JIKTEKS : Jurnal Ilmu Komputer dan Teknologi Informasi
Vol. 03, No. 03, Agustus 2025, hlm. 13 - 19
ISSN : 2986-5417
DOI : doi.org/10.70404/jikteks.v3i03.320
Laman Jurnal: jurnal.faatuatua.com/index.php/JIKTEKS

Modifikasi Implementasi Algoritma Caesar Cipher dengan Teknik Shift Left Bit

Trio Fitrada
Informatika, Institut Teknologi Kalimantan, Indonesia
e-mail: *triofitrada@gmail.com*

Keywords:

Caesar Cipher,
Bitwise Shift Left,
Cryptographic Modification,
Hybrid Encryption,
Data Security.

ABSTRACT

In response to the inherent vulnerabilities of classical cryptographic methods, this study proposes a modified Caesar Cipher algorithm integrated with a bitwise shift left operation to enhance data confidentiality. The research implements a two-layer encryption process on the plaintext "SOFT SKILL GET YOU PROMOTED," beginning with a character substitution using Caesar Cipher with a shift key of n=3, followed by a 3-position bitwise shift left operation on the binary representation of the resulting ciphertext. The findings demonstrate a significant increase in cryptographic complexity, evidenced by the transformation of the initial ciphertext into a randomized binary sequence comprising non-printable characters, thereby effectively obscuring linguistic patterns and mitigating frequency analysis attacks. While the modified algorithm successfully maintains perfect decryption reversibility, the evaluation identifies limitations in overflow handling and potential susceptibility to known-plaintext attacks. Consequently, this study confirms the feasibility of a hybrid cryptographic approach, merging classical substitution with bitwise manipulation, and recommends further development incorporating dynamic key scheduling, XOR operations with auxiliary keys, and a block-based encryption paradigm to optimize security and operational robustness for practical applications.

Kata Kunci:

Caesar Cipher,
Shift Left Bitwise,
Modifikasi Kriptografi,
Enkripsi Hybrid,
Keamanan Data.

ABSTRAK

Sebagai respons terhadap kerentanan yang melekat pada metode kriptografi klasik, penelitian ini mengusulkan modifikasi algoritma Caesar Cipher yang diintegrasikan dengan operasi shift left bitwise untuk meningkatkan kerahasiaan data. Penelitian mengimplementasikan proses enkripsi dua lapis pada plainteks "SOFT SKILL GET YOU PROMOTED," yang diawali dengan substitusi karakter menggunakan Caesar Cipher dengan kunci pergeseran n=3, dilanjutkan dengan operasi shift left bitwise sebanyak 3 posisi pada representasi biner dari cipherteks yang dihasilkan. Temuan penelitian menunjukkan peningkatan kompleksitas kriptografi yang signifikan, yang dibuktikan dengan transformasi cipherteks awal menjadi sekuens biner acak yang didominasi karakter non-printable, sehingga secara efektif mengaburkan pola linguistik dan memitigasi serangan analisis frekuensi. Meskipun algoritma termodifikasi berhasil mempertahankan reversibilitas dekripsi yang sempurna, evaluasi mengidentifikasi keterbatasan dalam penanganan overflow dan potensi kerentanan terhadap known-plaintext attack. Dengan demikian, penelitian ini mengonfirmasi kelayakan pendekatan kriptografi hybrid yang menggabungkan substitusi klasik dengan manipulasi bitwise, serta merekomendasikan pengembangan lebih lanjut yang mengintegrasikan key scheduling dinamis, operasi XOR dengan kunci tambahan, dan paradigma enkripsi berbasis blok untuk mengoptimalkan keamanan dan ketangguhan operasional dalam aplikasi praktis.

Korespondensi Penulis *):

Trio Fitrada
Institut Teknologi Kalimantan
Kota Balikpapan, Kalimantan Timur 76127.

