JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Perkembangan Teknik Kriptografi Modern: Dari Substitusi Klasik hingga Public-Key Encryption

Diva Nadya Putri[1*], Divia Permata Sari[2], Maulidayana[3], Muksalmina[4], Muhammad Raihan Syafiq Lubis[5]
[1,2,3,4,5] Universitas Malikussaleh, Indonesia
[1]diva.240170232@mhs.unimal.ac.id, [2]divia.240170097@mhs.unimal.ac.id,
[3]maulidayana.240170044@mhs.unimal.ac.id, [4]muksalmina.240170220@mhs.unimal.ac.id,
[5]muhammad.240170107@mhs.unimal.ac.id

ABSTRACT

The rapid development of digital technology has increased the need for secure information exchange, making cryptography a fundamental component of modern information security systems. In the early stages, cryptographic techniques were dominated by classical substitution ciphers, which are simple but vulnerable to various cryptanalysis attacks. This study aims to analyze the development of cryptographic techniques, from classical substitution ciphers to modern public-key encryption schemes. The research method used is a literature review by reviewing books, national journals, and international journals that discuss classical and modern cryptography. The results show that classical cryptographic methods are no longer adequate to meet current security needs because they have a limited key space and are vulnerable to attacks. In contrast, the emergence of modern cryptography, especially public-key encryption such as RSA and Diffie–Hellman, offers stronger security mechanisms, especially in the process of key distribution and secure communication over open networks. Based on these results, it can be concluded that public-key encryption plays a very important role in supporting the security of digital communications and has become the basis for various modern security applications.

Kata Kunci : *Kriptografi, Classical Substitution Chiper, Public-Key Encryption, Keamanan Informasi, Cryptanalysis.*

PENDAHULUAN

Kemajuan teknologi digital yang berlangsung sangat cepat telah mengubah secara signifikan cara manusia menyimpan, memproses, dan bertukar informasi. Berbagai aktivitas komunikasi dan transaksi yang sebelumnya dilakukan secara konvensional kini banyak dilakukan melalui media digital dan jaringan terbuka, seperti internet. Perkembangan ini memberikan peningkatan efisiensi dan kemudahan, namun juga memunculkan tantangan besar dalam aspek keamanan informasi. Tantangan tersebut terutama berkaitan dengan upaya menjaga kerahasiaan, integritas, dan keaslian data, sehingga diperlukan mekanisme keamanan yang mampu melindungi informasi dari akses tidak sah serta ancaman serangan siber.

Dalam konteks tersebut, kriptografi menjadi salah satu komponen utama dalam sistem keamanan informasi modern. Pada awal perkembangannya, teknik kriptografi didominasi oleh penggunaan sandi substitusi klasik yang bekerja dengan mengganti karakter atau simbol tertentu untuk menyamarkan pesan. Teknik ini mudah dipahami dan diimplementasikan, tetapi tingkat keamanannya rendah. Keterbatasan ruang kunci dan kerentanannya terhadap analisis kriptografi menjadikan metode ini tidak lagi efektif. Peningkatan kompleksitas sistem informasi serta kemajuan kemampuan komputasi semakin mempertegas bahwa kriptografi klasik tidak mampu memenuhi kebutuhan keamanan pada era digital saat ini.

Situasi tersebut mendorong lahirnya teknik kriptografi modern yang dirancang untuk menyediakan perlindungan yang lebih kuat. Salah satu perkembangan penting adalah diperkenalkannya kriptografi kunci publik (public-key encryption), seperti algoritma RSA dan Diffie–Hellman. Skema ini memberikan pendekatan yang lebih efisien dalam pengelolaan dan distribusi kunci. Selain itu, enkripsi kunci publik memungkinkan terwujudnya komunikasi yang aman melalui jaringan terbuka tanpa memerlukan pertukaran kunci rahasia secara langsung. Oleh karena itu, kriptografi modern menjadi dasar bagi berbagai penerapan keamanan, antara lain dalam transaksi elektronik, sistem autentikasi, dan perlindungan data digital.

