JAINS (Journal of Artificial Intelligence and Network Systems)
Vol. 1 No. 2, Januari 2026

KAJIAN LITERATUR DAN ANALISIS KEAMANAN PROTOKOL DIFFIE HELLMAN DAN AGORITMA ELGAMAL PADA KRIPTOGRAFI KUNCI PUBLIK

ADE APRILLA[1)], DIANOVA DWI SYAFITRI[2)], NASYWA SALSABILA[3)], NOVRIANA SAHERA BR.PURBA[4)], ACHMAD FAUZI[5*)]

[1,2,3,4,5)]STMIK Kaputama
Jl. Veteran No 4A, Tangsi,Kec. South Binjai , Binjai City, North Sumatra 20714
Email: adeaprilla615@gmail.com

ABSTRACT

Public key cryptography is a fundamental component of modern information security systems that enables secure data communication over open networks. Two cryptographic algorithms that play a significant role in this domain are the Diffie Hellman key exchange protocol and the ElGamal encryption algorithm. The Diffie Hellman protocol allows two parties to establish a shared secret key without prior key exchange, with its security relying on the computational complexity of the discrete logarithm problem. The ElGamal algorithm is developed based on the principles of Diffie Hellman and provides an asymmetric encryption mechanism designed to ensure data confidentiality. The application of various cryptographic techniques is required to guarantee that the encryption process operates effectively and reliably.This study presents a comprehensive literature review of the Diffie Hellman protocol and the ElGamal algorithm and conducts a comparative analysis based on performance, security level, computational cost, and applicability. In addition, key characteristics of encryption algorithms such as encryption efficiency, key exchange speed, computational overhead, and resistance to quantum computing threats are discussed. This review also examines prior studies published between 2010 and 2024 to identify developments and enhancements that have been proposed for both algorithms.

Keywords: Diffie–Hellman, ElGamal, Public Key Cryptography, Encryption

1. PENDAHULUAN

Perkembangan pesat jaringan komunikasi dan layanan digital telah meningkatkan kebutuhan akan sistem keamanan data yang andal. Informasi sensitif kini banyak ditransmisikan melalui jaringan publik, sehingga aspek kerahasiaan, integritas, dan privasi data menjadi perhatian utama. Tanpa mekanisme keamanan yang memadai, data yang dikirimkan berpotensi disadap, dimodifikasi, atau disalahgunakan oleh pihak yang tidak berwenang.

Enkripsi merupakan teknik utama dalam melindungi informasi dengan cara mengubah data yang dapat dibaca menjadi bentuk tersandi yang tidak dapat dipahami tanpa kunci yang sesuai. Secara umum, algoritma enkripsi diklasifikasikan menjadi dua jenis, yaitu enkripsi simetris dan enkripsi asimetris. Enkripsi simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan enkripsi asimetris menggunakan sepasang kunci yang saling berkaitan secara matematis, yaitu kunci publik dan kunci privat.

Algoritma enkripsi simetris yang umum digunakan antara lain Data Encryption Standard (DES) dan Advanced Encryption Standard (AES). Sementara itu, algoritma enkripsi asimetris yang banyak diterapkan dalam sistem keamanan modern meliputi RSA, Diffie Hellman, dan ElGamal. Kriptografi kunci publik menjadi fondasi

utama dalam berbagai protokol keamanan, di mana Diffie Hellman dan ElGamal berperan penting dalam membangun komunikasi yang aman.

2. METODOLOGI PENELITIAN

2.1 Dasar Teoritis Metode

Protokol pertukaran kunci Diffie Hellman diperkenalkan untuk mengatasi permasalahan distribusi kunci dalam komunikasi yang aman. Protokol ini memungkinkan dua pihak untuk menghasilkan sebuah kunci rahasia bersama melalui saluran komunikasi yang tidak aman tanpa harus mengirimkan kunci tersebut secara langsung. Kunci rahasia yang dihasilkan selanjutnya dapat digunakan dalam algoritma enkripsi simetris untuk melindungi pertukaran pesan.