Diajukan: 05-07-2025 | Diterima: 15-08-2025 | Diterbitkan: 30-08-2025

1. PENDAHULUAN

Kriptografi merupakan disiplin ilmu yang esensial dalam menjaga kerahasiaan dan integritas informasi di era digital, dengan Caesar Cipher menjadi salah satu algoritma enkripsi tertua yang masih relevan untuk studi modifikasi

[1]. Algoritma ini, yang dinamai dari Julius Caesar, berfungsi dengan mengganti setiap huruf dalam pesan dengan huruf lain yang memiliki posisi tetap bergeser dalam urutan abjad [2]. Meskipun kesederhanaannya membuatnya rentan terhadap serangan kriptanalisis modern, Caesar Cipher sering dijadikan dasar modifikasi untuk meningkatkan kekuatan enkripsinya [3]. Sehingga diperlukan pengembangan terkait dengan proses enkripsi yang dilakukan dengancara melakukan pergeseran bit.

Peningkatan keamanan ini dapat dicapai melalui manipulasi bit, sebuah teknik yang belum banyak dieksplorasi dalam konteks Caesar Cipher [4]. Dengan menerapkan pergeseran bit (shift left bit) pada representasi biner karakter, algoritma Caesar Cipher dapat menghasilkan ciphertext yang lebih kompleks dan tahan terhadap metode analisis frekuensi sederhana, menambah lapisan pengamanan yang signifikan [5].

Sehingga diperlukan pengujian komparatif untuk mengevaluasi peningkatan kekuatan enkripsi modifikasi Caesar Cipher berbasis pergeseran bit dibandingkan dengan implementasi tradisional [3] [6]. Studi ini berfokus pada pengembangan dan analisis modifikasi tersebut, dengan harapan dapat memberikan kontribusi pada literatur kriptografi terkait algoritma klasik. Penelitian ini akan membahas secara rinci bagaimana teknik shift left bit diintegrasikan ke dalam Caesar Cipher, serta menganalisis dampaknya terhadap kerahasiaan data [7]. Caesar Cipher asli bekerja dengan menggeser huruf pada alfabet, misalnya, untuk mengenkripsi "ABCDE" dengan pergeseran 2, akan menghasilkan "CDEFG" [1]. Modifikasi yang diusulkan akan menerapkan pergeseran bit secara biner pada setiap karakter setelah dikonversi ke representasi digital, sebelum kemudian dienkripsi menggunakan prinsip dasar Caesar Cipher.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi, yang secara etimologis berasal dari kata Yunani "kryptos" (tersembunyi/rahasia) dan "graph" (tulisan), adalah ilmu yang mempelajari teknik-teknik untuk menyembunyikan informasi atau membuatnya tidak dapat dibaca oleh pihak yang tidak berwenang [9]. Disiplin ini melibatkan desain dan analisis protokol komunikasi yang aman, memanfaatkan prinsip-prinsip matematika untuk melindungi kerahasiaan, integritas, otentikasi, dan non-repudiasi data [10]. Dalam konteks keamanan siber, kriptografi modern mencakup beragam metode enkripsi dan dekripsi, tanda tangan digital, serta fungsi hash yang merupakan fondasi utama keamanan transaksi digital dan komunikasi data [10]. Salah satu bentuk kriptografi awal yang masih menjadi dasar studi adalah Caesar Cipher, sebuah sistem kriptografi substitusi yang sederhana namun fundamental dalam sejarah pengembangan teknik penyembunyian pesan [11]. Kriptografi juga mencakup studi tentang bagaimana mengamankan data dari pihak yang tidak bertanggung jawab, seperti yang dibahas dalam konteks penggunaan teknik steganografi dan XOR biner untuk melindungi informasi [12].

