Jurnal Minfo Polgan (JMP)
Volume 15, Nomor 2, Mei 2026
DOI : https://doi.org/10.33395/jmp.v15i2.16080
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Peningkatan Keamanan Data Digital Dengan Pendekatan Kombinasi Algoritma Kriptografi OTP dan Cramer Shoup

[1]Gilang Dwi Fahri Harahap, [2] Budi Triandi, [3]Lili Tanti
[1*,2,3]Ilmu Komputer/Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama, Medan, Indonesia
*Korespondensi: gilangdwifahri063@gmail.com

Submit : 11 April 2026 | **Diterima** : 15 Mei 2026 | **Terbit** : 28 Mei 2026

ABSTRACT

The security of digital data has become increasingly critical due to the rising number of cyber threats targeting confidentiality, integrity, and data availability. This study aims to enhance digital data security through a hybrid approach combining the One-Time Pad (OTP) and Cramer-Shoup cryptographic algorithms. OTP is theoretically unbreakable and ensures strong confidentiality; however, it has limitations in key distribution and vulnerability to attacks such as Known-Plaintext Attack (KPA) when keys are reused or improperly managed. Meanwhile, the Cramer-Shoup algorithm, an asymmetric cryptographic scheme, provides strong resistance against adaptive chosen-ciphertext attacks and supports secure key distribution and authentication. This research employs a system design and implementation approach using Python to develop a hybrid encryption model. The OTP algorithm is utilized for message encryption, while the Cramer-Shoup algorithm secures the key distribution process. System evaluation is conducted through simulation of KPA attacks and performance analysis of encryption and decryption processes. The results demonstrate that the proposed hybrid approach significantly improves data security by addressing the key distribution weakness of OTP and enhancing resistance to KPA attacks. Furthermore, the system maintains efficient performance in terms of computational time. In conclusion, the integration of OTP and Cramer-Shoup algorithms offers an effective and adaptive solution for securing digital data, contributing to the development of more robust cryptographic systems for modern cybersecurity applications..

Keywords*: Cryptography, One-Time Pad, Cramer-Shoup, hybrid encryption, data security*

ABSTRAK

Keamanan data digital menjadi aspek krusial seiring meningkatnya ancaman siber terhadap kerahasiaan dan integritas informasi. Penelitian ini bertujuan untuk meningkatkan keamanan data digital melalui pendekatan kombinasi algoritma kriptografi One-Time Pad (OTP) dan Cramer-Shoup dalam sebuah skema hybrid. Algoritma OTP memiliki keunggulan dalam menjaga kerahasiaan data secara teoritis, namun memiliki kelemahan pada distribusi kunci dan potensi serangan seperti Known-Plaintext Attack (KPA). Sementara itu, algoritma Cramer-Shoup sebagai kriptografi asimetris menawarkan keamanan yang kuat terhadap serangan adaptif serta mendukung autentikasi data. Metode penelitian yang digunakan meliputi perancangan sistem hybrid, implementasi algoritma menggunakan bahasa pemrograman Python, serta pengujian keamanan dan kinerja sistem. Proses enkripsi dilakukan dengan mengombinasikan OTP untuk penyandian pesan dan Cramer-Shoup untuk pengamanan distribusi kunci. Evaluasi dilakukan melalui simulasi serangan KPA dan analisis perbandingan waktu proses enkripsi-dekripsi. Hasil penelitian menunjukkan bahwa kombinasi kedua algoritma mampu meningkatkan tingkat keamanan data secara signifikan, terutama dalam mengatasi kelemahan distribusi kunci pada OTP dan meningkatkan ketahanan terhadap serangan KPA. Selain itu, sistem hybrid yang diusulkan tetap mempertahankan efisiensi kinerja yang baik. Dengan demikian, pendekatan kombinasi OTP dan Cramer-Shoup dapat menjadi solusi efektif dalam meningkatkan keamanan data digital serta memberikan kontribusi dalam pengembangan sistem kriptografi yang lebih adaptif dan andal.

