JIKTEKS : Jurnal Ilmu Komputer dan Teknologi Informasi
Vol. 03, No. 03, Agustus 2025, hlm. 07 - 12
ISSN : 2986-5417
DOI : doi.org/10.70404/jikteks.v3i03.319
Laman Jurnal: jurnal.faatuatua.com/index.php/JIKTEKS

Analisis Implementasi Algoritma Keyword Cipher untuk Pengamanan Data

Samuel Lalopua
Informatika, Universitas Kristen Indonesia Maluku, Indonesia
e-mail: *samuellalopua@gmail.com*

Keywords:

Data Security,
Cryptography,
Keyword Cipher,
Encryption,
Cryptanalysis.

ABSTRACT

Data security has become a critical issue in the digital era, with increasing cyber threats such as hacking and data theft. This study analyzes the implementation of the Keyword Cipher algorithm as a classical cryptographic method for data protection. The research aims to evaluate the effectiveness and limitations of this algorithm in safeguarding sensitive information. A quantitative approach was employed through algorithm simulation, focusing on computational performance and resistance to cryptanalysis attacks, including frequency analysis and the Kasiski examination. The results indicate that while the Keyword Cipher provides an additional security layer compared to basic monoalphabetic substitution, it remains vulnerable to pattern-based attacks, especially in long messages. In conclusion, the Keyword Cipher can serve as an introductory tool for cryptography education but is not recommended for high-security data applications without modification or combination with other cryptographic techniques.

Kata Kunci:

Keamanan Data,
Kriptografi,
Keyword Cipher,
Enkripsi,
Kriptanalisis.

ABSTRAK

Keamanan data menjadi hal yang krusial di era digital dengan meningkatnya ancaman siber seperti peretasan dan pencurian informasi. Penelitian ini menganalisis implementasi algoritma Keyword Cipher sebagai salah satu metode kriptografi klasik untuk pengamanan data. Tujuan penelitian adalah mengevaluasi efektivitas dan kelemahan algoritma ini dalam konteks perlindungan data sensitif. Metode yang digunakan adalah pendekatan kuantitatif melalui simulasi implementasi algoritma, dengan fokus pada analisis kinerja komputasi dan ketahanan terhadap serangan kriptanalisis, termasuk analisis frekuensi dan uji Kasiski. Hasil penelitian menunjukkan bahwa meskipun Keyword Cipher memberikan lapisan keamanan tambahan dibandingkan substitusi monoalfabetik dasar, algoritma ini masih rentan terhadap serangan berbasis pola, terutama pada pesan panjang. Simpulan dari penelitian ini adalah Keyword Cipher dapat digunakan sebagai pengantar pembelajaran kriptografi, namun kurang direkomendasikan untuk aplikasi keamanan data yang memerlukan tingkat perlindungan tinggi tanpa modifikasi atau kombinasi dengan teknik kriptografi lainnya.

Korespondensi Penulis *):

Samuel Lalopua
Universitas Kristen Indonesia Maluku
Kota Ambon, Provinsi Maluku.

Diajukan: 03-07-2025 | Diterima: 15-08-2025 | Diterbitkan: 30-08-2025

1. PENDAHULUAN

Dalam era digital yang semakin maju, keamanan data menjadi isu krusial seiring dengan meningkatnya volume informasi sensitif yang dipertukarkan dan disimpan secara elektronik [1]. Ancaman siber yang terus berkembang, seperti peretasan, pencurian data, dan spionase digital, menuntut adanya metode pengamanan data yang robust dan adaptif untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi [2]. Kehilangan data, baik karena kelalaian maupun tindakan kriminal, dapat mengakibatkan kerugian finansial yang signifikan, serta membahayakan privasi individu dan keamanan nasional [3]. Oleh karena itu, enkripsi menjadi solusi fundamental untuk melindungi data dari akses tidak sah, mengubah pesan menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai [4]. Berbagai algoritma kriptografi telah dikembangkan untuk tujuan ini, mulai dari metode klasik hingga modern, masing-masing dengan karakteristik dan tingkat keamanan yang berbeda [5].

