Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 2, Issue 3, 2024 pp. 421-426 http://urj.uin-malang.ac.id/index.php/mij/index

Implementasi matematika di era teknologi: Peran kriptografi dalam mengamankan pesan

Ita Nuryanawati
Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail: 210601110037@student.uin-malang.ac.id

Kata Kunci:
pesan; kriptografi; matematika; rahasia; keamanan

Keywords:
messagin; cryptography; mathematics; secrets; security

A B S T R A K

Pesan merupakan aspek umum dalam interaksi kita, dan berbagai saluran digunakan untuk menyampaikan pesan. Bagi pesan yang membutuhkan kerahasiaan khusus, diperlukan langkah-langkah keamanan khusus pula. Kriptografi, yang didasarkan pada prinsip-prinsip matematika, merupaka cara yang efektif untuk mengatasi tantangan ini. Fokus dari penulisan ini adalah untuk memahami konsep serta teknik kriptografi yang mengandalkan aspek matematika dalam melindungi pesan. Keberhasilan sistem keamanan ini sangat terkait dengan kompleksitas matematika yang memerlukan waktu yang lama bagi pihak yang tidak berwenang untuk membongkarnya. Oleh karena itu, penerapan matematika dalam kriptografi memungkinkan pesan untuk diamankan secara efisien di tengah lingkungan digital yang penuh dengan potensi ancaman. Dengan demikian, pesan-pesan rahasia dan sensitif dapat dikomunikasikan tanpa risiko terhadap kebocoran atau manipulasi yang merugikan.

A B S T R A C T

Messages are a common aspect of our interactions, and various channels are used to convey messages. For messages that require special confidentiality, special security measures are also required. Cryptography, which is based on mathematical principles, is an effective way to overcome this challenge. The focus of this paper is to understand cryptographic concepts and techniques that rely on mathematical aspects in protecting messages. The success of this security system is closely related to the mathematical complexity that takes a long time for unauthorized parties to dismantle it. Therefore, the application of mathematics in cryptography allows messages to be efficiently secured in a digital environment full of potential threats. Thus, confidential and sensitive messages can be communicated without risk of leakage or harmful manipulation.

Pendahuluan

Pesan adalah sebuah pemberitahuan, kata, perintah, informasi, atau komunikasi dalam bentuk lisan maupun tulisan yang dibuat oleh pengirim kepada penerima pesan (Agustina et al., 2023). Agar pesan dapat sampai ke tujuannya dengan jelas dan efektif, media atau perantara dalam komunikasi memainkan peran penting. Media ini dapat berupa teknologi, saluran komunikasi, atau bahkan bahasa yang digunakan dalam pesan itu sendiri. Ada beberapa pesan yang bersifat rahasia, sehingga hanya pihak

tertentu yang boleh mengetahui pesan tersebut. Oleh karena itu keamanan pesan sangat penting untuk mencegah terjadinya kebocoran informasi.

Terdapat ilmu untuk menjaga keamanan suatu pesan, yaitu kriptografi. Kriptografi (*crytography*) berasal dari bahasa Yunani *"cryptos"* artinya *"secret"* (rahasia) sedangkan *"graphein"* artinya *"writing"* (tulisan). Secara umum kriptografi dapat diartikan sebagai suatu bidang ilmu yang memiliki kesenian dalam menjaga kerahasiaan dari suatu data atau informasi (Aufia et al., 2021). Mengandalkan prinsip-prinsip matematika yang rumit, kriptografi memfasilitasi proses enkripsi pesan sebelum pengiriman, memastikan bahwa hanya penerima yang memiliki akses ke kunci yang sesuai yang dapat melakukan dekripsi dan mengakses isi pesan tersebut. Dengan ini, kerahasiaan konten pesan tetap terjaga, bahkan jika pesan tersebut jatuh ke tangan yang tidak berwenang. Dalam esensinya, kriptografi menjadi metode utama yang mengandalkan konsep-konsep matematika untuk menjamin keamanan pesan.

Terdapat dua istilah dalam kriptografi yaitu plainteks (pesan asli) dan cipherteks (pesan yang telah diacak). Adapun proses yang terdapat dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi yaitu mengubah pesan asli menjadi pesan yang susah dimengerti sedangkan dekripsi merupakan proses mengubah pesan yang tidak dimengerti menjadi pesan bermakna atau pesan asli (Aufia et al., 2021).