Berdasarkan uraian tersebut, penelitian ini mengkaji perkembangan teknik kriptografi, mulai dari metode substitusi klasik hingga skema enkripsi kunci publik modern. Pembahasan ini diharapkan dapat memberikan pemahaman yang menyeluruh mengenai evolusi kriptografi serta menegaskan peran strategis enkripsi kunci publik dalam menjamin keamanan komunikasi digital pada era teknologi informasi.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

KAJIAN LITERATUR

Konsep Dasar Kriptografi

Kriptografi merupakan ilmu dan teknik yang digunakan untuk mengamankan informasi melalui proses penyandian data sehingga hanya pihak yang berwenang yang dapat mengakses informasi tersebut. Tujuan utama kriptografi meliputi kerahasiaan (confidentiality), integritas (integrity), autentikasi (authentication), dan non-repudiation. Dalam sistem informasi, kriptografi berfungsi sebagai lapisan pengaman yang melindungi data dari ancaman akses tidak sah dan manipulasi informasi. (Hasugian, 2017) menyatakan bahwa kriptografi merupakan komponen fundamental dalam sistem keamanan informasi karena mampu menjamin keamanan data baik pada proses penyimpanan maupun transmisi.

Secara umum, proses kriptografi melibatkan dua tahapan utama, yaitu enkripsi dan dekripsi. Enkripsi merupakan proses mengubah plaintext menjadi ciphertext menggunakan suatu algoritma dan kunci tertentu, sedangkan dekripsi merupakan proses kebalikan untuk mengembalikan ciphertext menjadi plaintext. (Amalya et al., 2023) menjelaskan bahwa kekuatan suatu sistem kriptografi sangat dipengaruhi oleh kompleksitas algoritma dan panjang kunci yang digunakan. Semakin kompleks algoritma dan semakin besar ruang kunci, maka semakin sulit sistem tersebut untuk dipecahkan oleh pihak yang tidak berwenang.

Kriptografi Klasik

Kriptografi klasik merupakan bentuk awal dari teknik pengamanan informasi yang umumnya berbasis pada manipulasi karakter, huruf, atau simbol. Metode yang digunakan dalam kriptografi klasik meliputi teknik substitusi dan transposisi. Contoh algoritma kriptografi klasik yang populer adalah Caesar Cipher, Vigenère Cipher, dan ROT13. Pada metode substitusi, setiap karakter pada plaintext digantikan dengan karakter lain berdasarkan aturan tertentu, sedangkan pada metode transposisi dilakukan pengacakan posisi karakter tanpa mengubah karakter itu sendiri (Permanasari, 2017).

(Kristianto Hondro & Fau, 2018) menjelaskan bahwa algoritma ROT13 merupakan salah satu bentuk sederhana dari Caesar Cipher yang menggunakan pergeseran tetap sebanyak 13 karakter. Meskipun mudah diimplementasikan dan dipahami, algoritma ini memiliki tingkat keamanan yang sangat rendah. Kriptografi klasik umumnya memiliki ruang kunci yang terbatas sehingga rentan terhadap serangan kriptanalisis, khususnya analisis frekuensi. Hal ini menyebabkan kriptografi klasik tidak lagi efektif untuk melindungi data pada sistem informasi modern.

Kelemahan Kriptografi Klasik dan Kebutuhan Kriptografi Modern

Seiring dengan berkembangnya teknologi komputer dan meningkatnya kemampuan pemrosesan data, berbagai kelemahan kriptografi klasik semakin mudah dieksploitasi. (Amin et al., 2016) menyatakan bahwa kriptografi klasik yang berbasis karakter tidak dirancang untuk menghadapi serangan komputasi modern. Serangan brute force dan analisis statistik dapat dilakukan dengan cepat menggunakan perangkat lunak dan perangkat keras yang tersedia saat ini (Surbakti et al., 2025).

Kondisi tersebut mendorong lahirnya kriptografi modern yang menggunakan pendekatan matematika dan komputasi yang lebih kompleks. Kriptografi modern beroperasi pada data biner dan memanfaatkan konsep matematika seperti teori bilangan dan aljabar modular. Menurut (Amalya et al., 2023) kriptografi modern menawarkan tingkat keamanan yang lebih tinggi karena memiliki ruang kunci yang besar dan dirancang untuk tahan terhadap berbagai jenis serangan kriptanalisis.