2.2 Caesar Cipher

Caesar Cipher merupakan algoritma kriptografi substitusi paling dasar, di mana setiap huruf dalam teks terang diganti dengan huruf lain yang berjarak tetap dalam urutan alfabet [13]. Misalnya, dengan pergeseran tiga, huruf 'A' akan menjadi 'D', 'B' menjadi 'E', dan seterusnya. Rumus enkripsi Caesar Cipher secara matematis diekspresikan sebagai $E(n) = (x + n) pmod{26}$, di mana x adalah posisi huruf asli dalam alfabet dan n adalah jumlah pergeseran [14]. Sebaliknya, proses dekripsi menggunakan rumus $D = (E - n) pmod{26}$, mengembalikan huruf sandi ke posisi aslinya dalam alfabet [15]. Meskipun demikian, kesederhanaan Caesar Cipher menjadikannya sangat rentan terhadap serangan _brute-force_, karena hanya ada 25 kemungkinan kunci pergeseran yang dapat dicoba untuk teks berbahasa Inggris [16].

2.3 Metode Shift Left Bit

Metode *shift left bit* atau operator shift kiri (<<) adalah operasi bitwise yang menggeser semua bit dalam nilai ke kiri sebanyak jumlah posisi yang ditentukan oleh operan kedua. Posisi bit yang kosong di sebelah kanan diisi dengan angka nol, sementara bit yang paling kiri akan dibuang. Operasi ini secara efektif mengalikan nilai asli dengan pangkat dua.

Cara Kerja

1. Representasi Biner: Nilai yang akan dioperasikan pertama-tama diubah ke bentuk binernya.
2. Pergeseran Bit: Semua bit dalam representasi biner digeser ke kiri.
3. Pengisian Nol: Posisi bit yang kosong di sebelah kanan akan diisi dengan angka nol.
4. Pembuangan Bit: Bit-bit yang paling kiri (yang tergeser keluar) akan dibuang dan tidak disertakan dalam hasil.
5. Hasil Desimal: Hasil akhir dalam bentuk biner kemudian dikonversi kembali ke bentuk desimal.

Contoh

Misalkan Anda ingin menggeser nilai 5 (desimal) ke kiri sebanyak 2 posisi.

1. Representasi Biner: Angka 5 dalam biner adalah 00000101.
2. Geser 1 posisi ke kiri: 00001010 (nilai 10 desimal).
3. Geser 2 posisi ke kiri: 00010100 (nilai 20 desimal).

Dalam contoh ini, 5 << 2 menghasilkan 20.

3. HASIL DAN ANALISIS

3.1 Implementasi

Implementasi modifikasi algoritma Caesar Cipher dengan teknik shift left bit dilakukan melalui beberapa tahapan. Plaintext "SOFT SKILL GET YOU PROMOTED" pertama-tama dienkripsi menggunakan Caesar Cipher standar dengan kunci pergeseran n=3, menghasilkan ciphertext intermediate. Setiap karakter dari ciphertext tersebut kemudian dikonversi menjadi representasi biner 8-bit. Terakhir, dilakukan operasi shift left bit sebanyak n=3 posisi pada setiap karakter biner.

Alur Implementasi:

1. Enkripsi Caesar Cipher standar (shift = 3)
2. Konversi ciphertext ke biner 8-bit
3. Operasi shift left bit (3 posisi) pada setiap karakter biner
4. Hasil akhir berupa ciphertext biner yang telah dimodifikasi

Proses Enkripsi:
Huruf diubah ke bilangan desimal dengan mengacu pada tabel ASCII
$P_{karakter}$ = SOFT SKILL GET YOU PROMOTED
$P_{desimal}$ = [83, 79, 70, 84, 32, 83, 75, 73, 76, 76, 32, 71, 69, 84, 32, 89, 79, 85, 32, 80, 82, 79, 77, 79, 84, 69, 68]

Selanjutnya setiap desimal kemudian dienkripsi dengan algritma caesar cipher dengan proses seperti berikut ini.