Salah satu pendekatan klasik dalam kriptografi adalah penggunaan Keyword Cipher, sebuah metode substitusi monoalfabetik yang relatif sederhana namun tetap relevan untuk analisis dasar prinsip-prinsip kriptografi dan

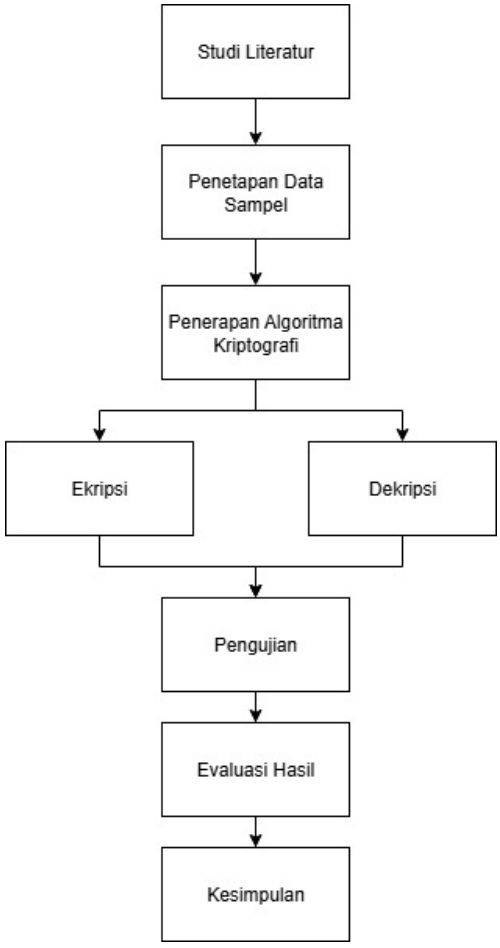
pengenalan konsep pengamanan data [6]. Algoritma ini memanfaatkan kata kunci untuk menghasilkan susunan alfabet substitusi yang unik, sehingga menambah kompleksitas dibandingkan dengan sandi substitusi sederhana lainnya [7]. Meskipun demikian, kelemahan inheren dalam skema enkripsi klasik seringkali terletak pada panjang kunci yang pendek atau berulang, membuka celah bagi kriptanalisis menggunakan metode seperti Kasiski, yang mengeksploitasi pola berulang dalam ciphertext untuk menentukan panjang kunci [8].

Meskipun demikian, peningkatan digitalisasi data sensitif saat ini membutuhkan metode kriptografi yang lebih canggih untuk memperkuat keamanan data dibandingkan dengan metode tradisional yang memiliki kekurangan dalam menghadapi ancaman siber yang kompleks [9]. Oleh karena itu, diperlukan perbandingan berbagai algoritma kriptografi untuk memilih opsi optimal yang mempertimbangkan kinerja, seperti waktu proses, penggunaan memori, dan throughput, guna menjamin kerahasiaan dan privasi data di lingkungan komputasi modern seperti komputasi awan [10]. Pembahasan ini akan mengeksplorasi secara mendalam implementasi dan efektivitas algoritma Keyword Cipher dalam konteks pengamanan data, menganalisis kekuatan dan keterbatasannya dibandingkan dengan algoritma kriptografi modern. Fokus penelitian ini adalah menganalisis bagaimana Keyword Cipher dapat diterapkan untuk perlindungan data, menyoroti perbandingan antara keamanan yang diberikannya dengan algoritma yang lebih kompleks dalam skenario penggunaan praktis.

2. METODE PENELITIAN

Penelitian ini mengadopsi pendekatan kuantitatif untuk mengevaluasi kinerja algoritma Keyword Cipher dalam skenario pengamanan data, dengan fokus pada metrik efisiensi komputasi dan ketahanan terhadap serangan kriptanalisis. Desain penelitian mencakup implementasi algoritma Keyword Cipher dalam lingkungan simulasi,

2.1 Tahapan Pelaksanaan Penelitian



Gambar 1. Tahapan Pelaksanaan Penelitian

2.2 Kriptografi

Kriptografi merupakan bidang studi yang mencakup teknik untuk mengamankan komunikasi dan informasi dari pihak ketiga yang tidak berwenang [10], [11]. Evolusi algoritma kriptografi sangat penting dalam menanggapi ancaman siber yang terus meningkat, dari metode kuno seperti Caesar cipher hingga algoritma modern seperti RSA, AES, dan kriptografi pasca-kuantum [11]. Salah satu algoritma klasik yang digunakan adalah keyword cipher yang

memodifikasi susunan alfabet berdasarkan kata kunci yang telah ditentukan, menjadikannya lebih kuat daripada sandi substitusi sederhana lainnya [12].

