. Lecture Notes in Computer Science. vol. 10449. Springer. Cham. 2017. https://doi.org/10.1007/978-3-319-67077-5_11

21. Amic S., Soyjaudah K.S., Mohabeer H., Ramsawock. G. Cryptanalysis of DES16 using binary firefly algorithm. In Proceedings of the 2016 *IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies.* IEEE: Balaclava. Mauritius. 2016. pp. 94–99. https://doi.org/10.1109/EmergiTech.2016.7737318

22. Amic S., Soyjaudah K.S., Ramsawock G. Binary cat swarm optimization for cryptanalysis. In Proceedings of the 2017 *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. Bhubaneswar. India. 2017. pp. 1–6. https://doi.org/10.1109/ANTS.2017.8384120

23. Candra A., Budiman M.A., Rachmawati D. On Factoring The RSA Modulus Using Tabu Search. *Journal of Computing and Applied Informatics*, vol. 1(1). 2017. pp. 30–37. https://doi.org/10.32734/JOCAI.V1.I1-65

24. Grari H., Azouaqui A., Zine-Dine K., Bakhouya M., Gaber J. Cryptanalysis of Knapsack Cipher Using Ant Colony Optimization. *Smart Application and Data Analysis for Smart Cities*. 2018. http://dx.doi.org/10.2139/ssrn.3185322

25. Grari H., Azouaoui A., Zine-Dine K. A Novel Ant Colony Optimization Based Cryptanalysis of Substitution Cipher. In: Abraham, A., Haqiq, A., Ella Hassanien, A., Snasel, V., Alimi, A. (eds) Proceedings of the *Third International*

Afro-European Conference for Industrial Advancement AECIA 2016. Advances in Intelligent Systems and Computing. vol. 565. 2016. pp. 180–187. https://doi.org/10.1007/978-3-319-60834-1_19

26. Grari H., Azouaoui A., Zine-Dine K. Ant colony optimization for cryptanalysis of simplified-DES. In *Advanced Intelligent Systems for Sustainable Development (AI2SD'2018)* Vol. 2: Advanced Intelligent Systems Applied to Energy. 2019. pp. 111–121. https://doi.org/10.1007/978-3-030-12065-8_11

27. Grari H., Azouaoui A., Zine-Dine K. A cryptanalytic attack of simplified-AES using ant colony optimization. *International Journal of Electrical & Computer Engineering*. 9(5). 2019. pp. 4287–4295. https://doi.org/10.11591/ijece.v9i5.pp4287-4295

28. Jain A., Chaudhari N. S. An improved genetic algorithm and a new discrete cuckoo algorithm for solving the classical substitution cipher. *International Journal of Applied Metaheuristic Computing (IJAMC)*. 10(2). 2019. pp. 109–130. DOI: 10.4018/IJAMC.2019040105

29. Amic S., Soyjaudah K.S., Ramsawock G. Dolphin swarm algorithm for cryptanalysis. In Information Systems Design and Intelligent Applications; Satapathy, S., Bhateja, V., Somanah, R., Yang, X.S., Senkerik, R., Eds.; *Advances in Intelligent Systems and Computing*. Vol. 863. 2019. pp. 149–163. https://doi.org/10.1007/978-981-13-3338-5_15

30. D. Rachmawati, H. Tamara, S. Sembiring, M. Budiman. RSA public key solving technique by using genetic algorithm. *Journal of Theoretical and Applied Information Technology,* Vol. 98. 15. 2020. pp. 2990–2999.