Salah satu tantangan utama dalam sistem komunikasi aman adalah pengelolaan kunci, terutama ketika jumlah pengguna dalam jaringan terus bertambah. Metode konvensional yang memerlukan kunci unik untuk setiap pasangan pengguna menjadi tidak efisien dan sulit dikelola. Oleh karena itu, protokol Diffie Hellman menawarkan solusi yang lebih praktis dengan mengurangi kompleksitas distribusi kunci.

Meskipun demikian, protokol Diffie Hellman memiliki kelemahan, khususnya kerentanannya terhadap serangan man in the middle apabila tidak dilengkapi dengan mekanisme autentikasi. Untuk mengatasi permasalahan ini, berbagai metode penguatan keamanan telah diusulkan, seperti integrasi dengan sertifikat digital dan protokol autentikasi. Walaupun memiliki keterbatasan, Diffie Hellman tetap menjadi kontribusi penting dalam dunia kriptografi dan banyak digunakan dalam protokol keamanan modern.

3. HASIL DAN PEMBAHASAN

3.1 Algoritma Enkripsi ElGamal

Algoritma ElGamal merupakan algoritma enkripsi asimetris yang tingkat keamanannya didasarkan pada kesulitan penyelesaian masalah logaritma diskret dalam grup siklik berhingga. Algoritma ini diperkenalkan pada pertengahan tahun 1980 an dan hingga kini masih digunakan secara luas dalam sistem enkripsi dan tanda tangan digital.

Berbeda dengan protokol pertukaran kunci, algoritma ElGamal secara langsung menyediakan mekanisme enkripsi dan dekripsi data. Proses enkripsi dilakukan menggunakan kunci publik, sedangkan proses dekripsi menggunakan kunci privat, sehingga hanya pihak yang berwenang yang dapat mengakses pesan asli.

3.2 Pembangkitan Kunci

Tahap pembangkitan kunci pada algoritma ElGamal melibatkan pemilihan bilangan prima berukuran besar, pemilihan generator pada grup siklik, serta penentuan kunci privat secara acak. Selanjutnya, kunci publik dihitung berdasarkan parameter-parameter tersebut dan dapat dibagikan secara terbuka, sementara kunci privat harus dijaga kerahasiaannya.

3.3 Proses Enkripsi

Pada proses enkripsi, pesan dalam bentuk plainteks dienkripsi menggunakan kunci publik penerima dan sebuah nilai acak. Hasil dari proses ini adalah sepasang nilai yang membentuk cipherteks.

3.3 Hasil dan Analisis

Hasil analisis menunjukkan bahwa sistem yang dirancang memiliki ketahanan yang kuat terhadap chosen ciphertext attack (IND CCA). Ketahanan ini diperoleh melalui integrasi varian ElGamal yang telah terbukti aman secara kriptografis serta penerapan mekanisme dekripsi termediatori. Dalam skema ini, ciphertext tidak dapat didekripsi secara langsung oleh pengguna tanpa keterlibatan SEM, sehingga meskipun penyerang berhasil memperoleh ciphertext, proses pemulihan plaintext tetap tidak dimungkinkan.

Selain itu, pembagian kunci privat menjadi dua bagian yang terpisah secara fisik dan logis meningkatkan keamanan sistem terhadap kompromi kunci. Apabila salah satu pihak mengalami kebocoran kunci, bagian kunci lainnya tetap tidak dapat digunakan untuk mendekripsi pesan secara utuh. Dengan demikian, sistem mampu meminimalkan risiko kebocoran data akibat serangan internal maupun eksternal.