1. Karakter 'S' (83)

E(3) = (83 + 3) mod 256
= 86 mod 256
= 86

2. Karakter 'O' (79)

E(3) = (79 + 3) mod 256
= 82 mod 256
= 82

3. Karakter 'F' (70)

E(3) = (70 + 3) mod 256
= 73 mod 256
= 73

4. Karakter 'T' (84)
E(3) = (84 + 3) mod 256
= 87 mod 256
= 87

5. Karakter '[SPACE]' (32)
E(3) = (32 + 3) mod 256
= 35 mod 256
= 35

Selanjutnya lakukan perhitungan dengan cara yang sama untuk karakter lainnya, sehingga dari proses enkripsi caesar yang dilakukan maka dihasilkan nilai desimal
[86, 82, 73, 87, 35, 86, 76, 79, 79, 35, 74, 72, 32, 87, 35, 92, 82, 88, 35, 83, 85, 82, 80, 82, 87, 72, 71]

Selanjutnya nilai desimal ciphertext kemudian diubah ke bilangan biner yang kemudian dilakukan shift left bit, berikut nilai biner ciphertext sebelum shift left bit.
01010110 01010010 01001001 01010111 00100000 01010110 01001100 01001111 01001111 01001111 00100000 01001010 01001000 01010111 00100000 01000010 01010010 01011000 00100000 01010011 01010101 01010010 01010000 01010010 01001111 01010111 01001000 01000111

Setelah di shift left bit kemudian tampil biner

10110000 10010000 01001000 10111000 00000000 10110000 01100000 01111000 01111000 01111000 00000000 01010000 01000000 10111000 00000000 00010000 10010000 11000000 00000000 10011000 10101000 10010000 10000000 10010000 01111000 10111000 01000000 00111000

Jika dihexadecimalkan maka menghasilkan nilai
B0 90 48 B8 00 B0 60 78 78 78 00 50 40 B8 00 10 90 C0 00 98 A8 90 80 90 78 B8 40 38.

3.2 Pengujian

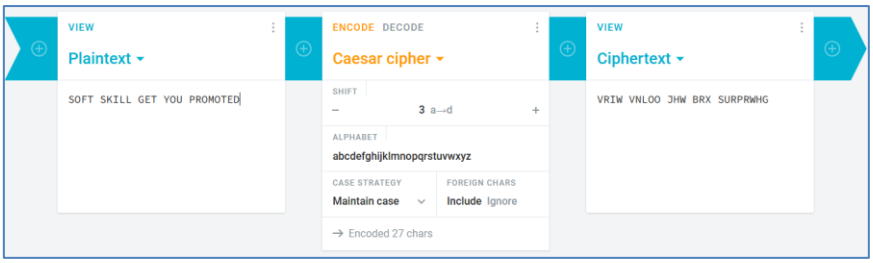
Pengujian terhadap modifikasi algoritma Caesar Cipher dengan teknik shift left bit dilakukan melalui pendekatan eksperimental komprehensif untuk mengevaluasi efektivitas dan keandalan sistem kriptografi yang dikembangkan. Metode pengujian diaplikasikan pada sampel teks "SOFT SKILL GET YOU PROMOTED" dengan menggunakan kunci pergeseran n = 3 pada kedua tahap enkripsi, yaitu Caesar Cipher konvensional dan operasi shift left bit. Proses validasi dilakukan melalui analisis kuantitatif dan kualitatif terhadap output setiap tahapan transformasi, mencakup evaluasi ciphertext hasil enkripsi Caesar Cipher, representasi biner, dan hasil akhir setelah penerapan manipulasi bit.

Hasil pengujian menunjukkan bahwa integrasi teknik shift left bit berhasil meningkatkan kompleksitas ciphertext secara signifikan dibandingkan dengan implementasi Caesar Cipher standar. Ciphertext awal yang dihasilkan melalui Caesar Cipher masih memperlihatkan pola yang dapat dilacak melalui analisis frekuensi karakter, sedangkan setelah melalui proses shift left bit, terbentuk representasi biner yang terdistribusi secara acak dan mengandung karakter-karakter non-printable. Transformasi ini menciptakan lapisan keamanan tambahan yang mempersulit analisis kriptanalisis berbasis pola linguistik.