Kata Kunci: Kriptografi, One-Time Pad, Cramer-Shoup, keamanan data, hybrid encryption

PENDAHULUAN

Di era digital yang berkembang pesat, data telah menjadi salah satu aset paling berharga dalam berbagai sektor kehidupan, seperti keuangan, kesehatan, pendidikan, dan pemerintahan. Transformasi digital yang masif memungkinkan proses pertukaran informasi berlangsung dengan cepat dan efisien, namun di sisi lain juga meningkatkan risiko terhadap ancaman keamanan siber (Disemadi et al., 2023; Setyowati et al., 2021). Berbagai jenis serangan seperti phishing, man-in-the-middle attack, brute force, hingga known-plaintext attack (KPA) menjadi ancaman nyata yang dapat merusak integritas serta kerahasiaan data (Chopra et al., 2024; Sorisa et al., 2024). Oleh karena itu, penguatan sistem keamanan data menjadi kebutuhan yang sangat penting dalam sistem informasi modern (Hoshmand et al., n.d.).

Salah satu pendekatan utama dalam menjaga keamanan data adalah dengan menggunakan kriptografi, yaitu teknik penyandian data agar hanya dapat diakses oleh pihak yang berwenang (Adee & Mouratidis, 2022; Genço?lu & Genço?lu, n.d.). Perkembangan kriptografi telah menghasilkan berbagai algoritma, baik yang bersifat simetris maupun asimetris, yang masing-masing memiliki kelebihan dan keterbatasan (Navid Bin Anwar et al., 2019; Kumar Sharma et al., 2021).

Algoritma kriptografi simetris seperti One-Time Pad (OTP) dikenal memiliki tingkat keamanan yang sangat tinggi secara teoritis karena tidak dapat dipecahkan apabila kunci yang digunakan benar-benar acak, sepanjang pesan, dan hanya digunakan satu kali. Namun, dalam praktiknya, OTP memiliki kelemahan utama pada distribusi dan manajemen kunci, serta rentan terhadap serangan jika terjadi penggunaan ulang kunci (Krianto Sulaiman et al., 2020; Shallal et al., 2016). Selain itu, beberapa penelitian juga menunjukkan bahwa penerapan OTP dalam berbagai sistem masih memerlukan penguatan pada aspek keamanan tambahan (Lestari et al., 2021).

Di sisi lain, algoritma kriptografi asimetris seperti Cramer-Shoup dikembangkan untuk meningkatkan keamanan terhadap serangan adaptive chosen-ciphertext, serta memberikan solusi yang lebih baik dalam distribusi kunci (Jain, 2017). Pendekatan ini didukung oleh perkembangan teori kriptografi modern dan penerapan konsep matematika seperti teorema bilangan prima dan Fermat dalam sistem keamanan (Samandari et al., 2023; Khoiruddin, 2016). Namun, algoritma asimetris umumnya memiliki kompleksitas komputasi yang lebih tinggi sehingga kurang efisien untuk pengolahan data dalam jumlah besar (Sarkar et al., 2024; Madhavan & Saxena, 2003).

Untuk mengatasi keterbatasan tersebut, pendekatan kriptografi hybrid dikembangkan dengan menggabungkan algoritma simetris dan asimetris guna memanfaatkan keunggulan masing-masing. Pendekatan ini terbukti mampu meningkatkan efisiensi sekaligus keamanan dalam berbagai implementasi sistem kriptografi modern (Sarumaha et al., 2023; Sarumaha et al., 2024). Selain itu, studi lain juga menunjukkan pentingnya integrasi berbagai teknik kriptografi dalam menghadapi ancaman keamanan yang semakin kompleks (Singh & Student, 2023; Radanliev, 2023).

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan pendekatan kriptografi hybrid dengan mengkombinasikan algoritma One-Time Pad (OTP) dan Cramer-Shoup untuk meningkatkan keamanan data digital. Pendekatan ini diharapkan mampu mengatasi kelemahan OTP dalam distribusi kunci, meningkatkan ketahanan terhadap serangan KPA, serta tetap mempertahankan efisiensi kinerja sistem.