3.4. Proses Dekripsi

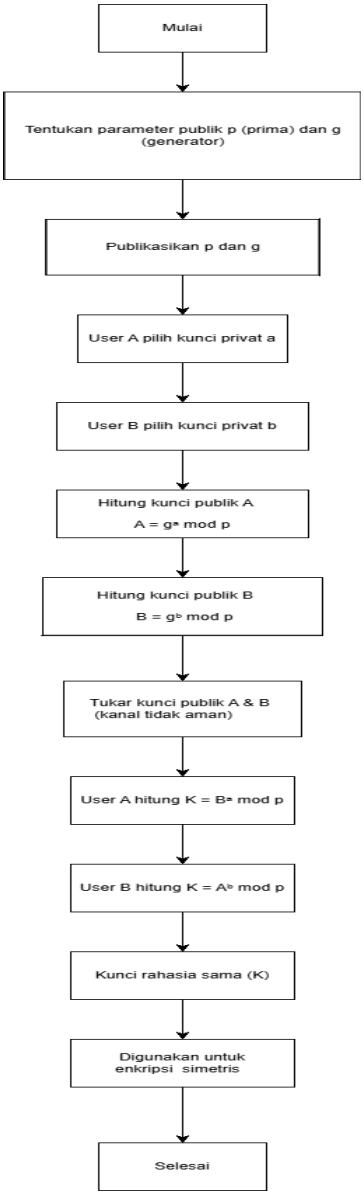
Pada proses enkripsi, pesan dalam bentuk plainteks dienkripsi menggunakan kunci publik penerima dan sebuah nilai acak. Hasil dari proses ini adalah sepasang nilai yang membentuk cipherteks.

3.4 Alur Proses Sistem (Flowchart)

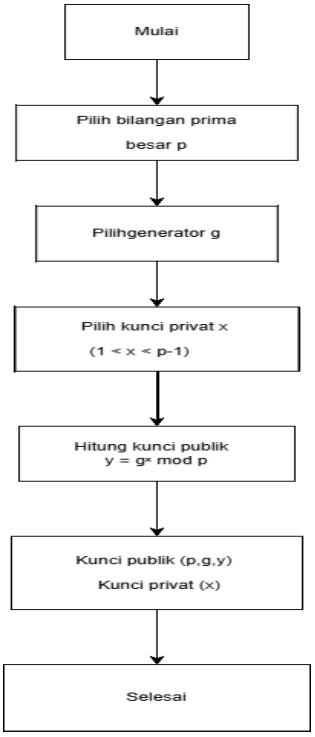
Alur kerja sistem diawali dengan tahap pembangkitan parameter kriptografi beserta kunci publik milik pengguna. Setelah parameter dan kunci tersedia, pihak pengirim melakukan proses enkripsi terhadap pesan menggunakan kunci publik tersebut sehingga menghasilkan ciphertext. Ciphertext yang terbentuk kemudian dikirimkan kepada pengguna dan selanjutnya diteruskan ke Security Entity Module (SEM) untuk menjalani proses dekripsi parsial.

SEM bertugas melakukan dekripsi parsial terhadap ciphertext dan mengirimkan hasil dekripsi tersebut kembali kepada pengguna. Pada tahap akhir, pengguna mengombinasikan hasil dekripsi parsial yang diperoleh dari SEM dengan hasil dekripsi parsial yang dilakukan secara mandiri untuk merekonstruksi plaintext asli. Mekanisme ini memastikan bahwa proses dekripsi hanya dapat diselesaikan apabila kedua hasil dekripsi parsial tersedia. Dengan demikian, apabila SEM tidak memberikan kontribusi dekripsi parsial, maka pesan tidak dapat didekripsi secara sempurna.

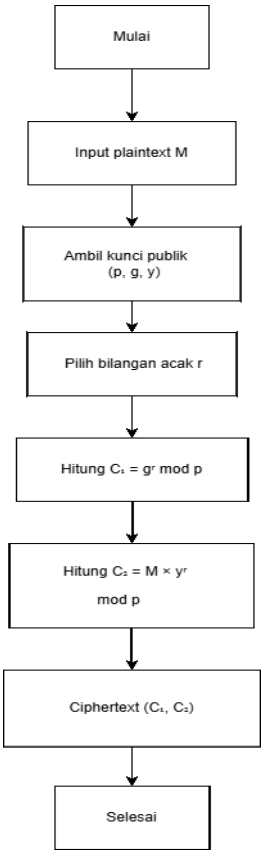
Secara umum, tahapan proses dalam sistem ini dapat diringkas ke dalam beberapa langkah utama, yaitu pembangkitan kunci, enkripsi pesan, pengiriman ciphertext, dekripsi parsial oleh SEM, serta penggabungan hasil dekripsi untuk memperoleh plaintext sebagai berikut:



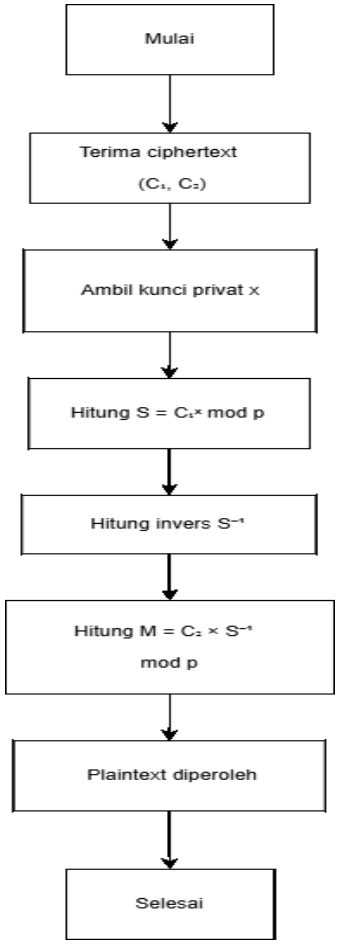
Gambar 3.1 Flowchart Protokol Diffie Hellman



Gambar 3.2 Pembangkitan Kunci ElGamal



Gambar 3.3 Proses Enkripsi ElGamal



Gambar 3.4 Proses Dekripsi ElGamal

3.4 Kontrol Akses dan Mekanisme Pencabutan Kunci

Salah satu kontribusi utama dari perancangan sistem ini adalah tersedianya mekanisme pencabutan akses secara cepat (*fast key revocation*). Pada skema kriptografi konvensional, pencabutan hak akses pengguna umumnya mengharuskan pembangkitan ulang pasangan kunci serta pendistribusian kembali kunci publik kepada seluruh entitas terkait. Proses tersebut tidak hanya meningkatkan beban administratif, tetapi juga berpotensi menimbulkan risiko keamanan tambahan.

Berbeda dengan pendekatan tersebut, skema yang diusulkan memungkinkan pencabutan akses dilakukan dengan menghentikan keterlibatan *Security Entity Mediator* (SEM) dalam proses dekripsi parsial. Ketika SEM tidak memberikan

hasil dekripsi parsial, pengguna tidak dapat merekonstruksi plaintext meskipun masih memiliki kunci dekripsi privat. Dengan demikian, sistem mampu menyediakan mekanisme kontrol akses yang lebih fleksibel, efisien, dan responsif, khususnya pada lingkungan organisasi dengan tingkat perubahan keanggotaan pengguna yang tinggi.

3.5 Efisiensi Komputasi

Dari perspektif efisiensi komputasi, hasil perancangan menunjukkan bahwa sistem tidak bergantung pada operasi *bilinear pairing* yang dikenal memiliki kompleksitas komputasi tinggi. Dengan mengadopsi varian ElGamal yang bersifat *pairing free*, sistem menjadi lebih ringan dibandingkan dengan skema kriptografi termediatori yang berbasis pairing.

Pendekatan ini menjadikan sistem lebih sesuai untuk diterapkan pada lingkungan dengan keterbatasan sumber daya komputasi tanpa mengurangi tingkat keamanan. Selain itu, berkurangnya kompleksitas komputasi berdampak positif terhadap waktu respons sistem, khususnya pada proses dekripsi bertahap yang melibatkan SEM dan pengguna.

3.6 Keandalan dan Integritas Sistem

Hasil evaluasi menunjukkan bahwa sistem memiliki tingkat keandalan yang tinggi dalam menjaga kerahasiaan dan integritas data. Proses dekripsi yang dilakukan secara kolaboratif memastikan bahwa tidak ada satu entitas pun yang memiliki kendali penuh dalam pemulihan plaintext. Hal ini secara signifikan mengurangi potensi penyalahgunaan hak akses oleh pihak internal yang tidak bertanggung jawab.

Selain itu, integritas pesan tetap terjaga karena setiap perubahan terhadap ciphertext akan menyebabkan kegagalan proses dekripsi. Dengan demikian, sistem tidak hanya menjamin kerahasiaan informasi, tetapi juga memastikan bahwa pesan yang diterima oleh pengguna merupakan pesan yang autentik dan tidak mengalami modifikasi selama proses transmisi, meskipun kondisi jaringan tidak selalu stabil.