Kriptografi Kunci Publik (Public-Key Encryption)

Kriptografi kunci publik atau public-key encryption merupakan salah satu tonggak utama dalam perkembangan kriptografi modern. Berbeda dengan kriptografi kunci simetris yang menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, kriptografi kunci publik menggunakan dua kunci yang berbeda, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk proses enkripsi dan dapat diketahui secara umum, sedangkan kunci privat bersifat rahasia dan digunakan untuk proses dekripsi. Konsep ini secara signifikan mengatasi permasalahan distribusi kunci yang menjadi kelemahan utama pada kriptografi klasik dan kriptografi simetris (Hasugian, 2017).

Penelitian yang dilakukan dalam jurnal Keamanan Kriptosistem Modern Berdasarkan Algoritma Kriptografi Kunci Publik menunjukkan bahwa algoritma kriptografi kunci publik seperti RSA, ElGamal, dan Elliptic Curve Cryptography (ECC) memiliki tingkat keamanan yang tinggi karena didasarkan pada permasalahan matematika yang sulit dipecahkan, seperti faktorisasi bilangan prima dan logaritma diskrit. Penelitian tersebut juga menegaskan bahwa kriptosistem berbasis kunci publik masih menjadi fondasi utama keamanan data digital, meskipun perkembangan komputasi kuantum mulai menjadi tantangan yang perlu diperhatikan di masa depan (Pongsitammu et al., 2023).

Selain aspek keamanan konseptual, tingkat kompleksitas dan performa algoritma kriptografi juga menjadi faktor penting dalam penerapannya. Studi komparatif yang membandingkan algoritma RSA, DES, dan AES menunjukkan bahwa RSA unggul sebagai algoritma kriptografi kunci publik dalam hal mekanisme pertukaran kunci dan keamanan komunikasi, sementara DES dinilai tidak lagi aman karena panjang kunci yang terbatas, dan AES menawarkan tingkat keamanan yang tinggi sebagai algoritma kriptografi simetris modern. Hasil penelitian ini memperkuat posisi RSA

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

sebagai salah satu algoritma utama dalam sistem keamanan berbasis public-key encryption (Zulfikar, 2023).

Penelitian Terkait dan Sintesis Kajian

Berbagai penelitian sebelumnya menunjukkan adanya pergeseran paradigma yang jelas dalam pengembangan teknik kriptografi, dari kriptografi klasik menuju kriptografi modern berbasis kunci publik. Penelitian mengenai kriptografi klasik, seperti yang dibahas oleh (Kristianto Hondro & Fau, 2018) serta (Amin et al., 2016), menegaskan bahwa algoritma substitusi dan teknik berbasis karakter, meskipun mudah dipahami dan diimplementasikan, memiliki tingkat keamanan yang rendah. Kelemahan utama kriptografi klasik terletak pada ruang kunci yang terbatas dan kerentanannya terhadap serangan kriptanalisis, khususnya analisis frekuensi, sehingga tidak lagi memadai untuk melindungi data dalam sistem informasi modern (Aminudin et al., 2024).

Penelitian lain yang membandingkan kriptografi klasik dengan algoritma yang lebih modern menunjukkan bahwa algoritma klasik tertinggal jauh dari sisi keamanan maupun efisiensi. Studi komparatif terhadap algoritma Caesar Cipher dan DES, serta perbandingan antara Vigenere Cipher dan algoritma kriptografi modern, memperlihatkan bahwa peningkatan kompleksitas algoritma dan panjang kunci berbanding lurus dengan peningkatan tingkat keamanan sistem. Temuan-temuan empiris ini memperkuat argumen bahwa kriptografi klasik lebih tepat digunakan sebagai media pembelajaran konsep dasar kriptografi daripada sebagai solusi keamanan pada lingkungan digital saat ini (Amin et al., 2016).

Seiring dengan meningkatnya kebutuhan keamanan informasi, berbagai penelitian mulai berfokus pada kriptografi modern, baik kriptografi kunci simetris maupun kunci publik. Penelitian oleh (Zulfikar, 2023) menunjukkan bahwa algoritma RSA memiliki peran penting dalam sistem keamanan modern sebagai algoritma kunci publik, terutama dalam mekanisme pertukaran kunci dan pengamanan komunikasi. Sementara itu, algoritma DES dinilai tidak lagi aman karena keterbatasan panjang kunci, sedangkan AES masih dianggap aman dan efisien sebagai algoritma kriptografi kunci simetris modern (Rosdiana & Sutriyatna, n.d.).

