STUDI LITERATUR MENGENAI KINERJA BLOWFISH, AES, CHACHA20, DAN GCM DALAM SISTEM KEAMANAN DATA

I Putu Aditya Brama Putra Cakra Negara¹, M. Naufal Nafian Abror², Niely Rejekinta Tarigan³

Universitas Pertahanan Republik Indonesia

E-mail: adityabrama5248@gmail.com¹, naufal.nafian92@gmail.com²,
nielytarigan14@gmail.com³

ABSTRAK

Keamanan data merupakan aspek krusial di era digital untuk melindungi informasi sensitif dari ancaman akses tidak sah dan pencurian data. Penelitian ini membandingkan empat algoritma enkripsi simetris, yaitu *Advanced Encryption Standard (AES)*, *Blowfish*, *ChaCha20*, dan *Galois/Counter Mode (GCM)*, berdasarkan efisiensi dan tingkat keamanan yang ditawarkan. Metodologi penelitian menggunakan tinjauan literatur untuk menganalisis kelebihan dan kekurangan masing-masing algoritma dalam berbagai aplikasi, termasuk komunikasi online, transaksi keuangan, dan penyimpanan data di *cloud*. Hasil analisis menunjukkan bahwa AES menawarkan keseimbangan optimal antara kecepatan dan keamanan, dengan dukungan akselerasi perangkat keras (AES-NI) yang meningkatkan efisiensinya pada sistem modern. Blowfish unggul dalam kecepatan, tetapi keterbatasan ukuran blok 64-bit membatasinya pada aplikasi dengan data berukuran besar. ChaCha20 menunjukkan performa tinggi dan keamanan pada perangkat tanpa akselerasi perangkat keras, sedangkan GCM menyediakan autentikasi data tambahan yang ideal untuk aplikasi yang membutuhkan integritas data. Penelitian menegaskan bahwa AES-GCM adalah solusi unggulan untuk enkripsi modern, menggabungkan efisiensi, keamanan, dan autentikasi dalam satu mekanisme, sehingga sangat cocok untuk lingkungan yang memerlukan throughput tinggi dan perlindungan data yang kuat, seperti sistem keuangan dan penyimpanan data di *cloud*.

Keyword: *Symmetric Encryption, Encryption Algorithm Comparison, cryptographic Performance*

Article History

Received: Januari 2025

Reviewed: Januari 2025

Published: Januari 2025

Plagiarism Checker:

No 234.GT8.,35

Prefix DOI :

10.3483/trigonometri.v1i1.800

Copyright : Author

Publishby : Trigonometri

INTRODUCTION

Keamanan data telah menjadi salah satu aspek paling krusial di era digital, dimana pertumbuhan teknologi dan konektivitas global semakin meningkatkan risiko terhadap akses tidak sah dan pencurian informasi. Algoritma enkripsi memainkan peran vital dalam melindungi data dari ancaman tersebut, dengan menyediakan lapisan perlindungan yang mengamankan informasi sensitive dari akses yang tidak sah. Berbagai algoritma enkripsi, seperti *Advanced Encryption Standard (AES)*, *Blowfish*, *ChaCha20*, dan *Galois/Counter Mode (GCM)*, telah digunakan secara luas dalam berbagai aplikasi, mulai dari komunikasi online, transaksi

keuangan, hingga penyimpanan data di *cloud*. Efektivitas algoritma ini tidak hanya bergantung pada tingkat keamanannya tetapi juga pada kinerjanya dalam memenuhi kebutuhan sistem yang berbeda (Assa-Agyei & Olajide, 2023).

Algoritma enkripsi seperti AES, Blowfish, ChaCha20, dan GCM memiliki kelebihan dan keterbatasan yang berbeda (Muhammed et al., 2024a). Beberapa algoritma unggul dalam kecepatan pada perangkat tertentu, sedangkan yang lain menawarkan tingkat keamanan lebih tinggi dengan kebutuhan sumber daya lebih besar. Variasi ini menciptakan tantangan dalam menentukan algoritma yang paling sesuai untuk aplikasi spesifik, termasuk perangkat dengan keterbatasan daya, sistem *real-time*, atau kebutuhan keamanan tingkat tinggi (Madhusudhan et al., 2021). Analisis yang komprehensif diperlukan untuk memahami performa relatif dari algoritma-algoritma tersebut.