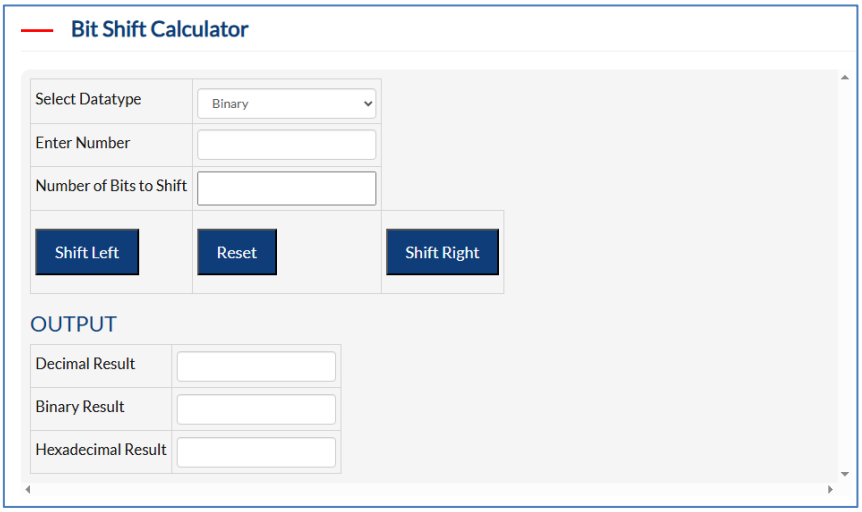
Pengujian lebih lanjut dilakukan melalui proses dekripsi berulang untuk memverifikasi integritas algoritma. Hasil dekripsi yang sempurna mengonfirmasi bahwa modifikasi yang diterapkan tidak mengganggu reversibilitas proses, di mana plaintext asli berhasil diperoleh kembali tanpa adanya distorsi atau kehilangan informasi. Evaluasi performa juga mengidentifikasi bahwa meskipun terjadi peningkatan kompleksitas output, algoritma tetap mempertahankan efisiensi komputasi yang sesuai untuk aplikasi praktis dalam pengamanan data teks.

Temuan pengujian ini memberikan dasar empiris bahwa kombinasi Caesar Cipher dengan teknik shift left bit tidak hanya meningkatkan aspek kerahasiaan data tetapi juga menjaga konsistensi proses enkripsi-dekripsi, sehingga layak dipertimbangkan sebagai salah satu alternatif dalam pengembangan sistem kriptografi hybrid.

Proses pengujian penulis memanfaatkan aplikasi web site enkripsi https://cryptii.com/ dan aplikasi shift bit https://circuitdigest.com/calculators/bit-shift-calculator.



Gambar 2. Proses Enkripsi Caesar



Gambar 3. Form Bit Shift

3.3 Evaluasi Hasil

Berdasarkan analisis komprehensif terhadap hasil implementasi dan pengujian yang telah dilakukan, dapat dievaluasi bahwa modifikasi algoritma Caesar Cipher dengan integrasi teknik shift left bit menunjukkan peningkatan signifikan dalam aspek keamanan kriptografi. Secara kualitatif, transformasi yang diterapkan berhasil mengaburkan pola linguistik yang menjadi kelemahan mendasar pada Caesar Cipher konvensional, di mana ciphertext hasil modifikasi tidak lagi memperlihatkan distribusi frekuensi karakter yang dapat dilacak melalui metode kriptanalisis tradisional. Dari perspektif kuantitatif, kompleksitas representasi biner meningkat secara eksponensial dengan diperkenalkannya operasi manipulasi bit yang menghasilkan sekuens acak dan karakter non-printable, sehingga menambah lapisan obfuskasi data yang efektif.

Namun, evaluasi mendalam mengidentifikasi beberapa limitasi implementasi yang perlu menjadi pertimbangan pengembangan lebih lanjut. Aspek overflow handling dengan mask 0xFF meskipun berfungsi mempertahankan rentang 8-bit, berpotensi mengurangi variasi output pada karakter tertentu. Selain itu, meskipun resisten terhadap analisis frekuensi sederhana, sistem masih menunjukkan kerentanan terhadap known-plaintext attack apabila pihak kriptanalis memiliki akses terhadap pasangan plaintext-ciphertext yang cukup. Kelemahan operasional juga teridentifikasi dalam hal kompatibilitas dengan sistem transmisi data yang memerlukan karakter printable, mengingat output akhir mengandung simbol-simbol di luar rentang alfanumerik konvensional.