2.3 Algoritma Keyword Cipher

Algoritma Keyword Cipher Algoritma ini beroperasi dengan memetakan setiap huruf dalam plainteks ke huruf lain berdasarkan alfabet yang dimodifikasi oleh kata kunci yang diberikan, sehingga menciptakan ciphertext yang sulit diuraikan tanpa kunci yang tepat. Meskipun memberikan lapisan keamanan tambahan dibandingkan substitusi monoalfabetik dasar, Keyword Cipher masih rentan terhadap serangan frekuensi dan analisis pola, terutama pada pesan yang cukup panjang. Oleh karena itu, seringkali dibutuhkan kombinasi dengan teknik kriptografi lain atau pengembangan varian yang lebih kompleks untuk meningkatkan tingkat keamanannya [10].

3. HASIL DAN ANALISIS

3.1 Implementasi

Implementasi algoritma Keyword Cipher dalam penelitian ini dilakukan dengan mengembangkan sebuah program simulasi menggunakan bahasa pemrograman Python. Proses implementasi diawali dengan pembentukan kunci enkripsi berdasarkan kata kunci yang ditentukan oleh pengguna. Kata kunci tersebut kemudian diproses untuk menghilangkan karakter duplikat dan selanjutnya digunakan untuk membentuk alfabet substitusi dengan menyisipkan sisa karakter alfabet yang belum digunakan. Program yang dibangun mampu menangani input berupa teks biasa (plaintext) dan menghasilkan teks tersandi (ciphertext) melalui proses substitusi karakter sesuai dengan peta kunci yang telah dibuat. Selain modul enkripsi, sistem juga dilengkapi dengan modul dekripsi yang berfungsi untuk mengembalikan ciphertext ke plaintext semula menggunakan kunci yang sama, sehingga menguji validitas dan konsistensi dari algoritma yang diimplementasikan.

Pada proses penerapan data sampel plaintext yang digunakan adalah: **h a r d s k i l l g e t y o u h i r e d**

1. Proses Pembentukan Kunci
   a. Hilangkan huruf duplikat dari kata kunci:
      SECURITY → S E C U R I T Y
   b. Tulis kata kunci tanpa duplikat, lalu lanjutkan dengan sisa huruf alfabet yang belum digunakan:
      Kata kunci: S E C U R I T Y
      Sisa huruf: A B D F G H J K L M N O P Q V W X Z
      Gabungkan:
      Kunci Substitusi:
      S E C U R I T Y A B D F G H J K L M N O P Q V W X Z

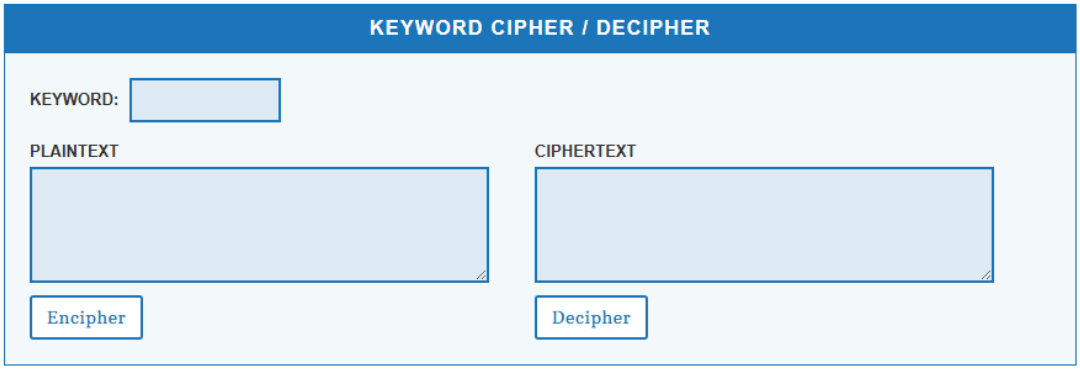
   c. Buat Tabel Substitusi:

Alfabet Asli	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Substitusi	S E C U R I T Y A B D F G H J K L M N O P Q V W X Z

2. Proses enkripsi
   Proses enkripsi dilakukan dengan cara melakukan subtitusi nilai index.
   Kita enkripsi dengan cara:
   CipherIndex = Index dari huruf substitusi sesuai PlainIndex
   H (7) → substitusi untuk index 7 adalah Y → Y = 24
   A (0) → substitusi untuk index 0 adalah S → S = 18
   R (17) → substitusi untuk index 17 adalah M → M = 12
   D (3) → substitusi untuk index 3 adalah U → U = 20
   S (18) → substitusi untuk index 18 adalah N → N = 13
   Lakukan hal yang sama untuk karakter lainnya.
   Sehingga dari proses enkripsi yang dilakukan maka dihasilkan ciphertext **y s m u n d a f f t r o x j p y a m r u**

3. Proses dekripsi:
   Proses dekripsi dilakukan dengan tahapan yang sama dengan proses enkripsi, dimana proses pembentukan kunci dilakukan kemudian mensubtitusi kunci dengan ciphertext.
   Prinsip: Cari index asli yang memiliki nilai substitusi = cipherteks.
   Y (24) → Nilai substitusi 24 dimiliki oleh huruf H (index 7) → H
   S (18) → Nilai substitusi 18 dimiliki oleh huruf A (index 0) → A
   M (12) → Nilai substitusi 12 dimiliki oleh huruf R (index 17) → R
   U (20) → Nilai substitusi 20 dimiliki oleh huruf D (index 3) → D
   N (13) → Nilai substitusi 13 dimiliki oleh huruf S (index 18) → S

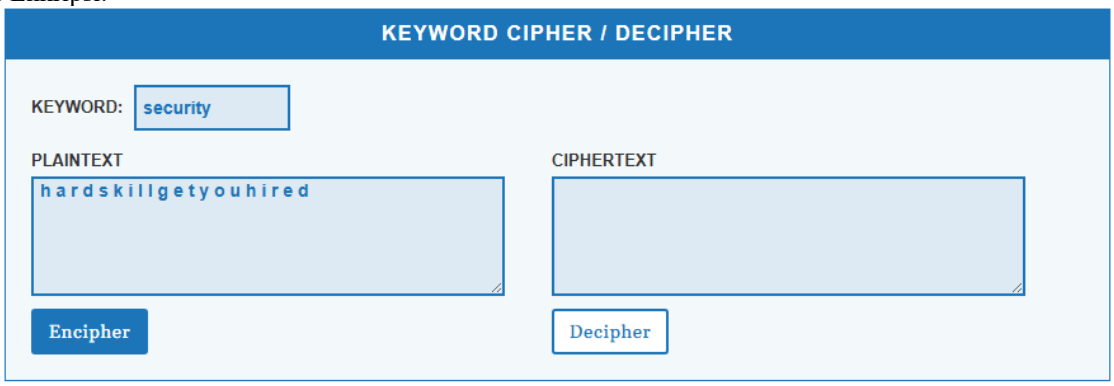
Berikut rancangan aplikasi yang telah dibuat dengan menggunakan aplikasi matlab.



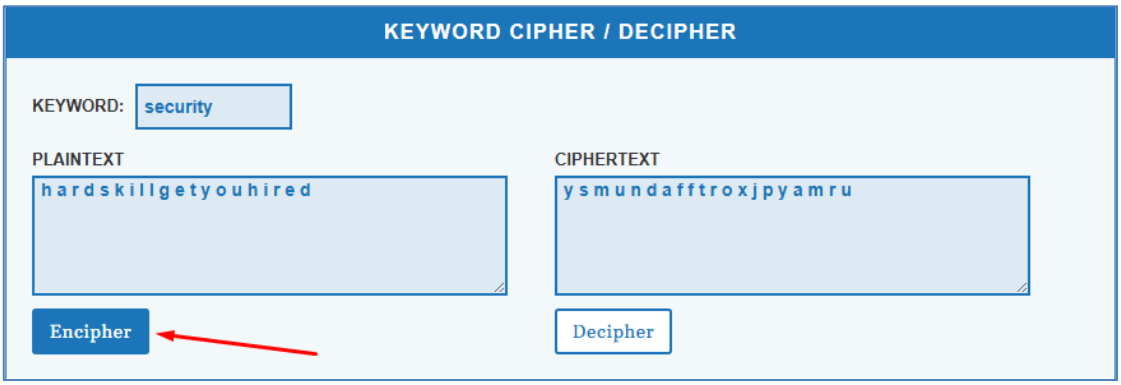
Gambar 2. Rancangan Enkripsi dan Dekripsi