Banyak penelitian yang telah mengkaji kinerja algoritma enkripsi, baik secara terpisah maupun dalam perbandingan yang terbatas (Ghosh, 2020). Beberapa studi fokus pada aspek kecepatan dan efisiensi, sementara yang lain menekankan keamanan terhadap serangan tertentu. Namun, tinjauan literatur yang mencakup analisis komprehensif terhadap algoritma Blowfish, AES, ChaCha20, dan GCM dalam berbagai konteks aplikasi masih jarang ditemukan. Hal ini menunjukkan adanya kebutuhan untuk menyusun kajian yang lebih terstruktur guna memberikan wawasan mendalam tentang keempat algoritma tersebut (Et. al., 2021).

Penelitian ini bertujuan untuk melakukan analisis komparatif terhadap algoritma enkripsi Blowfish, AES, ChaCha20, dan GCM berdasarkan studi literatur. Fokus utama penelitian adalah mengevaluasi aspek kecepatan, efisiensi, dan keamanan masing-masing algoritma dalam berbagai konteks aplikasi (Taha & Al-Tuwaijari, 2021). Kajian ini diharapkan dapat memberikan pemahaman yang lebih komprehensif mengenai keunggulan dan keterbatasan algoritma tersebut, sehingga dapat membantu dalam menentukan algoritma yang paling sesuai untuk kebutuhan tertentu (Muhammed et al., 2024a).

Penelitian ini memberikan kontribusi berupa tinjauan literatur yang komprehensif mengenai perbandingan algoritma Blowfish, AES, ChaCha20, dan GCM. Hasil analisis diharapkan dapat menjadi panduan bagi peneliti dan praktisi dalam memilih algoritma enkripsi yang optimal sesuai dengan kebutuhan spesifik, baik dari segi kecepatan, efisiensi, maupun keamanan (Salkanovic et al., 2021). Selain itu, kajian ini juga dapat memperkaya literatur terkait dengan menawarkan perspektif baru tentang bagaimana keempat algoritma ini berkinerja di berbagai skenario aplikasi.

METHOD

Scope Determination

Penelitian berfokus pada metode enkripsi simetris, dimana enkripsi simetris menawarkan efisiensi transmisi data yang tinggi, tingkat kesalahan bit yang rendah, serta proses transmisi yang lebih aman (Cai & Yao, 2022). Keunggulan metode enkripsi simetris itu yang menjadikan ketertarikan penelitian ini untuk membandingkan metode enkripsi kunci simetris berdasarkan literatur review yang digunakan dari beberapa literatur. Metode yang dibandingkan antara lain *Blowfish Method*, *Advanced Encryption Standard* (AES), ChaCha20, dan *Galois/Counter Mode* (GCM). Metode enkripsi simetris yang terus berkembang, namun sampai saat ini metode enkripsi lama seperti metode blowfish masih relevan untuk digunakan. Metode yang lama masih relevan namun metode yang baru dikembangkan juga sudah lebih kompleks, sehingga tujuan dari penelitian ini adalah untuk membandingkan keempat metode serta mencari keunggulan dari keempat metode enkripsi simetris tersebut.

Penelitian ini menggunakan jenis penelitian *literatur review*, dimana artikel ilmiah dan buku yang menyangkut informasi mengenai metode blowfish, metode AES, metode ChaCha20, dan metode CGM serta penerapan dari keempat metode tersebut digunakan dalam penelitian ini. Rentang waktu literatur yang digunakan dalam penelitian ini berkisar 20 tahun kebelakang, rentang waktu ini digunakan karena metode blowfish merupakan metode enkripsi yang sudah

lampau dikembangkan namun masih relevan digunakan dalam enkripsi data sehari-hari hingga sekarang.

Literature search

Enkripsi kunci simetris menggunakan kode yang sama antara pengirim dan penerima, dimana metode AES menjadi metode yang paling sering digunakan dalam jenis enkripsi ini (Singh, 2022). Metode enkripsi simetris dapat dibandingkan menjadi beberapa variabel seperti tingkat keamanan antar metode, kecepatan tingkat enkripsi antar metode, serta kecukupan sumber data yang akan dienkripsi juga dapat menjadi perbandingan diantara keempat metode enkripsi simetris yang digunakan (Muhammed et al., 2024b).