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen dan simulasi untuk menganalisis tingkat keamanan serta efisiensi dari algoritma kriptografi yang diusulkan. Pendekatan yang digunakan adalah hybrid cryptography, yaitu kombinasi antara algoritma simetris One-Time Pad (OTP) dan algoritma asimetris Cramer-Shoup dalam satu sistem terpadu.

Tahapan penelitian dimulai dengan studi literatur untuk mengidentifikasi kelemahan dari masing-masing algoritma, khususnya terkait distribusi kunci pada OTP dan kompleksitas komputasi pada Cramer-Shoup. Selanjutnya dilakukan perancangan model sistem kriptografi hybrid yang mengintegrasikan kedua algoritma tersebut guna memanfaatkan keunggulan masing-masing.

Implementasi sistem dilakukan menggunakan bahasa pemrograman Python. Proses enkripsi diawali dengan penyandian plaintext menggunakan algoritma OTP untuk menghasilkan ciphertext. Selanjutnya, kunci OTP yang digunakan dalam proses tersebut dienkripsi menggunakan algoritma Cramer-Shoup dengan public key, sehingga menghasilkan cipherkey

yang aman untuk didistribusikan melalui media komunikasi yang tidak aman.
Pada tahap dekripsi, penerima akan menerima ciphertext dan cipherkey. Cipherkey kemudian didekripsi menggunakan private key Cramer-Shoup untuk memperoleh kembali kunci OTP. Kunci tersebut digunakan untuk mendekripsi ciphertext sehingga menghasilkan kembali plaintext asli secara utuh.

Pengujian sistem dilakukan melalui simulasi untuk mengevaluasi dua aspek utama, yaitu tingkat keamanan dan kinerja sistem. Pengujian keamanan difokuskan pada ketahanan terhadap serangan Known-Plaintext Attack (KPA), khususnya pada skenario penggunaan kunci OTP. Sementara itu, pengujian kinerja dilakukan dengan mengukur waktu proses enkripsi dan dekripsi guna mengetahui efisiensi sistem yang diusulkan.

Dengan metode ini, diharapkan dapat diperoleh sistem kriptografi hybrid yang tidak hanya meningkatkan keamanan data digital, tetapi juga tetap mempertahankan efisiensi dalam proses komputasi.

HASIL DAN PEMBAHASAN

Hasil Implementasi Sistem

Implementasi sistem dilakukan terhadap tiga skenario utama, yaitu penggunaan algoritma One-Time Pad (OTP), algoritma Cramer-Shoup, serta skema hybrid OTP–Cramer-Shoup. Pengujian dilakukan menggunakan data teks sepanjang 212 karakter.

Pada algoritma OTP, proses enkripsi menghasilkan waktu sebesar 0,001246 detik, sedangkan proses dekripsi membutuhkan waktu 0,002131 detik. Hasil ini menunjukkan bahwa OTP memiliki performa yang sangat cepat dalam proses enkripsi dan dekripsi karena menggunakan operasi sederhana berbasis XOR .

Pada algoritma Cramer-Shoup, waktu enkripsi tercatat sebesar 0,138612 detik, sedangkan waktu dekripsi sebesar 0,000043 detik. Hal ini menunjukkan bahwa proses enkripsi pada algoritma asimetris cenderung lebih lambat dibandingkan algoritma simetris karena melibatkan operasi matematika kompleks seperti eksponensiasi modular .

Pada skema hybrid OTP–Cramer-Shoup, waktu enkripsi sebesar 0,732833 detik dan waktu dekripsi sebesar 0,307569 detik. Waktu yang lebih tinggi dibandingkan OTP disebabkan oleh kombinasi dua proses, yaitu enkripsi pesan menggunakan OTP dan enkripsi kunci menggunakan Cramer-Shoup.