Pembahasan

Dalam dunia yang semakin terhubung dan rentan terhadap ancaman ciber, kriptografi telah menjadi pondasi penting dalam menjaga kerahasiaan dan keamanan komunikasi. Melalui penerapan konsep matematika yang canggih, kriptografi memungkinkan pesan untuk melintasi saluran komunikasi dengan jaminan bahwa hanya penerima yang dimaksud yang dapat mengakses informasi yang tersimpan di dalamnya. Di bawah ini adalah beberapa konsep dan teknik kriptografi yang menggunakan matematika untuk mengamankan pesan:

Enkripsi Simetris

Enkripsi simteris atau algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan untuk proses dekripsi (Basri, 2016). Dalam konteks ini, kunci yang sama digunakan untuk menyandikan pesan asli menjadi *cipherteks* serta untuk mengembalikan *cipherteks* ke dalam bentuk pesan yang dapat dimengerti. Dalam ranah algoritma kriptografi simetris terdapat dua kategori utama, yaitu algoritma aliran *(Stream Ciphers)* dan algoritma blok *(Block Ciphers)*. Algoritma aliran melibatkan proses enkripsi satu bit pada satu waktu, sehingga cocok untuk mengamankan aliran data kontinu seperti komunikasi audio atau video secara *real-time.* Sementara itu, algoritma blok bekerja dengan blok pesan yang lebih besar, membagi pesan menjadi blok-blok yang kemudian dienkripsi secara terpisah. Ini lebih cocok untuk mengamankan data dalam format file atau pesan yang lebih besar.

Algoritma RC-5 adalah metode enkripsi yang menggunakan pendekatan simetrik dan melibatkan pemrosesan dalam bentuk blok chipper. Teknik RC-5 menjalankan langkah-langkah dasar dalam proses enkripsi sebagai berikut:

1. Data yang akan dienkripsi dipecah menjadi dua bagian terpisah, yaitu bagian kiri dan bagian kanan. Kemudian, keduanya dijumlahkan dengan kata kunci yang telah di-expand sebelumnya. Operasi penjumlahan ini ditandai dengan tanda "+", dan hasilnya disimpan dalam dua register, yakni register A dan register B.
2. Langkah selanjutnya melibatkan operasi EX-OR, yang dinyatakan dengan simbol "R".
3. Proses berikutnya melibatkan rotasi ke kiri (shift left) sepanjang y pada kata x. Simbol x <<< y menunjukkan operasi rotasi ini. Nilai y diinterpretasikan modulo w, di mana w adalah jumlah kata dalam blok. Jumlah putaran yang dilakukan ditentukan oleh lg[w].
4. Tahap akhir melibatkan penggabungan hasil operasi untuk menghasilkan data yang telah dienkripsi.

Sementara itu, langkah-langkah dalam proses dekripsi berdasarkan konsep dasar adalah sebagai berikut:

1. Data yang telah mengalami enkripsi dipecah menjadi dua bagian dan disimpan dalam dua register, yaitu register A dan register B.
2. Selanjutnya, dilakukan operasi rotasi ke kanan sejauh r satuan.
3. Langkah berikutnya melibatkan operasi EX-OR yang ditandai dengan simbol "R".
4. Pada tahap akhir, dilakukan pengurangan terhadap setiap register dengan menggunakan kata kunci (key word) yang ditandai dengan tanda "-", untuk mendapatkan pesan asli (plaintext).

Enkripsi Asimetris

Kunci asimetris menjadi landasan revolusioner dalam dunia kriptografi, membawa solusi yang cerdas untuk tantangan distribusi kunci yang telah menghambat keamanan data selama bertahun-tahun. Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi (Basri, 2016). Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci private untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.

Kunci asimetris telah memecahkan salah satu tantangan utama yang dihadapi oleh enkripsi simetris, yaitu bagaimana mendistribusikan kunci dengan aman. Melalui penggunaan kunci publik dan kunci privat, konsep ini mengizinkan kunci publik untuk menjadi akses terbuka bagi semua pihak yang ingin berkomunikasi secara aman. Kunci publik ini dapat digunakan oleh siapa pun untuk mengamankan pesan sebelum mengirimkannya. Hal ini menghindarkan masalah distribusi kunci yang rumit yang menjadi kelemahan enkripsi simetris. Namun, kendati memiliki keuntungan besar dalam hal distribusi kunci, teknik enkripsi asimetris cenderung lebih lambat daripada metode enkripsi simetris. Oleh karena itu, praktik umumnya adalah dengan tidak langsung mengenkripsi seluruh pesan menggunakan kunci asimetris yang lebih lambat,

melainkan hanya menggunakan kunci asimetris untuk mengamankan kunci simetris. Kunci simetris ini kemudian digunakan untuk mengenkripsi pesan itu sendiri dengan kecepatan yang lebih tinggi. Dalam proses ini, pesan yang ingin dikirim tidak dienkripsi secara langsung menggunakan kunci asimetris yang lambat, melainkan dengan kunci simetris yang lebih cepat, yang sebelumnya telah diamankan menggunakan kunci asimetris. Dengan demikian, teknik enkripsi asimetris memberikan solusi cerdas yang mengatasi tantangan distribusi kunci dalam enkripsi simetris, sambil mengatasi keterbatasan kecepatan melalui penggunaan kombinasi kunci simetris dan asimetris dalam proses enkripsi dan dekripsi.