Literature Selection

Pengambilan *literatur review* dijadikan sebuah patokan untuk membandingkan keempat model enkripsi setara dalam penelitian ini, jurnal penelitian serta artikel ilmiah yang digunakan harus dalam lingkup metode pengembangan enkripsi data. Literatur yang digunakan dipilih berdasarkan banyak jurnal rujukan yang merujuk pada literatur yang kami gunakan, setidaknya lebih dari lima jurnal rujukan yang merujuk pada satu penelitian maka penelitian tersebut yang dapat kami gunakan dan kami bandingkan. Sumber literatur yang setara dapat menjadikan perbandingan hasil antara literatur menjadi seimbang dan dapat dijadikan pembandingan satu dengan yang lainnya (Shabani & Lam, 2013). Literatur yang tidak sesuai dengan kriteria maka diabaikan untuk dibandingkan dalam penelitian ini.

Literature Analysis

Penelitian yang dilakukan (Assa-Agyei & Olajide, 2023) membandingkan antara metode blowfish dengan AES dimana waktu proses enkripsi dengan kecepatan enkripsi menjadi parameter pembandingan. Penelitian (Verma et al., 2011) juga membandingkan kecepatan namun penambahan keamanan metode enkripsi blowfish dan AES dalam mengatasi serangan dalam proses enkripsi juga dipertimbangkan. Penelitian (Mandal, 2012) selain membandingkan waktu dalam proses enkripsi, waktu dalam proses CPU, *throughput*, serta konsumsi daya yang digunakan metode blowfish dan AES juga menjadi perbandingan dalam penelitian ini.

Penelitian (Ashur et al., 2017) membandingkan metode ChaCha20 dengan GCM menggunakan parameter keamanan enkripsi dari masing-masing metode dalam mengatasi serangan enkripsi dari luar. Penelitian (Katz & Shacham, 2017) membandingkan metode GCM dengan ChaCha dengan menguji keamanan enkripsi namun yang menjadi ketertarikan adalah metode yang lebih cepat pulih dalam mengatasi serangan enkripsi tersebut. Penelitian (Noura et al., 2022) juga membandingkan kedua metode yaitu ChaCha20 dengan GCM dimana perbandingan meliputi waktu proses enkripsi, *throughput*, serta sistem keamanan enkripsi dari kedua metode. Perbandingan serupa juga digunakan dalam penelitian (Muhammed et al., 2024a). Selain itu Penelitian (Degabriele et al., 2021) menyebutkan bahwa perbandingan model AES, ChaCha20, dan GCM dapat menemukan metode yang paling aman dalam pengembangan metode enkripsi.

Reporting the Data

Jurnal dan Penulis	Tahun Terbit	Metode Blowfish	Metode AES	Metode ChaCha20	Metode GCM	Waktu Enkripsi	Keamanan Enkripsi	Parameter Lainnya
A Comparative Study of Twofish, Blowfish, and Advanced	2023	+	+	-	-	AES lebih lambat dibandingkan Blowfish	AES memiliki standar keamanan ganda sehingga lebih aman	Dalam melihat kecepatan metode enkripsi digunakan Bahasa

Encryption Standard for Secured Data Transmission (Assa-Agyei, 2023)							dibandingkan blowfish	pemrograman Python 3.10.
Performance Analysis of Data Encryption Algorithms (Verma, 2011)	2011	+	+	-	-	Blowfish mengungguli AES dalam hal kecepatan mengenkripsi data	Blowfish menjadi algoritma dengan keamanan yang baik dibandingkan AES dalam mengatasi serangan tidak sah	Digunakan beragam ukuran blok data untuk melihat kecepatan dari metode yang dibandingkan serta menguji keamanan metode.
Evaluation of Performance of the Symmetric Key Algorithms: DES, 3DES, AES, and Blowfish (Mandal, 2012)	2012	+	+	-	-	Blowfish lebih unggul dibandingkan AES dalam waktu enkripsi	Walaupun lebih lambat tetapi metode AES lebih aman jika menghadapi serangan gangguan yang besar	AES lebih unggul dalam membaca blok yang besar, dimana metode AES menawarkan keseimbangan yang baik antara kecepatan enkripsi dengan keamanan
Boosting Authenticated Encryption Robustness with Minimal Modifications (Ashur, 2017)	2017	-	-	+	+	Metode ChaCha20 dapat mengguli GCM dalam waktu enkripsi serta kompleksitas hasil	GCM dapat menyediakan keamanan Ketika teks belum diverifikasi, hal ini menjadikan keunggulan GCM dalam	Perbandingan ChaCha20 dan GCM pada penelitian ini bergantung pada keberadaan AES-NI sebagai pembandingan tambahan antara