Analisis Kinerja Sistem

Berdasarkan hasil pengujian, dapat disimpulkan bahwa:

1. OTP memiliki kinerja tercepat, namun memiliki kelemahan pada distribusi kunci
2. Cramer-Shoup memiliki keamanan tinggi, tetapi kurang efisien untuk data besar
3. Hybrid OTP–Cramer-Shoup memberikan keseimbangan antara keamanan dan efisiensi

Meskipun waktu komputasi pada metode hybrid lebih tinggi, peningkatan tersebut masih dalam batas yang dapat diterima untuk sistem keamanan data. Hal ini karena Cramer-Shoup hanya digunakan untuk mengenkripsi kunci OTP yang berukuran kecil, sehingga tidak membebani sistem secara keseluruhan.

Pengujian Keamanan terhadap Known-Plaintext Attack (KPA)

Pengujian keamanan dilakukan untuk mengetahui ketahanan sistem terhadap serangan Known-Plaintext Attack (KPA). Pada algoritma OTP, serangan KPA dapat terjadi apabila kunci digunakan berulang, sehingga memungkinkan penyerang untuk menebak pola dan memperoleh plaintext. Namun, pada skema hybrid OTP–Cramer-Shoup, kunci OTP terlebih dahulu dienkripsi menggunakan algoritma Cramer-Shoup. Hal ini menyebabkan penyerang tidak dapat memperoleh kunci OTP meskipun berhasil melakukan analisis terhadap ciphertext.
Dengan demikian, sistem hybrid mampu menciptakan lapisan keamanan ganda, yaitu:

1. Lapisan pertama: enkripsi pesan menggunakan OTP
2. Lapisan kedua: pengamanan kunci menggunakan Cramer-Shoup

Pendekatan ini terbukti efektif dalam meningkatkan ketahanan terhadap serangan KPA, karena keberhasilan serangan pada satu lapisan tidak secara langsung membuka akses ke seluruh sistem.

Pengujian Keamanan terhadap Known-Plaintext Attack (KPA)

Pengujian keamanan dilakukan untuk mengetahui ketahanan sistem terhadap serangan Known-Plaintext Attack (KPA). Pada algoritma OTP, serangan KPA dapat terjadi apabila kunci digunakan

berulang, sehingga memungkinkan penyerang untuk menebak pola dan memperoleh plaintext. Namun, pada skema hybrid OTP–Cramer-Shoup, kunci OTP terlebih dahulu dienkripsi menggunakan algoritma Cramer-Shoup. Hal ini menyebabkan penyerang tidak dapat memperoleh kunci OTP meskipun berhasil melakukan analisis terhadap ciphertext.

Dengan demikian, sistem hybrid mampu menciptakan lapisan keamanan ganda, yaitu:
Lapisan pertama: enkripsi pesan menggunakan OTP
Lapisan kedua: pengamanan kunci menggunakan Cramer-Shoup
Pendekatan ini terbukti efektif dalam meningkatkan ketahanan terhadap serangan KPA, karena keberhasilan serangan pada satu lapisan tidak secara langsung membuka akses ke seluruh sistem.

Tabel 1. Perbandingan Waktu Enkripsi dan Dekripsi

Metode	Enkripsi (detik)	Dekripsi (detik)
One-Time Pad (OTP)	0,001246	0,002131
Cramer-Shoup	0,138612	0,000043
Hybrid OTP–Cramer-Shoup	0,732833	0,307569

Tabel 1 menyajikan hasil pengujian kinerja sistem berdasarkan waktu enkripsi dan dekripsi pada algoritma One-Time Pad (OTP), Cramer-Shoup, dan metode hybrid OTP–Cramer-Shoup. Pengujian dilakukan menggunakan data teks dengan panjang 212 karakter. Hasil menunjukkan bahwa OTP memiliki waktu proses tercepat, sedangkan metode hybrid membutuhkan waktu lebih tinggi akibat kombinasi dua algoritma, namun memberikan peningkatan pada aspek keamanan.

Pembahasan

Berdasarkan hasil pengujian yang disajikan pada Tabel 1, terlihat adanya perbedaan signifikan pada kinerja dan karakteristik masing-masing algoritma. Algoritma One-Time Pad (OTP) menunjukkan waktu enkripsi dan dekripsi yang paling cepat dibandingkan metode lainnya. Hal ini disebabkan oleh mekanisme OTP yang menggunakan operasi sederhana berupa XOR, sehingga tidak memerlukan komputasi kompleks. Namun, keunggulan tersebut tidak diimbangi dengan aspek keamanan pada distribusi kunci, yang menjadi kelemahan utama OTP dalam implementasi praktis.