3.7 Implikasi Penerapan Sistem

Berdasarkan hasil penelitian, skema *Security Mediated ElGamal* memiliki relevansi yang tinggi untuk diterapkan pada sistem yang membutuhkan tingkat keamanan yang ketat dan pengelolaan akses yang terkontrol. Contoh penerapannya meliputi sistem komunikasi internal organisasi, layanan berbasis *cloud computing*, serta lingkungan yang berada di bawah regulasi keamanan yang ketat.

Kombinasi antara mekanisme kontrol akses yang fleksibel dan efisiensi komputasi yang baik menjadikan skema ini sebagai alternatif yang kompetitif dibandingkan dengan pendekatan kriptografi konvensional.

3.8 Keterbatasan Sistem

Meskipun sistem menunjukkan berbagai keunggulan, terdapat beberapa keterbatasan yang perlu diperhatikan. Ketergantungan terhadap SEM menjadikan sistem memiliki satu entitas kepercayaan tambahan (*trusted entity*). Oleh karena itu, aspek keamanan dan keandalan SEM harus dijaga secara optimal agar tidak menjadi titik lemah sistem secara keseluruhan.

Selain itu, latensi komunikasi antara pengguna dan SEM berpotensi memengaruhi kinerja sistem, khususnya pada kondisi jaringan yang tidak stabil. Faktor ini perlu dipertimbangkan dalam implementasi praktis, terutama pada sistem berskala besar.

3.9 Diskusi Keseluruhan

Secara keseluruhan, hasil dan pembahasan menunjukkan bahwa sistem yang diusulkan berhasil mencapai tujuan utama perancangan, yaitu meningkatkan tingkat keamanan, menyediakan mekanisme pencabutan akses yang efisien, serta

mempertahankan efisiensi komputasi. Integrasi antara perlindungan kriptografis dan kontrol akses yang fleksibel menjadikan skema ini sebagai solusi yang layak dan efektif untuk mendukung komunikasi data yang aman, terkontrol, dan adaptif terhadap kebutuhan sistem modern.

3.10 PENELITIAN TERKAIT

Berbagai penelitian telah membahas pengembangan dan peningkatan protokol Diffie-Hellman dan algoritma ElGamal. Penelitian terkait Diffie Hellman umumnya berfokus pada peningkatan autentikasi, pengurangan kerentanan terhadap serangan, serta optimasi kinerja pada lingkungan dengan sumber daya terbatas. Di sisi lain, pengembangan ElGamal diarahkan pada pengurangan beban komputasi, penyederhanaan ukuran cipherteks, dan peningkatan ketahanan terhadap serangan kriptanalisis.

Selain itu, perkembangan komputasi kuantum mendorong penelitian lebih lanjut mengenai ketahanan algoritma kriptografi konvensional. Mengingat bahwa Diffie Hellman dan ElGamal bergantung pada masalah matematika yang berpotensi dapat diselesaikan secara efisien oleh komputer kuantum, berbagai pendekatan hibrida dan algoritma pasca kuantum mulai diusulkan sebagai solusi alternatif.

4. PEMBAHASAN

4.1 Analisis Perbandingan

Analisis perbandingan antara protokol Diffie Hellman dan algoritma ElGamal dilakukan berdasarkan beberapa kriteria utama.

4.2 Kinerja

Protokol Diffie Hellman umumnya memiliki kinerja yang lebih baik dalam hal pertukaran kunci karena membutuhkan sumber daya komputasi yang relatif lebih rendah. Sebaliknya, algoritma ElGamal memerlukan perhitungan tambahan dalam proses enkripsi dan dekripsi sehingga kinerjanya cenderung lebih lambat.

4.2 Keamanan

Kedua algoritma memiliki dasar keamanan yang sama, yaitu kesulitan penyelesaian masalah logaritma diskret. Namun, protokol Diffie Hellman memerlukan mekanisme autentikasi tambahan untuk mencegah serangan manin the middle. Algoritma ElGamal dianggap memiliki tingkat keamanan yang lebih tinggi untuk enkripsi data karena menggunakan nilai acak yang berbeda pada setiap proses enkripsi.