							bidang keamanan	kedua metode.
Advances in Cryptology (Kittler, 2017)	2017	-	-	+	+	GCM umumnya bekerja lebih baik dalam perangkat yang keras, sehingga dapat menyesuaikan akselerasi dengan kebutuhan yang digunakan	GCM lebih unggul karena dapat mengacak nonce dalam protocol seperti TLS 1.3 untuk keamanan multi pengguna	Metode ChaCha20 dan GCM lebih unggul jika dibandingkan dengan metode OCB, karena memiliki efisiensi waktu dan keamanan yang tinggi.
A Single-Pass and One-Round Message Authentication Encryption for Limited IoT Devices (Noura, 2022)	2022	-	-	+	+	ChaCha20 lebih efisien dibandingkan GCM terutama bila tidak ditambahkan perangkat keras secara bersamaan.	Dalam proteksi keamanan enkripsi GCM lebih unggul 1% dibandingkan ChaCha20 dalam mengamankan enkripsi model	Penilaian metode terbaik menggunakan pendekatan statis nilai MAE dalam membandingkan metode yang digunakan.
The Security of ChaCha20-Poly1305 in the Multi-User Setting (Degabriele, 2021)	2021	-	+	+	+	Metode ChaCha20 unggul dalam efisiensi dalam implementasi perangkat lunak dan juga perangkat keras.	Metode AES yang dipadukan dengan ChaCha20 menjadikan metode yang unggul dalam tingkat keamanan karena dapat mengatur multi pengguna yang	Dalam membandingkan metode enkripsi metode AES digabungkan dengan ChaCha20 dan GCM serta dilihat efisiensi dari gabungan metode tersebut.

							Tangguh terhadap penyalahgunaan nonce	
Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption (Aladdin, 2024)	2024	+	+	+	-	ChaCha20 dirancang untuk mengatasi perangkat keras sehingga lebih efisien dibandingkan metode Blowfish dan AES dalam mengenkripsi data.	ChaCha20 lebih unggul dibandingkan metode yang lain karena memiliki tingkat ketahanan yang tinggi sehingga dapat diterapkan dalam kondisi lingkungan apapun.	Dalam penelitian ini metode AES, Blowfish, Twofish, Salsa20, dan ChaCha20 digunakan untuk mengenkripsi gambar guna mengevaluasi waktu proses enkripsi dan kecepatan metode untuk mengamankan data.

RESULTS AND DISCUSSION

Dari perbandingan antara algoritma Blowfish, AES, ChaCha20, dan GCM, setiap metode memiliki keunggulan dan keterbatasan dalam aspek kecepatan dan keamanan. AES merupakan pilihan paling populer dengan keseimbangan optimal antara kedua faktor tersebut, terutama dengan dukungan akselerasi perangkat keras (AES-NI), yang menjadikannya sangat efisien untuk lingkungan modern. Blowfish, meskipun menawarkan kecepatan tinggi, memiliki keterbatasan pada ukuran blok 64-bit yang membuatnya kurang cocok untuk aplikasi dengan volume data besar. ChaCha20 unggul dalam performa dan keamanan pada perangkat yang tidak mendukung akselerasi perangkat keras AES, sementara GCM memberikan perlindungan tambahan melalui autentikasi, membuatnya ideal untuk aplikasi yang membutuhkan integritas data yang kuat. Dengan mempertimbangkan kecepatan dan keamanan secara menyeluruh, model terbaik untuk mengenkripsi data adalah AES-GCM, yang menggabungkan efisiensi, keamanan, dan autentikasi data dalam satu solusi.

Dalam memilih algoritma enkripsi untuk membaca dan mengenkripsi data dengan efisiensi waktu dan keamanan yang tinggi, AES-GCM adalah pilihan paling unggul pada perangkat keras modern yang mendukung akselerasi AES-NI karena performa superior dan autentikasi bawaan. Namun, jika lingkungan target tidak memiliki dukungan tersebut, ChaCha20 adalah alternatif terbaik dengan keamanan setara dan kinerja optimal. Penggunaan Blowfish sebaiknya dibatasi pada aplikasi sederhana atau dengan sumber daya terbatas, mengingat algoritma yang lebih aman dan efisien tersedia untuk kebutuhan modern. Pemilihan algoritma yang tepat harus mempertimbangkan karakteristik perangkat, kebutuhan keamanan, dan ketersediaan akselerasi perangkat keras untuk mencapai keseimbangan terbaik antara kinerja dan perlindungan data.