Sebaliknya, algoritma Cramer-Shoup menunjukkan waktu enkripsi yang lebih tinggi dibandingkan OTP, meskipun waktu dekripsinya relatif sangat cepat. Hal ini disebabkan oleh penggunaan operasi matematika kompleks seperti eksponensiasi modular dalam proses enkripsi. Meskipun demikian, algoritma ini memiliki keunggulan dalam hal keamanan, khususnya dalam menghadapi serangan adaptive chosen-ciphertext, sehingga lebih andal dalam pengamanan kunci.

Pada metode hybrid OTP–Cramer-Shoup, waktu enkripsi dan dekripsi mengalami peningkatan dibandingkan kedua metode tunggal. Hal ini merupakan konsekuensi dari kombinasi dua proses kriptografi, yaitu enkripsi pesan menggunakan OTP dan pengamanan kunci menggunakan Cramer-Shoup. Meskipun demikian, peningkatan waktu tersebut masih dalam batas yang dapat diterima, mengingat ukuran data yang diuji relatif kecil dan Cramer-Shoup hanya digunakan untuk mengenkripsi kunci.

Dari sisi keamanan, metode hybrid menunjukkan keunggulan yang lebih signifikan. Penggunaan Cramer-Shoup untuk mengenkripsi kunci OTP mampu mengatasi kelemahan utama OTP dalam distribusi kunci. Selain itu, pendekatan ini juga meningkatkan ketahanan terhadap serangan Known-Plaintext Attack (KPA), karena penyerang tidak dapat memperoleh kunci meskipun memiliki akses terhadap sebagian plaintext dan ciphertext. Dengan demikian, sistem hybrid menciptakan mekanisme keamanan berlapis yang lebih sulit ditembus.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa pendekatan hybrid OTP–Cramer-Shoup mampu memberikan keseimbangan antara efisiensi dan keamanan. Metode ini tidak hanya mempertahankan kecepatan relatif dari algoritma simetris, tetapi juga memanfaatkan keunggulan keamanan dari algoritma asimetris, sehingga menjadi solusi yang efektif dalam pengamanan data digital.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa penerapan metode kriptografi hybrid dengan mengombinasikan algoritma One-Time Pad (OTP) dan Cramer-Shoup mampu meningkatkan keamanan data digital secara signifikan. Algoritma OTP terbukti memiliki keunggulan dalam kecepatan proses enkripsi dan dekripsi, namun memiliki kelemahan pada aspek distribusi kunci. Sementara itu, algoritma Cramer-Shoup menawarkan tingkat keamanan yang tinggi dalam pengamanan kunci, meskipun memiliki kompleksitas komputasi yang lebih besar. Kombinasi kedua algoritma dalam skema hybrid berhasil mengatasi kelemahan masing-masing metode, di mana OTP digunakan untuk menjaga kerahasiaan pesan, sedangkan Cramer-Shoup digunakan untuk mengamankan distribusi kunci. Hasil pengujian menunjukkan bahwa meskipun waktu komputasi metode hybrid lebih tinggi dibandingkan metode tunggal, peningkatan tersebut masih dalam batas yang dapat diterima dengan mempertimbangkan peningkatan keamanan yang diperoleh. Selain itu, metode yang diusulkan terbukti lebih tahan terhadap serangan Known-Plaintext Attack (KPA), karena kunci OTP tidak didistribusikan secara langsung, melainkan dienkripsi terlebih dahulu menggunakan Cramer-Shoup. Dengan demikian, pendekatan hybrid ini mampu memberikan mekanisme keamanan berlapis yang lebih kuat. Secara keseluruhan, penelitian ini memberikan kontribusi dalam pengembangan sistem kriptografi yang lebih aman dan adaptif, serta dapat menjadi alternatif solusi dalam pengamanan data pada berbagai aplikasi berbasis teknologi informasi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Allah SWT atas segala berkah dan karunia-Nya, yang memungkinkan penelitian ini selesai dengan sukses. Penulis juga mengucapkan terima kasih kepada semua yang telah membantu, membimbing, atau mendukung mereka selama proses penelitian, terutama dosen pembimbing yang telah memberikan nasihat dan umpan balik yang berguna. Sebagai kesimpulan, penulis berharap bahwa penelitian ini akan memberikan manfaat dan kemajuan dalam bidang pengetahuan, terutama dalam keamanan data dan kriptografi.