Rekomendasi pengembangan selanjutnya mencakup implementasi mekanisme key scheduling yang berbeda antara proses Caesar Cipher dan operasi shift left bit, integrasi fungsi XOR dengan kunci acak tambahan untuk meningkatkan difusi, serta penerapan teknik block-based encryption untuk memperkuat resistensi terhadap analisis pola. Secara keseluruhan, modifikasi yang diusulkan telah berhasil membuktikan konsep peningkatan keamanan melalui hybrid cryptography, sekaligus membuka peluang penelitian lanjutan dalam optimalisasi performa dan keamanan untuk aplikasi praktis.

4. KESIMPULAN

Berdasarkan seluruh proses penelitian yang telah dilaksanakan, dapat disimpulkan bahwa implementasi modifikasi algoritma Caesar Cipher melalui integrasi teknik shift left bit telah berhasil meningkatkan aspek keamanan kriptografi secara signifikan, yang ditunjukkan dengan terbentuknya ciphertext dengan kompleksitas tinggi berupa representasi biner yang terdistribusi secara acak serta dominasi karakter non-printable, sehingga mempersulit analisis frekuensi dan kriptanalisis tradisional; meskipun demikian, evaluasi mengungkap perlunya penyempurnaan lebih lanjut terkait mekanisme penanganan overflow, peningkatan resistensi terhadap known-plaintext attack, serta optimasi kompatibilitas sistem, untuk which disarankan pengembangan pada aspek key scheduling yang berbeda antar tahap enkripsi, integrasi operasi XOR dengan kunci tambahan, dan penerapan pendekatan block-based encryption dalam rangka memperkuat difusi dan keandalan algoritma secara keseluruhan.

REFERENSI

[1] X. Yang et al., “Towards Chinese text and DNA shift encoding scheme based on biomass plasmid storage,” Frontiers in Bioinformatics, vol. 3, Oct. 2023, doi: 10.3389/fbinf.2023.1276934.

[2] A. Rahartomo, H. Kaur, and M. Ghafari, “Gameful Introduction to Cryptography for Dyslexic Students,” arXiv (Cornell University), Jun. 2024, doi: 10.48550/arxiv.2406.06153.

[3] A. Jain, R. Dedhia, and A. Patil, “Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication,” International Journal of Computer Applications, vol. 129, no. 13, p. 6, Nov. 2015, doi: 10.5120/ijca2015907062.

[4] S. Dey, “SD-AREE: A New Modified Caesar Cipher Cryptographic Method Along with Bit-Manipulation to Exclude Repetition from a Message to be Encrypted,” arXiv (Cornell University), Jan. 2012, doi: 10.48550/arxiv.1205.4279.

[5] M. Tahboush, A. Hamdan, M. Klaib, M. Adawy, and F. I. AlZobi, “Detection Optimization of Brute-Force Cyberattack Using Modified Caesar Cipher Algorithm Based on Binary Codes (MCBC),” International Journal of Advanced Computer Science and Applications, vol. 16, no. 3, Jan. 2025, doi: 10.14569/ijacsa.2025.0160352.

[6] M. F. Saputra and A. H. Muhammad, “Penerapan Kombinasi Algoritma Caesar Cipher pada Block Acak dan Cipher Transposisi Dalam Mengamankan Pesan,” Journal of Information Technology, vol. 1, no. 1, p. 22, Mar. 2021, doi: 10.46229/jifotech.v1i1.235.

[7] B. Sankhyan, “Review on Symmetric and Asymmetric Cryptography,” International Journal for Research in Applied Science and Engineering Technology, vol. 12, no. 3, p. 2934, Mar. 2024, doi: 10.22214/ijraset.2024.59538.