Lebih lanjut, penelitian mengenai keamanan kriptosistem modern berbasis kunci publik menegaskan bahwa algoritma seperti RSA, ElGamal, dan Elliptic Curve Cryptography (ECC) menjadi fondasi utama dalam pengamanan data digital. (Pongsitammu et al., 2023) menyatakan bahwa kekuatan kriptografi kunci publik terletak pada dasar matematisnya yang kompleks, sehingga sulit dipecahkan menggunakan metode kriptanalisis konvensional. Namun demikian, penelitian tersebut juga menyoroti tantangan baru yang muncul seiring perkembangan komputasi kuantum, yang berpotensi memengaruhi keamanan algoritma kunci publik di masa depan.

Berdasarkan sintesis kajian teori dan hasil penelitian empiris tersebut, dapat disimpulkan bahwa perkembangan teknik kriptografi merupakan respons terhadap meningkatnya kompleksitas ancaman keamanan informasi. Kriptografi klasik memiliki peran historis dan edukatif, namun tidak lagi relevan sebagai solusi keamanan utama. Kriptografi modern, khususnya public-key encryption, hadir sebagai jawaban atas keterbatasan kriptografi klasik dengan menawarkan mekanisme keamanan yang lebih kuat, fleksibel, dan sesuai untuk komunikasi pada jaringan terbuka. Sintesis ini menjadi dasar konseptual bagi penelitian ini dalam mengkaji perkembangan teknik kriptografi dari substitusi klasik hingga public-key encryption.

METODE PENELITIAN

Penelitian ini termasuk dalam jenis penelitian kualitatif dengan pendekatan kajian literatur (literature review). Pendekatan tersebut dipilih karena penelitian bertujuan untuk menelaah, menganalisis, dan mengintegrasikan perkembangan teknik kriptografi, mulai dari metode klasik hingga kriptografi modern berbasis enkripsi kunci publik. Melalui kajian literatur, peneliti dapat memperoleh pemahaman yang mendalam mengenai landasan teoretis, evolusi historis, serta hasil-hasil penelitian sebelumnya yang relevan dengan bidang kriptografi.

Sumber Data Penelitian

Data yang digunakan dalam penelitian ini merupakan data sekunder yang bersumber dari artikel ilmiah pada jurnal nasional dan internasional yang berkaitan dengan topik kriptografi. Literatur yang dianalisis mencakup pembahasan mengenai kriptografi klasik, kriptografi modern, dan kriptografi kunci publik. Sumber-sumber tersebut diperoleh melalui portal jurnal ilmiah terbuka (open access), seperti jurnal berbasis Open Journal Systems (OJS) di perguruan tinggi, jurnal nasional terakreditasi, serta repositori ilmiah internasional.

Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui studi pustaka dengan beberapa tahapan sistematis. Tahap pertama adalah penentuan kata kunci pencarian, antara lain kriptografi, kriptografi klasik, substitution cipher, kriptografi modern, dan public-key encryption. Tahap berikutnya adalah penelusuran artikel ilmiah yang relevan melalui portal jurnal daring. Selanjutnya, dilakukan seleksi artikel berdasarkan kesesuaian judul, abstrak, dan ruang lingkup penelitian. Artikel yang memenuhi kriteria kemudian dikumpulkan untuk dianalisis lebih lanjut. Literatur yang dipilih mencakup penelitian yang membahas aspek teoretis maupun empiris terkait keamanan serta implementasi kriptografi.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Teknik Analisis Data

Analisis data dilakukan menggunakan pendekatan deskriptif dan komparatif. Analisis deskriptif digunakan untuk mengkaji konsep, definisi, dan karakteristik kriptografi klasik serta kriptografi modern berdasarkan sumber literatur yang dikumpulkan. Selanjutnya, analisis komparatif diterapkan untuk membandingkan keunggulan dan keterbatasan kriptografi klasik dengan kriptografi modern, khususnya enkripsi kunci publik. Hasil dari kedua analisis tersebut kemudian disintesis guna memperoleh pemahaman yang utuh mengenai perkembangan teknik kriptografi dan relevansinya terhadap kebutuhan keamanan informasi saat ini.