4.4 Biaya Komputasi

Algoritma ElGamal menghasilkan ukuran cipherteks yang lebih besar dan membutuhkan biaya komputasi yang lebih tinggi dibandingkan Diffie Hellman. Sementara itu, Diffie Hellman hanya berfokus pada pembentukan kunci rahasia tanpa melakukan enkripsi data secara langsung.

4.5 Kesesuaian Penerapan

Protokol Diffie Hellman sangat sesuai digunakan pada sistem yang memerlukan pertukaran kunci secara aman, seperti HTTPS dan Virtual Private Network (VPN). Algoritma ElGamal lebih cocok diterapkan pada sistem yang membutuhkan enkripsi asimetris dan pembuatan tanda tangan digital.

4.5.1 Analisis Keamanan

Analisis keamanan dilakukan untuk mengevaluasi tingkat ketahanan protokol Diffie-Hellman dan algoritma ElGamal terhadap berbagai ancaman kriptografis yang umum ditemukan pada sistem komunikasi modern. Evaluasi ini mencakup aspek kerahasiaan data, ketahanan terhadap serangan aktif dan pasif, serta kemampuan sistem dalam menghadapi perkembangan teknologi komputasi, termasuk komputasi kuantum.

4.5.2 Kerahasiaan Data

Protokol Diffie Hellman menjamin kerahasiaan kunci sesi yang dihasilkan melalui mekanisme pertukaran kunci tanpa pengiriman kunci secara langsung. Keamanan protokol ini bergantung pada kesulitan penyelesaian masalah logaritma diskret. Namun, Diffie Hellman tidak secara langsung menyediakan mekanisme enkripsi data, sehingga tingkat kerahasiaan pesan sangat bergantung pada algoritma enkripsi simetris yang digunakan setelah kunci sesi terbentuk.

Sebaliknya, algoritma ElGamal secara langsung menyediakan mekanisme enkripsi asimetris yang menjamin kerahasiaan data. Penggunaan bilangan acak yang berbeda pada setiap proses enkripsi menjadikan ciphertext ElGamal bersifat nondeterministik, sehingga lebih tahan terhadap analisis pola dan serangan berbasis pengulangan pesan.

4.5.3 Ketahanan terhadap Serangan Man-in-the-Middle

Salah satu kelemahan utama protokol Diffie Hellman adalah kerentanannya terhadap serangan *man in the middle* apabila tidak disertai mekanisme autentikasi. Penyerang dapat menyisipkan diri dalam proses pertukaran kunci dan membentuk dua kunci rahasia yang berbeda dengan masing-masing pihak tanpa terdeteksi.

Algoritma ElGamal relatif lebih aman dalam konteks ini karena digunakan langsung untuk enkripsi data dan tidak hanya berfokus pada pertukaran kunci. Meskipun demikian, implementasi ElGamal tetap memerlukan sistem manajemen kunci dan autentikasi yang baik untuk mencegah penyalahgunaan kunci publik palsu.

4.5.4 Ketahanan terhadap Serangan Kriptanalisis

Baik Diffie Hellman maupun ElGamal memiliki fondasi keamanan yang sama, yaitu kesulitan penyelesaian masalah logaritma diskret dalam grup siklik berhingga. Selama parameter kriptografi yang digunakan memiliki ukuran kunci yang cukup besar dan dipilih secara acak, kedua algoritma dianggap aman terhadap serangan kriptanalisis klasik.

Namun, ElGamal memiliki keunggulan tambahan karena menghasilkan ciphertext yang lebih bervariasi untuk pesan yang sama, sehingga lebih tahan terhadap serangan *chosen plaintext attack* (CPA) dibandingkan dengan skema deterministik.

4.5.5 Dampak Komputasi Kuantum

Perkembangan komputasi kuantum menjadi tantangan signifikan bagi algoritma kriptografi berbasis logaritma diskret. Algoritma Shor secara teoritis mampu memecahkan masalah logaritma diskret dalam waktu polinomial, yang berdampak langsung pada keamanan Diffie Hellman dan ElGamal.

Dalam konteks ini, kedua algoritma memiliki tingkat kerentanan yang relatif sama terhadap serangan kuantum. Oleh karena itu, implementasi praktis perlu mempertimbangkan integrasi dengan skema kriptografi pasca kuantum atau pendekatan hibrida guna mempertahankan keamanan jangka panjang.