Tanda Tangan Digital

Tanda digital adalah suatu mekanisme otentikasi yang mengijinkan pemilik pesan membubuhkan sebuah sandi pada pesannya yang bertindak sebagai tanda tangan. Tanda tangan digital di sini bukanlah tanda tangan yang discan, melainkan suatu bilangan yang diolah secara matematis sedemikian sehingga menghasilkan kesimpulan bahwa suatu dokumen masih asli atau bukan (Naji Maruf Ilyas, 2018). Terdapat tiga proses dalam tanda tangan digital, yaitu proses pembuatan kunci, proses menandatangani dokumen digital dan proses verivikasi tanda tangan digital. Proses pembuatan kunci akan menghasilkan kunci publik dan kunci rahasia. Kunci rahasia digunakan untuk menandatangani dokumen dikital, sedangkan kunci publik digunakan untuk memverifikasi tanda tangan digital.

Tanda tangan digital memegang peranan sentral dalam berbagai konteks, melibatkan bisnis, transaksi online, serta pengiriman dan penerimaan dokumen digital dengan tingkat keamanan yang tinggi. Kemampuannya untuk memastikan keaslian, integritas, dan otentikasi dari dokumen digital menjadikannya sebuah alat yang tak tergantikan di era digital ini. Tanda tangan digital tidak hanya menjamin identitas penandatangan, tetapi juga memastikan bahwa konten dokumen tidak mengalami perubahan yang tidak sah selama proses perjalanan dan tiba di tangan penerima dengan keadaan yang sama seperti saat ditandatangani. Namun, seperti aspek-aspek keamanan dalam bidang kriptografi lainnya, integritas tanda tangan digital sangat bergantung pada perlindungan yang kuat terhadap kunci rahasia yang digunakan dalam proses tanda tangan. Akses yang tidak sah atau penyalahgunaan terhadap kunci rahasia dapat mengancam integritas dan keandalan tanda tangan digital, mengurangi kepercayaan pada mekanisme ini. Oleh karena itu, selain memahami dan menerapkan dengan benar mekanisme tanda tangan digital, perlindungan yang tepat terhadap kunci rahasia juga harus diutamakan untuk memastikan tingkat keamanan yang optimal dalam penggunaannya.

Enkripsi Homomorfik

Enkripsi digunakan untuk melindungi semua data yang disimpan pada cloud. Data akan didekripsi jika pengguna akan melakukan pemrosesan di dalam cloud agar data tidak rentan dari hacker. Pada saat pengguna mengakses atau mengolah data di penyimpanan berbasis cloud, hacker akan lebih mudah meretas data tersebut, maka dari itu Enkripsi Homomorfik dikembangkan untuk menghindari peretasan data (Deviani et al., 2022)

Teknologi enkripsi homomorfik bisa diklasifikasikan ke dalam tiga kategori berikut:

1. Teknik pertama, yang dirintis oleh Gentry, menggunakan dasar lattice ideal dan mencakup konstruksi enkripsi homomorfik yang agak terbatas (SomeWhat Homomorphic Encryption - SWHE). Dalam metode ini, operasi dilakukan pada kumpulan bilangan terbatas, termasuk penjumlahan dan perkalian.
2. Berdasarkan prinsip yang sama dari Gentry, skema enkripsi homomorfik yang berfokus pada bilangan bulat dikembangkan. Skema ini tidak mengandalkan struktur lattice ideal dari cincin polinomial. Operasi dalam skema ini hanya menggunakan bilangan bulat, dan skema ini dikenal sebagai Partially Homomorphic Encryption (PHE). Di dalam tipe enkripsi ini, hanya satu operasi yang bisa dijalankan pada data terenkripsi, baik itu penambahan atau perkalian. Kriptosistem seperti Pillar hanya melibatkan operasi penambahan, sementara RSA menggunakan operasi perkalian pada data.
3. Metode terakhir adalah sistem enkripsi homomorfik sepenuhnya (Fully Homomorphic Encryption - FHE), yang berasal dari konsep Learning with Errors (LWE) atau Learning with Errors over Ring (R-LWE). Sistem ini dibangun di atas toleransi terhadap kesalahan dalam pembelajaran dan menghasilkan skema enkripsi yang benar-benar homomorfik dengan memanfaatkan aspek non-linear. Salah satu contoh skema enkripsi semacam ini adalah skema Brakerski-Gentry-Vaikuntanathan (BGV).Keuntungan utama dari enkripsi homomorfik adalah kemampuannya mengurangi risiko potensial terhadap keamanan data saat proses pemrosesan dilakukan dalam lingkungan cloud. Dalam hal ini, pengguna memiliki kesempatan untuk memanfaatkan kapabilitas cloud untuk mengolah data tanpa perlu mengorbankan keamanan dengan cara mendekripsi data terlebih dahulu. Ini memiliki potensi untuk mengubah paradigma dalam pengolahan data di lingkungan cloud, dimana prioritas utama diberikan pada menjaga privasi dan keamanan, sementara tetap mempertahankan fungsionalitas yang diperlukan.