CONCLUSION

Dari analisis komparatif terhadap algoritma enkripsi Blowfish, AES, ChaCha20, dan GCM, dapat disimpulkan bahwa masing-masing algoritma memiliki keunggulan dan kelemahan tersendiri yang membuatnya lebih sesuai untuk konteks aplikasi tertentu berdasarkan kebutuhan sistem. AES muncul sebagai algoritma enkripsi yang paling serbaguna dengan keseimbangan optimal antara kecepatan dan keamanan. Dukungan akselerasi perangkat keras melalui AES-NI meningkatkan efisiensinya, menjadikannya pilihan unggul untuk aplikasi modern yang membutuhkan throughput tinggi dan perlindungan data yang kuat. Integrasi AES dengan *Galois/Counter Mode* (GCM) semakin memperkuat fungsinya dengan menambahkan mekanisme autentikasi data bawaan. Kombinasi ini, yakni AES-GCM, sangat ideal untuk lingkungan yang memerlukan enkripsi cepat dan integritas data tinggi, seperti sistem keuangan, komunikasi aman, dan penyimpanan data di cloud.

Blowfish, meskipun merupakan algoritma yang lebih tua, tetap menunjukkan keunggulan dalam lingkungan dengan sumber daya terbatas berkat desainnya yang sederhana dan kecepatan enkripsi yang tinggi. Namun, ukuran blok yang lebih kecil (64-bit) membuatnya kurang cocok untuk aplikasi dengan volume data besar karena rentan terhadap serangan tertentu, seperti *birthday attack*. Oleh karena itu, Blowfish lebih sesuai untuk aplikasi sederhana atau sistem dengan daya komputasi terbatas.

ChaCha20 muncul sebagai alternatif yang kuat untuk AES, terutama dalam lingkungan yang tidak mendukung akselerasi perangkat keras. Algoritma ini dirancang untuk memprioritaskan kecepatan dan keamanan, dengan performa yang sangat baik di platform berbasis perangkat lunak. Penggunaannya secara luas di perangkat mobile dan IoT mencerminkan efisiensi serta keandalannya dalam lingkungan dengan keterbatasan perangkat keras. Ketahanan ChaCha20 terhadap penyalahgunaan *nonce* juga menjadikannya pilihan utama untuk protokol komunikasi aman, seperti TLS 1.3.

Sementara itu, GCM, meskipun bukan algoritma enkripsi mandiri, memberikan nilai tambah yang signifikan ketika digunakan bersama AES. Mekanisme autentikasi data yang dimilikinya menjadikannya sangat sesuai untuk aplikasi yang memerlukan jaminan integritas data, seperti transaksi web yang aman dan tanda tangan digital. Kemampuannya untuk memparallelkan proses enkripsi juga memastikan efisiensinya dalam lingkungan berkinerja tinggi.

Pemilihan algoritma enkripsi harus disesuaikan dengan kebutuhan spesifik aplikasi. Aplikasi dengan kebutuhan keamanan tinggi dan dukungan perangkat keras modern, AES-GCM direkomendasikan karena menawarkan kombinasi performa superior dan autentikasi bawaan. ChaCha20 adalah alternatif terbaik karena efisiensi dan keandalannya dalam perangkat tanpa akselerasi perangkat keras untuk lingkungan dengan sumber daya terbatas. Blowfish tetap dapat diandalkan dengan syarat volumenya tidak besar dan risiko serangan tidak terlalu signifikan untuk aplikasi sederhana atau sistem lama.

Penelitian di masa depan dapat difokuskan pada pengembangan implementasi hibrida dari algoritma ini, sehingga kekuatan masing-masing algoritma dapat dimanfaatkan untuk memenuhi kebutuhan kriptografi yang beragam. Dengan memahami karakteristik unik dari setiap algoritma, para peneliti dan praktisi dapat mengambil keputusan yang tepat untuk mengoptimalkan keamanan data dan performa sistem.