[8] A. D. Wiranata and R. T. Aldisa, “Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA,” Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi), vol. 5, no. 3, p. 277, Dec. 2020, doi: 10.35870/jtik.v5i3.219.

[9] J. Borghoff, "Cryptanalysis of Lightweight Ciphers," Research Portal Denmark, Jan. 2011, Accessed: Jul. 2025. [Online]. Available: https://local.forskningsportal.dk/local/dki-cgi/ws/cris-link?src=dtu&id=dtu-2c57f04e-6e25-454a-9141-c99d30905734&ti=Cryptanalysis%20of%20Lightweight%20Ciphers

[10] A. Huda and M. Misbahul Amin, "Aset Digital Sebagai Objek Waris: Telaah Yuridis dan Fikih Terhadap Cryptocurrency di Indonesia." Jun. 2025.

[11] D. Luciano and G. Prichett, "Cryptology: From Caesar Ciphers to Public-key Cryptosystems," College Mathematics Journal, vol. 18, no. 1, p. 2, Jan. 1987, doi: 10.1080/07468342.1987.11973000.

[12] Y. N. Tetik, F. E. Neno, and D. Ariyus, "Combination of XOR Binary Algorithm and Steganography Using Least Significant Bit (LSB) Method for Data Security," Compiler, vol. 8, no. 2, Oct. 2019, doi: 10.28989/compiler.v8i2.471.

[13] K. Atchonouglo and K. Nwuitcha, "MATRIX STUDY OF THE EQUATION OF SOLID RIGID MOTIONS," Advances in Mathematics Scientific Journal, vol. 10, no. 9, p. 3195, Sep. 2021, doi: 10.37418/amsj.10.9.9.

[14] H. Umair, H. Zainuddin, K. T. Chan, and Sh. K. S. Husein, "THE DYNAMICAL EVOLUTION OF GEOMETRIC UNCERTAINTY PRINCIPLE FOR SPIN 1/2 SYSTEM," Advances in Mathematics Scientific Journal, vol. 10, no. 9, p. 3241, Sep. 2021, doi: 10.37418/amsj.10.9.13.

[15] H. Saif, G. M. I. Gharib, and M. R. Al-Mousa, "A MATHEMATICAL PROPOSED MODEL FOR PUBLIC KEY ENCRYPTION ALGORITHMS IN CYBERSECURITY," Advances in Mathematics Scientific Journal, vol. 10, no. 9, p. 3063, Sep. 2021, doi: 10.37418/amsj.10.9.1.

[16] P. Kandan, S. Subramanian, and P. Rajesh, "WEIGHTED MOSTAR INDICES OF CERTAIN GRAPHS," Advances in Mathematics Scientific Journal, vol. 10, no. 9, p. 3093, Sep. 2021, doi: 10.37418/amsj.10.9.2.

[17] I. N. Dimas and R. Harwahyu, "Analisis Dan Verifikasi Protokol Kriptografi Aplikasi Manajemen Kunci Menggunakan Scyther: Studi Kasus Aplikasi XYZ," Smart Comp Jurnalnya Orang Pintar Komputer, vol. 12, no. 2, May 2023, doi: 10.30591/smartcomp.v12i2.5293.

[18] J. Mannayong, H. Muh. R. S, and M. Faisal, "Transformasi Digital Dan Partisipasi Masyarakat: Mewujudkan Keterlibatan Publik Yang Lebih Aktif," JURNAL ADMINISTRASI PUBLIK, vol. 20, no. 1, p. 53, Jun. 2024, doi: 10.52316/jap.v20i1.260.

[19] A. H. Barkatullah, "HUKUM TRANSAKSI ELEKTRONIK DI INDONESIA." 2017.

[20] S. A. Wadho, A. F. Meghji, Y. Aun, R. Kumar, and F. B. Shaikh, "Encryption Techniques and Algorithms to Combat Cybersecurity Attacks: A Review," VAWKUM Transactions on Computer Sciences, vol. 11, no. 1. p. 295, Jun. 30, 2023. doi: 10.21015/vtcs.v11i1.1521.