Meskipun demikian, penting untuk diingat bahwa enkripsi homomorfik masih berada dalam tahap pengembangan, dan ada sejumlah tantangan teknis yang harus dihadapi. Kinerja dan kompleksitas komputasi pada data yang telah terenkripsi, serta perlunya menemukan keseimbangan antara tingkat keamanan dan performa yang optimal, merupakan beberapa aspek yang perlu diberikan perhatian saat menerapkan teknologi ini. Dalam konteks perkembangan terus menerus dalam bidang keamanan siber, enkripsi homomorfik berpotensi menjadi alat yang sangat efektif dalam menjaga keamanan dan privasi data di dalam lingkungan cloud yang semakin kompleks.

Kesimpulan dan Saran

Pembahasan di atas membahas berbagai konsep dan teknik kriptografi yang menggunakan matematika untuk mengamankan pesan dalam dunia yang semakin terhubung dan rentan terhadap ancaman siber. Bebrapa teknik yang dibahas meliputi:

1. Enkripsi simetris, yaitu menggunakan kunci yang sama untuk proses enkripsi dan deskripsi. Terdapat algoritma aliran dan algoritma blok untuk mengamankan aliran data kontinu dan data dalam format file atau pesan yang lebih besar.
2. Enkripsi asimetris, menggunakan pasangan kunci publik dan kunci privat. Kunci publik digunakan untuk mengenkripsi pesan, sementara kunci privat digunakan untuk mendekripsi pesan. Teknik ini mengatasi masalah distribusi kunci yang aman.
3. Tanda tangan digital: mekanisme otentikasi yang memungkinkan pembubuhan tanda tangan pada pesan. Tanda tangan digital memastikan keaslian, integritas, dan otentikasi dokumen digital.
4. Enkripsi homomorfik, yaitu teknologi yang mengizinkan pemrosesan data yang terenkripsi tanpa perlu mendekripsi terlebih dahulu. Ini memungkinkan pengolahan data di lingkungan cloud dengan menjaga privasi dan keamanan.

Untuk menjaga keamanan dan privasi dalam dunia yang semakin terhubung dan rentan terhadap ancaman siber, ada beberapa langkah yang dapat diambil. Pertama, perlu terus mengembangkan teknologi keamanan, terutama dalam hal enkripsi homomorfik, dengan fokus pada penyelesaian tantangan teknis dan menjaga keseimbangan antara tingkat keamanan dan kinerja yang optimal. Kedua, pendidikan dan kesadaran tentang pentingnya kriptografi dan praktik keamanan siber harus ditingkatkan di semua lapisan masyarakat. Ketiga, penting bagi pemerintah untuk mengembangkan hukum dan kebijakan yang mendukung penggunaan kriptografi yang aman. Sehingga kita dapat terus memanfaatkan kemajuan kriptografi untuk menjaga keamanan dan privasi dalam era digital yang terus berkembang.

Daftar Pustaka

Agustina, L., Sujarwo, I., & Khudzaifah, M. (2023). Membangun Super Enkripsi untuk Mengamankan Pesan. *Jurnal Riset Mahasiswa Matematika*, *2*(5), 195–200. https://doi.org/10.18860/jrmm.v2i5.21036

Aufia, Z., Turmudi, T., & Alisah, E. (2021). Enkripsi dan Dekripsi Pesan Menggunakan Metode Vigenere Cipher dan Route Cipher. *Jurnal Riset Mahasiswa Matematika*, *1*(2), 93–104. https://doi.org/10.18860/jrmm.v1i2.14207

Basri. (2016). Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Jurnal Ilmiah Ilmu Komputer*, *2*(2). http://ejournal.fikom-unasman.ac.id/index.php/jikom/article/view/82%0Ahttp://ejournal.fikom-unasman.ac.id/index.php/jikom/article/download/82/55

Deviani, R., Nazhifah, S. A., Aulia, D., & Aziz, S. (2022). Fully Homomorphic Encryption (FHE) pada Penyimpanan Data E-Government Berbasis Cloud. *Jurnal Pendidikan Teknologi Informasi*, *6*(2), 105–118.

Naji Maruf Ilyas, K. (2018). Digital Signature with Cryptosystem Algorithm Rivest Shamir and Adleman (RSA). *Jurnal Kajian Dan Terapan Matematika*, *7*(4), 1–9. https://doi.org/10.31857/s013116462104007x