Alur Penelitian

Alur penelitian diawali dengan identifikasi permasalahan dan penetapan fokus kajian, yaitu perkembangan teknik kriptografi dari metode substitusi klasik hingga skema enkripsi kunci publik. Tahap selanjutnya meliputi pengumpulan serta seleksi literatur yang relevan. Literatur terpilih kemudian dianalisis dan disintesis untuk memperoleh temuan yang komprehensif. Tahap akhir penelitian adalah penarikan kesimpulan berdasarkan hasil kajian literatur yang telah dianalisis secara sistematis. Metodologi ini diharapkan mampu menghasilkan pembahasan yang mendalam dan relevan dalam menjelaskan evolusi teknik kriptografi pada sistem keamanan informasi modern.

HASIL DAN PEMBAHASAN

Hasil

Hasil kajian literatur menunjukkan bahwa teknik kriptografi mengalami perkembangan yang signifikan seiring dengan meningkatnya kompleksitas ancaman keamanan informasi dan kemajuan teknologi komputasi. Literatur yang dianalisis secara konsisten menyebutkan bahwa kriptografi klasik merupakan fondasi awal dalam pengamanan informasi, namun memiliki keterbatasan mendasar. Teknik substitusi dan transposisi, seperti Caesar Cipher, Vigenère Cipher, dan ROT13, hanya efektif pada konteks komunikasi sederhana dan tidak dirancang untuk menghadapi serangan berbasis komputasi modern.

Keterbatasan utama kriptografi klasik terletak pada ruang kunci yang sempit dan pola bahasa yang masih dapat dianalisis. Kondisi ini menjadikan algoritma klasik rentan terhadap serangan analisis frekuensi dan brute force, terutama dengan dukungan perangkat lunak dan perangkat keras yang semakin canggih. Oleh karena itu, kriptografi klasik dinilai tidak lagi memadai untuk melindungi data pada sistem informasi modern (Kurnia Dewi, 2024).

Sebaliknya, kriptografi modern dikembangkan dengan memanfaatkan pendekatan matematis dan komputasi yang lebih kompleks. Kriptografi modern bekerja pada data biner dan dirancang untuk memiliki ruang kunci yang besar, sehingga lebih tahan terhadap berbagai bentuk kriptanalisis. Salah satu perkembangan paling penting dalam kriptografi modern adalah munculnya kriptografi kunci publik (public-key encryption), yang menawarkan solusi terhadap permasalahan distribusi kunci pada kriptografi klasik dan kriptografi kunci simetris.

Untuk memperjelas perbedaan mendasar antara kriptografi klasik dan kriptografi modern, Tabel 1 menyajikan perbandingan karakteristik utama kedua pendekatan tersebut berdasarkan hasil sintesis kajian literatur.

Table 1. Perbandingan Karakteristik Kriptografi Klasik dan Kriptografi Modern

Aspek Perbandingan	Kriptografi Klasik	Kriptografi Modern
Dasar Teknik	Manipulasi karakter dan simbol	Operasi matematika dan komputasi kompleks
Contoh Algoritma	Caesar Cipher, Vigenère Cipher, ROT13	RSA, Diffie–Hellman, ElGamal, ECC
Ruang Kunci	Terbatas	Sangat Besar
Ketahanan Terhadap Serangan	Rentan terhadap analisis frekuensi dan brute force	Tahan terhadap kriptanalisis konvensional
Distribusi Kunci	Tidak aman dan tidak efisien	Aman melalui mekanisme kunci publik
Relevansi pada Era Digital	Bersifat historis dan edukatif	Digunakan secara luas pada sistem keamanan modern

Berdasarkan Tabel 1, dapat disimpulkan bahwa kriptografi modern memiliki keunggulan signifikan dibandingkan kriptografi klasik, terutama dari aspek keamanan, distribusi kunci, dan relevansinya terhadap kebutuhan sistem informasi saat ini.