31. Sabonchi A. K. S., Akay B. Cryptanalysis of polyalphabetic cipher using differential evolution algorithm. Tehnički vjesnik. 27(4). 2020. pp. 1101–1107. https://doi.org/10.17559/TV-20190314095054

32. Akay B. A binomial crossover based artificial bee colony algorithm for cryptanalysis of polyalphabetic cipher. *Tehnički vjesnik*. 27(6). 2020. pp. 1825–1835. https://doi.org/10.17559/TV-20190422225110

33. Sabonchi A. K. S., Akay B. A survey on the Metaheuristics for Cryptanalysis of Substitution and Transposition Ciphers. *Computer Systems Science And Engineering*, vol. 39. 1. 2021. pp. 87–106. http://doi.org/10.32604/csse.2021.05365

34. Grari H., Lamzabi S., Azouaoui A., Zine-Dine K. Cryptanalysis of Merkle-Hellman cipher using ant colony optimization. *Int J Artif Intell*. 2021. pp. 490–500. DOI: 10.11591/ijai.v10.i2

35. Dworak K., Boryczka U. Breaking Data Encryption Standard with a Reduced Number of Rounds Using Metaheuristics Differential Cryptanalysis. *Entropy*. vol. 23. 12. 2021. pp. 1697–1718. https://doi.org/10.3390/e23121697

References

1. Hulianytskyi L., Mulesa O. (2016). Applied methods of combinatorial optimization. Kyiv, P. 142. [in Ukrainian]

2. Andrew Clark, Ed Dawson. (1998).Optimisation Heuristics for the Automated Cryptanalysis of Classical Ciphers. *Journal of Combinatorial Mathematics and Combinatorial Computing*. Vol. 28. pp. 63–86.

3. M. D. Russell, J. A. Clark and S. Stepney. (2003). Making the most of two heuristics: breaking transposition ciphers with ants. *The 2003 Congress on Evolutionary Computation, 2003. CEC '03.,* Canberra, ACT, Australia. Vol.4. pp. 2653–2658. https://doi.org/10.1109/CEC.2003.1299423

4. Dimovski A., Gligoroski D. (2003). Attacks on the Transposition Ciphers Using Optimization Heuristics. *International Scientific Conference on Information, Communication Energy Systems, Technologies ICEST* 2003, Sofia, Bulgaria, October 2003.

5. Toemeh R., Arumugam S. (2007). Breaking Transposition Cipher with Genetic Algorithm. *Elektronika Ir Elektrotechnika*. 79(7). pp. 75–78. https://eejournal.ktu.lt/index.php/elt/article/view/10844

6. Uddin M. F., Youssef A. M. An artificial life technique for the cryptanalysis of simple substitution ciphers. In 2006 *Canadian Conference on Electrical and Computer Engineering. IEEE.* 2006. 1582 1585). http://dx.doi.org/10.1109%2FCCECE.2006.277769

7. Song, J.; Zhang, H.; Meng, Q.; Zhangyi, W. (2007). Cryptanalysis of Four-Round DES Based on Genetic Algorithm. *Wirel. Commun. Netw. Mob. Comput. IEEE.* 10. pp. 2326–2329. https://doi.org/10.1109/WICOM.2007.580

8. Garg P. (2009). A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm. *Int. J. Netw. Secur. Its Appl. (IJNSA)*. 1. pp. 34–42. https://doi.org/10.48550/arXiv.1004.0574

9. Hu W. (2010). Cryptanalysis of TEA using quantum-inspired genetic algorithms. *J. Softw. Eng. Appl.* 3. pp. 50–57. http://dx.doi.org/10.4236/jsea.2010.31006

10. Abd-Elmonim W.G., Ghali N.I., Hassanien A.E., Abraham. A. (2011). Known-Plaintext Attack of DES16 Using Particle Swarm Optimization. *In Proceedings of the Third IEEE World Congress on Nature and Biologically Inspired Computing, Salamanca, Spain.* pp. 12–16. https://doi.org/10.1109/NaBIC.2011.6089410

11. Mekhaznia T., Menai M. (2014). Cryptanalysis of classical ciphers with ant algorithms. *International Journal of Metaheuristics*. 3(3). pp. 175–198. https://doi.org/10.1504/IJMHEUR.2014.065159