REFERENCES

- Ashur, T., Dunkelman, O., & Luykx, A. (2017). *Boosting Authenticated Encryption Robustness with Minimal Modifications* (pp. 3-33). https://doi.org/10.1007/978-3-319-63697-9_1
- Assa-Agyei, K., & Olajide, F. (2023). A Comparative Study of Twofish, Blowfish, and Advanced Encryption Standard for Secured Data Transmission. *International Journal of Advanced Computer Science and Applications*, 14(3), 393-398. <https://doi.org/10.14569/IJACSA.2023.0140344>

- Cai, W., & Yao, H. (2022). A Secure Transmission Method of Network Communication Data Based on Symmetric Key Encryption Algorithm. *Wireless Personal Communications*, 127(1), 341-352. <https://doi.org/10.1007/s11277-021-08266-w>
- Degabriele, J. P., Govinden, J., Günther, F., & Paterson, K. G. (2021). The Security of ChaCha20-Poly1305 in the Multi-User Setting. *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 1981-2003. <https://doi.org/10.1145/3460120.3484814>
- Et. al., P. S. (2021). Performance Analysis of Cascaded Hybrid Symmetric Encryption Models. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(2), 1699-1708. <https://doi.org/10.17762/turcomat.v12i2.1506>
- Ghosh, A. (2020). Comparison of Encryption Algorithms : AES , Blowfish and Twofish for Security of Wireless Networks. *International Research Journal of Engineering and Technology (IRJET)*, June, 4656-4659. <https://doi.org/10.13140/RG.2.2.31024.38401>
- Katz, J., & Shacham, H. (Eds.). (2017). *Advances in Cryptology - CRYPTO 2017* (Vol. 10403). Springer International Publishing. <https://doi.org/10.1007/978-3-319-63697-9>
- Madhusudhan, N., Padma, P., & Rao, R. (2021). Development of Pipelined Blowfish Algorithm with Memory based S-Box. *Journal of Physics: Conference Series*, 1804(1). <https://doi.org/10.1088/1742-6596/1804/1/012159>
- Mandal, P. C. (2012). Evaluation of performance of the Symmetric Key Algorithms : DES , 3DES , AES and Blowfish. *Journal of Global Research in Computer Science*, 3(8), 67-70.
- Muhammed, R. K., Aziz, R. R., Hassan, A. A., Aladdin, A. M., Saydah, S. J., Rashid, T. A., & Hassan, B. A. (2024a). Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption. *Kurdistan Journal of Applied Research*, 9(1), 52-65. <https://doi.org/10.24017/science.2024.1.5>
- Muhammed, R. K., Aziz, R. R., Hassan, A. A., Aladdin, A. M., Saydah, S. J., Rashid, T. A., & Hassan, B. A. (2024b). Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption. *Kurdistan Journal of Applied Research*, 9(1), 52-65. <https://doi.org/10.24017/science.2024.1.5>
- Noura, H. N., Salman, O., Couturier, R., & Chehab, A. (2022). A Single-Pass and One-Round Message Authentication Encryption for Limited IoT Devices. *IEEE Internet of Things Journal*, 9(18), 17885-17900. <https://doi.org/10.1109/JIOT.2022.3161192>
- Salkanovic, A., Ljubic, S., Stankovic, L., & Lerga, J. (2021). Analysis of Cryptography Algorithms Implemented in Android Mobile Application. *Information Technology and Control*, 50(4), 786-807. <https://doi.org/10.5755/j01.itc.50.4.29464>
- Shabani, D. B., & Lam, W. Y. (2013). A REVIEW OF COMPARISON STUDIES IN APPLIED BEHAVIOR ANALYSIS. *Behavioral Interventions*, 28(2), 158-183. <https://doi.org/10.1002/bin.1361>
- Singh, P. K. (2022). A Note on Symmetric Key Cryptosystems. *International Journal of Advanced Networking and Applications*, 15-18. <https://doi.org/10.35444/IJANA.2022.ICCMEApaper05>
- Taha, M. H., & Al-Tuwaijari, J. M. (2021). Improvement of Chacha20 algorithm based on tent and Chebyshev chaotic maps. *Iraqi Journal of Science*, 62(6), 2029-2039. <https://doi.org/10.24996/ij.s.2021.62.6.29>
- Verma, O. P., Agarwal, R., Dafouti, D., & Tyagi, S. (2011). Notice of Violation of IEEE Publication Principles - Performance analysis of data encryption algorithms. *2011 3rd International Conference on Electronics Computer Technology*, 399-403. <https://doi.org/10.1109/ICECTECH.2011.5942029>