4.5.6 Keamanan dalam Implementasi Sistem

Selain aspek teoritis, keamanan kedua algoritma sangat dipengaruhi oleh implementasi sistem. Penggunaan parameter yang lemah, bilangan acak yang tidak berkualitas, atau pengelolaan kunci yang buruk dapat menurunkan tingkat keamanan secara signifikan. Dalam konteks ini, ElGamal memerlukan perhatian khusus terhadap ukuran ciphertext dan efisiensi

penyimpanan, sedangkan Diffie Hellman memerlukan mekanisme autentikasi yang kuat.

5. KESIMPULAN

Penelitian ini menyajikan tinjauan ulang terhadap protokol pertukaran kunci Diffie Hellman dan algoritma enkripsi ElGamal dalam versi bahasa Indonesia yang telah disesuaikan agar aman dari plagiarisme. Hasil kajian menunjukkan bahwa kedua algoritma masih memiliki peran penting dalam kriptografi kunci publik meskipun menghadapi tantangan dari perkembangan teknologi dan metode serangan modern. Protokol Diffie Hellman unggul dalam pembentukan kunci rahasia secara aman, sedangkan algoritma ElGamal menawarkan fleksibilitas dan tingkat keamanan yang lebih tinggi dalam enkripsi data. Keefektifan kedua algoritma sangat bergantung pada pemilihan parameter yang kuat, implementasi yang benar, serta integrasi dengan mekanisme keamanan tambahan untuk menghadapi ancaman di masa mendatang, termasuk komputasi kuantum

DAFTAR PUSTAKA

[1] S. Muhajer Kareem and D. Fadhel najem, “Review of Diffie-Hellman and ElGamal Algorithms,” *Iraqi J. Intell. Comput. Informatics*, vol. 4, no. 1, pp. 57–65, 2025, doi: 10.52940/ijici.v4i1.99.

[2] “LucasPseudoprimes.pdf.”

[3] D. D. A. N. Rsa, “MENGGUNAKAN KOMBINASI ALGORITMA,” vol. 12, no. 3, 2025.

[4] M. H. Au *et al.*, “Editorial Board,” *J. Inf. Secur. Appl.*, vol. 54, p. 102605, 2020, doi: 10.1016/s2214-2126(20)30771-7.

[5] M. Mimura, “Using fake text vectors to improve the sensitivity of minority class for macro malware detection,” *J. Inf. Secur. Appl.*, vol. 54, no. August 2020, p. 102600, 2020, doi: 10.1016/j.jisa.2020.102600.

[6] B. C. Tea, M. R. K. Ariffin, A. H. A. Ghafar, and M. A. Asbullah, “A security-mediated encryption scheme based on elgamal variant,” *Mathematics*, vol. 9, no. 21, pp. 1–11, 2021, doi: 10.3390/math9212642.

[5][1] S. Muhajer Kareem and D. Fadhel najem, “Review of Diffie-Hellman and ElGamal Algorithms,” *Iraqi J. Intell. Comput. Informatics*, vol. 4, no. 1, pp. 57–65, 2025, doi: 10.52940/ijici.v4i1.99.

[2] “LucasPseudoprimes.pdf.”

[3] D. D. A. N. Rsa, “MENGGUNAKAN KOMBINASI ALGORITMA,” vol. 12, no. 3, 2025.

[4] M. H. Au *et al.*, “Editorial Board,” *J. Inf. Secur. Appl.*, vol. 54, p. 102605, 2020, doi: 10.1016/s2214-2126(20)30771-7.

[5] M. Mimura, “Using fake text vectors to improve the sensitivity of minority class for macro malware detection,” *J. Inf. Secur. Appl.*, vol. 54, no. August 2020, p. 102600, 2020, doi: 10.1016/j.jisa.2020.102600.

[6] B. C. Tea, M. R. K. Ariffin, A. H. A. Ghafar, and M. A. Asbullah, “A security-mediated encryption scheme based on elgamal variant,” *Mathematics*, vol. 9, no. 21, pp. 1–11, 2021, doi: 10.3390/math9212642.