12. Boryczka U., Dworak K. (2014). Genetic Transformation Techniques in Cryptanalysis. In: Nguyen, N.T., Attachoo, B., Trawiński, B., Somboonviwat, K. (eds) *Intelligent Information and Database Systems. ACIIDS 2014. Lecture Notes in Computer Science*. vol. 8398. Springer, Cham. https://doi.org/10.1007/978-3-319-05458-2_16

13. Dadhich A., Gupta A., Yadav S. (2014). Swarm Intelligence based linear cryptanalysis of four-round Data Encryption Standard algorithm. In 2014 *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*. pp. 378–383. http://dx.doi.org/10.1109%2FICICICT.2014.6781312

14. Sadeghzadeh M, Taherbaghal M. (2014). A new method for decoding an encrypted text by genetic algorithms and its comparison with tabu search and simulated annealing.Management Science Letters. 4(2). pp. 213–220. https://doi.org/10.5267/j.msl.2013.12.037

15. Teytaud F., Fonlupt, C. (2014). A Critical Reassessment of Evolutionary Algorithms on the cryptanalysis of the simplified data encryption standard algorithm. ArXiv, abs/1407.1993. https://doi.org/10.5121/IJCIS.2014.4201

16. Ashok K. Bhateja, Aditi Bhateja, Santanu Chaudhury, P.K. Saxena (2015). Cryptanalysis of Vigenere cipher using Cuckoo Search. *Applied Soft Computing*. Vol. 26. pp. 315–324. https://doi.org/10.1016/j.asoc.2014.10.004

17. Tahar, M. (2015). BAT algorithm for Cryptanalysis of Feistel cryptosystems. *International Journal of Intelligent Systems and Applications in Engineering*. 3(2). pp. 82–85. https://doi.org/10.18201/ijisae.82426

18. Dworak K., Boryczka U. (2016). Differential Cryptanalysis of FEAL4 Using Evolutionary Algorithm. In: Nguyen, N., Iliadis, L., Manolopoulos, Y., Trawiński, B. (eds) *Computational Collective Intelligence. ICCCI 2016. Lecture Notes in Computer Science*. vol. 9876. Springer, Cham. https://doi.org/10.1007/978-3-319-45246-3_10

19. Dworak, K., Nalepa, J., Boryczka, U., Kawulok, M. (2016). Cryptanalysis of SDES Using Genetic and Memetic Algorithms. In: Król, D., Madeyski, L., Nguyen, N. (eds) *Recent Developments in Intelligent Information and Database Systems. Studies in Computational Intelligence*, vol 642. Springer, Cham. https://doi.org/10.1007/978-3-319-31277-4_1

20. Dworak, K., Boryczka, U. (2017). Genetic Algorithm as Optimization Tool for Differential Cryptanalysis of DES6. In: Nguyen, N., Papadopoulos, G., Jędrzejowicz, P., Trawiński, B., Vossen, G. (eds) *Computational Collective Intelligence. ICCCI 2017. Lecture Notes in Computer Science*, vol 10449. Springer, Cham. https://doi.org/10.1007/978-3-319-67077-5_11

21. Amic S., Soyjaudah K.S., Mohabeer H., Ramsawock. G. (2016). Cryptanalysis of DES16 using binary firefly algorithm. In Proceedings of the 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies, Balaclava, Mauritius, 3–6 August 2016; IEEE: Balaclava, Mauritius. pp. 94–99. https://doi.org/10.1109/EmergiTech.2016.7737318

22. Amic S., Soyjaudah K.S., Ramsawock G. (2017). Binary cat swarm optimization for cryptanalysis. In Proceedings of the *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India*. pp. 1–6. https://doi.org/10.1109/ANTS.2017.8384120

23. Candra A., Budiman M.A., Rachmawati D. (2017). On Factoring The RSA Modulus Using Tabu Search. J*ournal of Computing and Applied Informatics*. vol. 1. n. 1. pp. 30–37. https://doi.org/10.32734/JOCAI.V1.I1-65