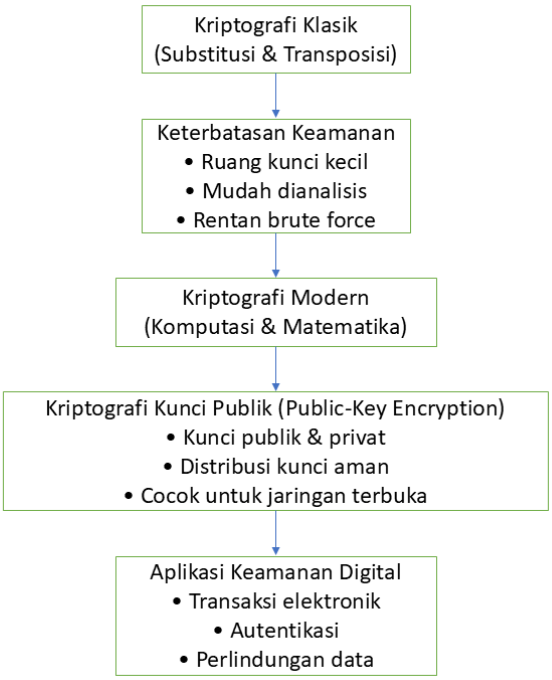
Pembahasan

Hasil kajian literatur yang diperoleh selaras dengan tujuan penelitian, yaitu menganalisis perkembangan teknik kriptografi dari metode substitusi klasik hingga skema enkripsi kunci publik. Kriptografi klasik memiliki peran penting secara historis dan konseptual dalam perkembangan ilmu kriptografi, namun tidak lagi relevan sebagai mekanisme pengamanan utama pada lingkungan digital modern. Temuan ini sejalan dengan berbagai penelitian terdahulu yang

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

menegaskan bahwa kriptografi klasik lebih tepat digunakan sebagai media pembelajaran konsep dasar kriptografi.

Perkembangan kriptografi modern dapat dipahami sebagai respons terhadap meningkatnya kebutuhan keamanan informasi dan kemampuan komputasi yang semakin maju. Kriptografi kunci publik, seperti RSA dan Diffie–Hellman, menjadi solusi utama karena mampu mengatasi permasalahan distribusi kunci serta memungkinkan komunikasi yang aman melalui jaringan terbuka. Dalam praktiknya, kriptografi kunci publik sering dikombinasikan dengan kriptografi kunci simetris modern, seperti AES, untuk membentuk sistem keamanan hibrida yang efisien dan kuat. Untuk memberikan gambaran yang lebih jelas mengenai alur perkembangan teknik kriptografi, Gambar 1 menyajikan bagan konsep evolusi kriptografi dari metode klasik hingga penerapannya pada sistem keamanan digital modern.



Gambar 1. Bagan Konsep Perkembangan Teknik Kriptografi

Gambar 1 menunjukkan bahwa kriptografi modern, khususnya public-key encryption, hadir sebagai solusi atas keterbatasan kriptografi klasik. Evolusi ini mencerminkan upaya berkelanjutan dalam meningkatkan keamanan informasi agar sesuai dengan karakteristik jaringan terbuka dan kebutuhan komunikasi digital saat ini.

KESIMPULAN

Berdasarkan kajian literatur dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa perkembangan teknik kriptografi muncul sebagai respons atas semakin meningkatnya kebutuhan keamanan informasi di era digital. Pada tahap awal, kriptografi klasik yang menggunakan teknik substitusi dan transposisi memiliki peran penting dalam sejarah perkembangan kriptografi. Metode ini menjadi fondasi awal dalam upaya melindungi informasi. Namun, keterbatasan ruang kunci serta tingginya kerentanan terhadap serangan kriptanalisis menyebabkan kriptografi klasik tidak lagi mampu memenuhi tuntutan keamanan pada sistem informasi modern.

Hasil kajian juga menunjukkan bahwa kriptografi modern menawarkan tingkat keamanan yang jauh lebih baik melalui pemanfaatan konsep matematika dan komputasi yang lebih kompleks. Kriptografi kunci publik (public-key encryption), seperti RSA dan Diffie–Hellman, hadir sebagai solusi utama dalam mengatasi permasalahan distribusi kunci serta memungkinkan terjadinya komunikasi yang aman melalui jaringan terbuka. Oleh karena itu, enkripsi kunci publik memiliki peran yang sangat strategis dan menjadi dasar bagi berbagai aplikasi keamanan digital, seperti transaksi elektronik, sistem autentikasi, dan perlindungan data.

Penelitian ini memberikan kontribusi berupa pemahaman yang lebih menyeluruh mengenai evolusi teknik kriptografi serta relevansinya terhadap kebutuhan keamanan informasi saat ini. Selain itu, hasil kajian ini dapat dimanfaatkan sebagai referensi akademik bagi mahasiswa maupun peneliti untuk memahami perbedaan mendasar antara kriptografi klasik dan kriptografi modern, khususnya dalam konteks penerapannya pada sistem keamanan informasi. Meskipun demikian, penelitian ini masih memiliki keterbatasan karena hanya berfokus pada kajian literatur tanpa disertai dengan pengujian atau implementasi algoritma kriptografi secara langsung. Selain itu, pembahasan yang dilakukan masih terbatas pada algoritma kriptografi kunci publik yang umum digunakan, sehingga belum mencakup

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

perkembangan terbaru secara lebih mendalam, seperti kriptografi pasca-kuantum.

Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan untuk mengembangkan kajian ini melalui pendekatan eksperimental atau studi implementasi agar kinerja dan tingkat keamanan algoritma kriptografi dapat dianalisis secara empiris. Selain itu, penelitian di masa mendatang juga dapat difokuskan pada pengaruh perkembangan komputasi kuantum terhadap keamanan kriptografi kunci publik serta eksplorasi algoritma kriptografi baru yang lebih adaptif terhadap tantangan teknologi di masa depan.

REFERENSI

Amalya, N., Sopiana Silalahi, S. M., Nasution, D. F., Sari, M., & Gunawaan, I. (2023). *JURNAL MEDIA INFORMATIKA [JUMIN] Kriptografi dan Penerapannya Dalam Sistem Keamanan Data*.

Amin, M. M., Komputer, J. T., Negeri, P., & Palembang, S. (2016). IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS. *Jurnal Pseudocode*, *2*.

Aminudin, A., Hakim, L., Nuryasin, I., & Santiyas, H. R. (2024). Kriptosistem Hybrid Algoritme RSA dan El-Gamal Menggunakan Socket TCP pada Instant Messaging. *JRST (Jurnal Riset Sains Dan Teknologi)*, *8*(1), 1. https://doi.org/10.30595/jrst.v8i1.17124

Hasugian. (2017). PERANAN KRIPTOGRAFI SEBAGAI KEAMANAN SISTEM. *PERANAN KRIPTOGRAFI SEBAGAI KEAMANAN SISTEM INFORMASI PADA USAHA KECIL DAN MENENGAH*.

Kristianto Hondro, R., & Fau, A. (2018). PERANCANGAN APLIKASI PENYANDIAN TEKS DENGAN ALGORITMA ROT13 DAN TRIANGLE CHAIN CIPHER (TCC). *Jurnal Mahajana Informasi*, *3*(2).

Kurnia Dewi, S. (2024). *Perbandingan Cryptography Klasik Vigenere Cipher Dengan Cryptography Modern RC4 Dalam Tingkat Keamanan Jaringan Komputer*. 130–137. https://doi.org/10.46961/jommit.v8i2

Permanasari, Y. (2017). *Kriptografi Klasik Monoalphabetic*. *16*(1). http://ejournal.unisba.ac.idDiterima:7/01/2017

Pongsitammu, V., Renta Yani Simatupang, A., Annura, D., Sari Dachi, Y., & Rollando Harries, D. (2023). *KEAMANAN KRIPTOSISTEM MODERN BERDASARKAN ALGORITMA KRIPTOGRAFI KUNCI PUBLIK* (Vol. 2, Issue 1). https://journal.iteba.ac.id/index.php/jurnalsiteba/indexSITEBA

Rosdiana, M., & Sutriyatna, E. (n.d.). *Penerapan Kriptografi Dalam Keamanan Data Pada Layanan Cloud Computing*.

Surbakti, N., Kartika, D., Lestari, A. D., Puspita, M., Pandiangan, P. P. S., Singarimbun, R., & Suryani, W. (2025). Implementasi Algoritma Kriptografi RSA dalam Proses Enkripsi dan Dekripsi untuk Mengamankan Pesan Singkat pada Aplikasi Chatting Berbasis Web. *Jurnal Ilmiah Teknik Informatika Dan Komunikasi*, *5*(3), 647–659. https://doi.org/10.55606/juitik.v5i3.1711

Zulfikar. (2023). 4.+ANALISIS+PERBANDINGAN+TINGKAT+KOMPLEKSITAS+WAKTU+ENKRIPSI+DAN+TINGKAT+KEAMANAN+ENKRIPSI+PADA+ALGORIT. *ANALISIS PERBANDINGAN TINGKAT KOMPLEKSITAS WAKTU ENKRIPSI DAN TINGKAT KEAMANAN ENKRIPSI PADA ALGORITMA KRIPTOGRAFI RSA, DES, AES*.