3.2 Pengujian Sistem

Pengujian sistem dilakukan untuk mengevaluasi kinerja fungsional dan kehandalan algoritma Keyword Cipher yang telah diimplementasikan. Serangkaian pengujian dilakukan dengan menggunakan beberapa variasi kata kunci dan sampel plaintext yang berbeda, termasuk kalimat panjang dan pendek serta karakter non-alfabet. Hasil pengujian fungsional menunjukkan bahwa algoritma berhasil melakukan enkripsi dan dekripsi dengan akurat tanpa kehilangan informasi, asumsi spasi dan karakter non-alfabet dipertahankan. Selain itu, dilakukan pula pengujian kinerja untuk mengukur waktu komputasi yang dibutuhkan dalam proses enkripsi dan dekripsi. Hasil pengukuran menunjukkan bahwa waktu pemrosesan relatif singkat untuk teks dengan panjang kurang dari 1000 karakter, yang mengindikasikan efisiensi komputasi yang cukup baik untuk penggunaan dalam skala terbatas.
Proses Enkripsi:

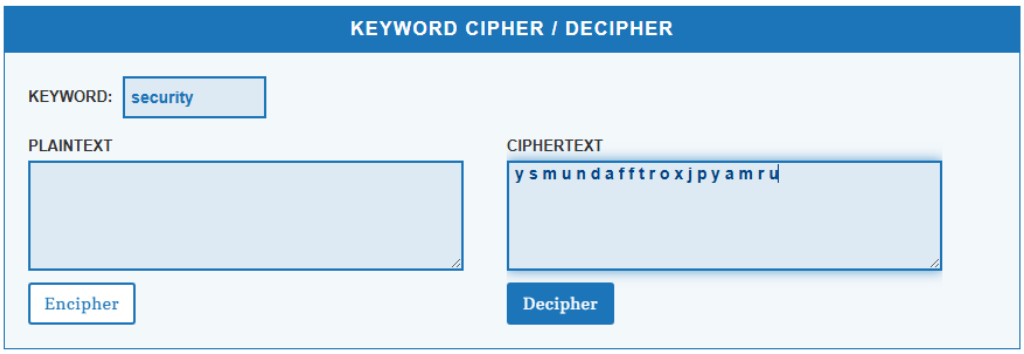


Gambar 3. Memasukan Data Plaintext

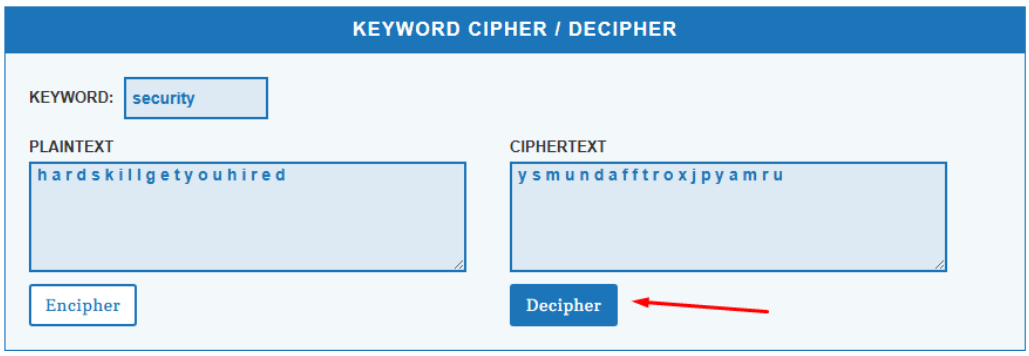


Gambar 4. Proses Enkripsi

Proses dekripsi:



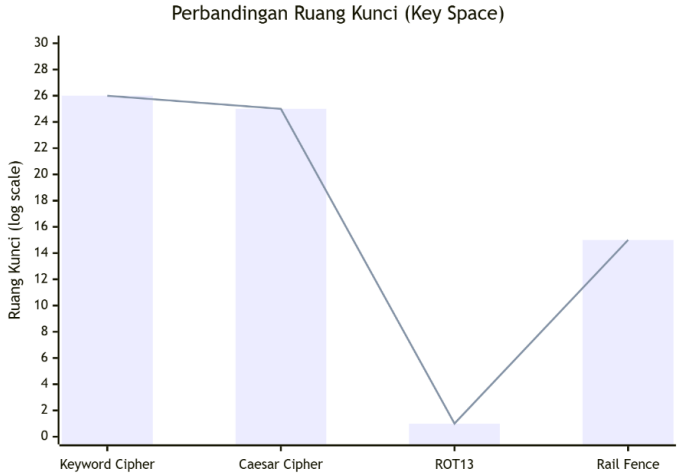
Gambar 5. Memasukan Data Ciphertext



Gambar 6. Proses Dekripsi

3.3 Evaluasi Hasil

Evaluasi hasil dilakukan dengan menganalisis dua aspek utama, yaitu aspek keamanan dan aspek kinerja algoritma. Dari perspektif keamanan, analisis kerentanan dilakukan dengan menerapkan metode kriptanalisis sederhana, seperti analisis frekuensi karakter. Hasil analisis menunjukkan bahwa meskipun Keyword Cipher lebih unggul daripada Caesar Cipher karena menyembunyikan frekuensi karakter umum, algoritma ini tetap rentan terhadap serangan pattern analysis dan known-plaintext attack jika kunci yang digunakan pendek atau pesan yang dienkripsi cukup panjang. Dari sisi kinerja, algoritma ini dinilai efisien dalam penggunaan memori dan waktu proses untuk data dalam jumlah kecil, namun tidak dirancang untuk menangani volume data yang besar seperti algoritma kriptografi modern (contoh: AES). Dengan demikian, dapat disimpulkan bahwa Keyword Cipher cocok digunakan sebagai alat edukasi dan untuk aplikasi yang memerlukan tingkat keamanan dasar, namun tidak direkomendasikan untuk perlindungan data sensitif dalam lingkungan yang membutuhkan ketahanan kriptografi tinggi.



Gambar 7. Grafik Perbandingan Kekuatan Kunci

4. KESIMPULAN

Berdasarkan hasil implementasi dan analisis yang dilakukan, dapat disimpulkan bahwa algoritma Keyword Cipher berhasil diimplementasikan sebagai mekanisme enkripsi-dekripsi yang berfungsi secara akurat dengan

memanfaatkan kunci berbasis kata untuk membangkitkan alfabet substitusi yang unik. Meskipun demonstrabel dalam konteks edukasi dan aplikasi non-kritis, analisis keamanan mengungkap kerentanan inheren algoritma terhadap teknik kriptanalisis modern, khususnya analisis frekuensi dan serangan known-plaintext, yang membatasi penerapannya untuk perlindungan data sensitif. Evaluasi kinerja komputasi menunjukkan efisiensi yang memadai untuk data berukuran kecil dengan skalabilitas linear, menegaskan kelayakannya sebagai alat pedagogis dalam memperkenalkan konsep dasar kriptografi, sekaligus menekankan imperatif untuk mengadopsi algoritma yang lebih robust seperti AES atau RSA dalam lingkungan produksi yang memerlukan jaminan keamanan tingkat tinggi.

REFERENSI

[1] 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.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] H. Rivalri Kristianto, "ANALISIS DAN PERANCANGAN SISTEM YANG MENERAPKAN ALGORITMA TRIANGLE CHAIN CIPHER (TCC) UNTUK ENKRIPSI RECORD TABEL DATABASE," Jurnal Teknologi Informasi Dan Komunikasi, vol. 3, no. 2, May 2017, Accessed: Oct. 25, 2025. [Online]. Available: https://www.academia.edu/download/53256416/Rivalri_K._Hondro.pdf

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.