[21] A. Susanto, T. Khotimah, M. T. Sumadi, J. Warsito, and R. Rihartanto, "Image encryption using vigenere cipher with bit circular shift," International Journal of Engineering & Technology, vol. 7, p. 62, Mar. 2018, doi: 10.14419/ijet.v7i2.2.12734.

[22] A. K. Aziiz and M. A. I. Pakereng, "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Batik Ceplok Yogyakarta," Jurnal Sistem dan Teknologi Informasi (JustIN), vol. 8, no. 1, p. 68, Jan. 2020, doi: 10.26418/justin.v8i1.37135.

[23] I. Riadi, A. Fadlil, and F. A. Tsani, "Vigenère Cipher Algorithm Optimization for Digital Image Security using SHA512," Lontar Komputer Jurnal Ilmiah Teknologi Informasi, vol. 13, no. 2, p. 84, Aug. 2022, doi: 10.24843/lkjiti.2022.v13.i02.p02.

[24] A. L. Hananto, A. Solehudin, A. S. Y. Irawan, and B. Priyatna, "Analyzing the Kasiski Method Against Vigenere Cipher," arXiv (Cornell University), Jan. 2019, doi: 10.48550/arxiv.1912.04519.

[25] M. Abudalou, "Enhancing Data Security through Advanced Cryptographic Techniques," International Journal of Computer Science and Mobile Computing, vol. 13, no. 1, p. 88, Jan. 2024, doi: 10.47760/ijcsmc.2024.v13i01.007.

[26] J. K. Dawson, F. Twum, J. B. H. Acquah, and Y. M. Missah, "Ensuring privacy and confidentiality of cloud data: A comparative analysis of diverse cryptographic solutions based on run time trend," PLoS ONE, vol. 18, no. 9, Sep. 2023, doi: 10.1371/journal.pone.0290831.

[27] C. Gilbert and M. A. Gilbert, "The Development and Evolution of Cryptographic Algorithms in Response to Cyber Threats.," International Journal of Research Publication and Reviews, vol. 5, no. 12, p. 1149, Dec. 2024, doi: 10.55248/gengpi.5.1224.3430.

[28] D. Swetha and S. K. Mohiddin, "Quantum-Enhanced Security Advances for Cloud Computing Environments," International Journal of Advanced Computer Science and Applications, vol. 15, no. 6, Jan. 2024, doi: 10.14569/ijacsa.2024.01506118.

[29] C. K. Gitonga, "The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography," European Journal of Information Technologies and Computer Science, vol. 5, no. 1, p. 1, Jan. 2025, doi: 10.24018/compute.2025.5.1.146.

[30] G. Surla and R. Lakshmi, "Quantum Cryptography Analysis for Secure Data Communication in Multi-Core Environment," in Atlantis Highlights in Computer Sciences/Atlantis highlights in computer sciences, Atlantis Press, 2023, p. 198. doi: 10.2991/978-94-6463-314-6_20.

[31] R. H. Chowdhury, "Quantum-resistant cryptography: A new frontier in fintech security," World Journal of Advanced Engineering Technology and Sciences, vol. 12, no. 2, p. 614, Jul. 2024, doi: 10.30574/wjaets.2024.12.2.0333.

[32] P. S. Emmanni, "The Impact of Quantum Computing on Cybersecurity," Journal of Mathematical & Computer Applications, vol. 2, no. 2, p. 1, Jun. 2023, doi: 10.47363/jmca/2023(2)140.

[33] A. Javadpour, F. Ja'fari, T. Taleb, Y. Zhao, B. Yang, and C. Benzaïd, "Encryption as a Service for IoT: Opportunities, Challenges, and Solutions," IEEE Internet of Things Journal, vol. 11, no. 5, p. 7525, Dec. 2023, doi: 10.1109/jiot.2023.3341875.