24. Grari H., Azouaqui A., Zine-Dine K., Bakhouya M., Gaber J. (2018). Cryptanalysis of Knapsack Cipher Using Ant Colony Optimization. *Smart Application and Data Analysis for Smart Cities*. http://dx.doi.org/10.2139/ssrn.3185322

25. Grari H., Azouaoui A., Zine-Dine K. (2016). A Novel Ant Colony Optimization Based Cryptanalysis of Substitution Cipher. In: Abraham, A., Haqiq, A., Ella Hassanien, A., Snasel, V., Alimi, A. (eds) Proceedings of the *Third International Afro-European Conference for Industrial Advancement AECIA 2016. Advances in Intelligent Systems and Computing*. vol. 565. pp. 180–187 https://doi.org/10.1007/978-3-319-60834-1_19

26. Grari H., Azouaoui A., Zine-Dine K. (2019). Ant colony optimization for cryptanalysis of simplified-DES. In Advanced Intelligent Systems for Sustainable Development (AI2SD'2018) Vol 2: *Advanced Intelligent Systems Applied to Energy*. pp. 111–121. https://doi.org/10.1007/978-3-030-12065-8_11

27. Grari H., Azouaoui A., Zine-Dine K. (2019). A cryptanalytic attack of simplified-AES using ant colony optimization. *International Journal of Electrical & Computer Engineering*. 9(5). pp. 4287–4295. https://doi.org/10.11591/ijece.v9i5.pp4287-4295

28. Jain A., Chaudhari N. S. (2019). An improved genetic algorithm and a new discrete cuckoo algorithm for solving the classical substitution cipher. *International Journal of Applied Metaheuristic Computing (IJAMC).* 10(2), 109 130. DOI: 10.4018/IJAMC.2019040105

29. Amic S., Soyjaudah K.S., Ramsawock G. (2019). Dolphin swarm algorithm for cryptanalysis. In Information Systems Design and Intelligent Applications; Satapathy, S., Bhateja, V., Somanah, R., Yang, X.S., Senkerik, R., Eds.; *Advances in Intelligent Systems and Computing.* Vol. 863. pp. 149–163. https://doi.org/10.1007/978-981-13-3338-5_15

30. D. Rachmawati, H. Tamara, S. Sembiring, M. Budiman. (2020). RSA public key solving technique by using genetic algorithm. *Journal of Theoretical and Applied Information Technology*. Vol. 98. No. 15. pp .2990–2999. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85053419786&partnerID=40&md5=1072f49ab20414f2288933fefbef056e

31. Sabonchi A. K. S., Akay B. (2020). Cryptanalysis of polyalphabetic cipher using differential evolution algorithm. *Tehnički vjesnik.* 27(4). pp. 1101–1107. https://doi.org/10.17559/TV-20190314095054

32. Akay B. (2020). A binomial crossover based artificial bee colony algorithm for cryptanalysis of polyalphabetic cipher. *Tehnički vjesnik*. 27(6). pp. 1825–1835. https://doi.org/10.17559/TV-20190422225110

33. Sabonchi A. K. S., Akay B. (2021). A survey on the Metaheuristics for Cryptanalysis of Substitution and Transposition Ciphers. *Computer Systems Science And Engineering*. vol. 39. no. 1. pp. 87–106. http://doi.org/10.32604/csse.2021.05365

34. Grari H., Lamzabi S., Azouaoui A., Zine-Dine K. (2021). Cryptanalysis of Merkle-Hellman cipher using ant colony optimization. *Int J Artif Intell.* pp. 490–500. DOI: 10.11591/ijai.v10.i2

35. Dworak K., Boryczka U. (2021). Breaking Data Encryption Standard with a Reduced Number of Rounds Using Metaheuristics Differential Cryptanalysis. *Entropy*. vol. 23. no. 12 pp. 1697–1718. https://doi.org/10.3390/e23121697