REFERENSI

Radanliev, P. (2023). Cryptography romance and war. https://doi.org/10.20944/preprints202310.0106.v1

Samandari, N., Olfat, J. A., Rafi, R., Zahirzai, M., Nazari, M., Azizi, Z., & Niazi, M. J. (2023). Applications of Fermat's little theorem. Turkish Journal of Computer and Mathematics Education, 14(3).

Sarkar, B., Saha, A., Dutta, D., De Sarkar, G., & Karmakar, K. (2024). A survey on the Advanced Encryption Standard (AES): A pillar of modern cryptography. International Journal of Computer Science and Mobile Computing, 13(4), 68–87.

Sarumaha, D., Mardiah, M., Amir, S., Gafur, A., & Zega, I. (2024). Penerapan algoritma enhanced dual Rivest Shamir Adleman untuk pengamanan data. Digital Transformation Technology, 4(1), 34–41.

Sarumaha, D., Budiman, M. A., & Zarlis, M. (2023). Performance analysis of hybrid cryptographic algorithms Rabbit Stream and enhanced dual RSA. Data Science: Journal of Computing and Applied Informatics, 7(1), 35–43.

Setyowati, W., Widayanti, R., & Supriyanti, D. (2021). Implementation of e-business information system in Indonesia: Prospects and challenges. International Journal of Cyber and IT Service Management, 1(2).

Shallal, Q. M., Bokhari, M. U., & Shallal, Q. M. (2016). A review on symmetric key encryption techniques in cryptography. International Journal of Computer Applications, 147(10).

Singh, R., & Student, A. (2023). Cryptography and encryption: Protecting digital information. International Journal of Novel Research and Development, 8(7).

Sorisa, C., et al. (2024). Etika keamanan siber: Studi kasus kebocoran data BPJS Kesehatan di Indonesia. Jurnal Sains Student Research, 2(6), 586–593.

Setyowati, W., Widayanti, R., & Supriyanti, D. (2021). Implementation Of E-Business Information System In Indonesia : Prospects And Challenges. In International Journal of Cyber and IT Service Management (IJCITSM) (Vol. 1, Issue 2). https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/49

Shallal, Q. M., Bokhari, M. U., & Shallal, Q. M. (2016). A Review on Symmetric Key Encryption Techniques in Cryptography. In Article in International Journal of Computer Applications International Journal of Computer Applications (Vol. 147, Issue 10). https://www.researchgate.net/publication/333118027

Singh, R., & Student, A. (2023). Cryptography and Encryption: Protecting Digital Information. In IJNRD.ORG IJNRD2307055 International Journal of Novel Research and Development (Vol. 8, Issue 7). www.ijnrd.org

Sorisa, C., Palangka, U., Cindi, R., Kiareni, L., Paalngka, U., Jadiaman, R., Universitas, P., Raya, P., Timang, J. H., & Tengah, K. (2024). Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia. Jurnal Sains Student Research, 2(6), 586–593. https://doi.org/10.61722/jssr.v2i6.2996

Taqwim, M. A., Kusyanti, A., & Siregar, R. A. (2021). Implementasi Algoritme Speck Untuk Enkripsi One-Time Password Pada Two-Factor Authentication (Vol. 5, Issue 7). http://j-ptiik.ub.ac.id

Thilagavathy, D. ., Babu, P. Srinivasa., & Adhiyamaan College of Engineering, . (2014). 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE) : 17 & 18 November 2014, venue, Adhiyamaan College of Engineering. IEEE.