

Penerapan Algoritma Kriptografi Dalam Menjaga Keamanan Data Pada Kehidupan Sehari-Hari

Rudi Arachman

Universitas Qamarul Huda Badaruddin – Nusa Tenggara Barat

hamjahdiha@unighba.ac.id

| 5

ARTICLE INFO**Article history:**

Received Maret, 2026

Revised April , 2026

Accepted Juli, 2026

Available online Juli 2026

Kata Kunci: *Algoritma, Kriptografi, Enkripsi, Keamanan Data, Privasi Digital*

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.
Copyright © 2026 by Author. Published by KABAR_MOE

ABSTRAK

Di era transformasi digital, keamanan dan privasi data menjadi aspek fundamental dalam menunjang mobilitas masyarakat. Setiap aktivitas komunikasi, transaksi keuangan, dan penyimpanan data pribadi yang terhubung dengan jaringan publik sangat rentan terhadap ancaman kejahatan siber seperti penyadapan, peretasan, dan pencurian identitas. Penelitian ini bertujuan untuk mengkaji secara komprehensif implementasi serta mekanisme kerja algoritma kriptografi modern dalam melindungi data pribadi pengguna pada berbagai aplikasi kehidupan sehari-hari. Metode yang digunakan dalam penelitian ini adalah metode kualitatif deskriptif berbasis studi pustaka (*literature review*) dengan menganalisis literatur ilmiah, standar industri, dan kajian teknis terkait. Hasil kajian menunjukkan bahwa algoritma kriptografi seperti *Advanced Encryption Standard* (AES), *Rivest–Shamir–Adleman* (RSA), *Elliptic Curve Cryptography* (ECC), dan

Secure Hash Algorithm (SHA-256) bekerja secara terintegrasi di belakang layar (*invisible*). Penggunaan enkripsi simetris, asimetris, fungsi *hash*, hingga *end-to-end encryption* berhasil memberikan jaminan terhadap empat pilar keamanan informasi: *confidentiality*, *integrity*, *authentication*, dan *non-repudiation*. Kehadiran teknologi ini terbukti efektif menjadi benteng pertahanan utama dalam menjaga privasi dan keamanan data pengguna pada platform pemesanan instan, perbankan digital, transaksi *e-commerce*, protokol HTTPS, hingga kartu berbasis cip.

LATAR BELAKANG

Perkembangan teknologi informasi di era digital secara fundamental telah mengubah paradigma interaksi, pola kerja, serta mekanisme transaksi masyarakat modern. Hampir seluruh aktivitas harian kini telah terintegrasi secara dinamis dengan jaringan internet global. Aktivitas seperti pengiriman pesan instan, belanja melalui platform *e-commerce*, pengaksesan dokumen cloud, hingga pengelolaan aset finansial via *mobile banking* telah menjadi bagian yang tak terpisahkan dari gaya hidup digital. Tingkat mobilitas dan ketergantungan digital yang sangat tinggi tersebut menghasilkan arus lalu lintas data yang sangat masif setiap detiknya. Data yang lalu lalang di dalam jaringan publik ini mencakup beragam informasi penting, mulai dari percakapan pribadi, data kredensial login, nomor rekening, hingga catatan riwayat transaksi keuangan. Kondisi ini menempatkan data sebagai salah satu komoditas berharga yang memerlukan perlindungan ekstra.

Namun, di balik segala kemudahan dan efisiensi yang ditawarkan, ruang digital juga membawa ancaman dan potensi bahaya yang sangat besar terkait keamanan informasi. Arsitektur jaringan internet yang bersifat terbuka secara inherent rentan terhadap tindak kejahatan siber (*cybercrime*). Berbagai kejahatan seperti penyadapan (*eavesdropping*), peretasan (*hacking*), penipuan (*phishing*), dan pencurian identitas (*identity theft*) terus mengalami peningkatan kompleksitas.

| 6

Tanpa adanya mekanisme perlindungan yang memadai, privasi dan data sensitif milik pengguna di ruang digital akan berada dalam posisi yang sangat rawan disalahgunakan. Kebocoran data pribadi dapat menimbulkan kerugian finansial yang signifikan, rusaknya reputasi individu maupun institusi, hingga potensi pelanggaran hukum. Oleh karena itu, ketersediaan arsitektur perlindungan data yang andal dan kokoh mutlak diperlukan sebagai syarat utama keberlanjutan ekosistem digital. Dalam menjawab ancaman kejahatan siber modern tersebut, salah satu pilar utama yang bertindak sebagai fondasi keamanan dalam arsitektur teknologi informasi adalah kriptografi. Kriptografi menyajikan sekumpulan instrumen matematika dan prosedur teknis yang dirancang untuk mengamankan data. Melalui pendekatan ini, data mentah yang rahasia diubah sedemikian rupa sehingga tidak dapat dibaca oleh pihak-pihak yang tidak terotorisasi.

Meskipun pada dasarnya kriptografi berlandaskan pada teori matematika dan algoritma terstruktur yang terkesan rumit, manifestasi serta penerapan dari teknologi ini sebenarnya sangat dekat dengan aktivitas masyarakat sehari-hari. Tanpa disadari, berbagai platform digital, perangkat pintar, dan aplikasi komunikasi yang digunakan secara rutin terus menjalankan fungsi kriptografi di balik layar (*invisible process*). Sayangnya, karena mekanisme keamanan ini bekerja secara otomatis dan tidak kasat mata, sebagian besar masyarakat awam belum menyadari keberadaan teknologi ini. Banyak pengguna aktif internet yang belum memahami secara mendalam bagaimana data dan hak privasi mereka dilindungi oleh sistem keamanan berbasis kriptografi tersebut. Rendahnya pemahaman ini juga berpotensi mengurangi kewaspadaan pengguna terhadap ancaman keamanan siber.

Oleh sebab itu, penting untuk mengangkat topik ini ke dalam sebuah kajian ilmiah. Pemahaman mengenai cara kerja pertahanan data digital tidak boleh hanya didominasi oleh para praktisi IT atau akademisi keamanan siber, melainkan juga perlu dipahami oleh masyarakat luas sebagai pengguna aktif teknologi. Berdasarkan urgensi tersebut, artikel ilmiah ini disusun untuk mengupas secara mendalam contoh nyata pemanfaatan algoritma kriptografi pada kehidupan sehari-hari serta mekanismenya dalam menjaga kerahasiaan dan privasi data. Berdasarkan perumusan masalah yang diangkat, penelitian ini memiliki beberapa tujuan utama sebagai berikut: (a) Mengidentifikasi dan menganalisis secara mendalam berbagai bentuk implementasi algoritma kriptografi yang sering ditemui dalam aktivitas dan aplikasi kehidupan sehari-hari, dan (b) Menjelaskan secara teknis dan konseptual mekanisme kerja algoritma kriptografi dalam menjamin keamanan, integritas, autentikasi, serta perlindungan privasi data pengguna di ruang digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif berbasis metode studi pustaka (*literature review*). Data dan informasi dihimpun dari berbagai sumber literatur sekunder yang relevan, seperti buku teks ilmiah mengenai keamanan jaringan, publikasi standar keamanan nasional/internasional (NIST, FIPS), serta artikel jurnal terindeks yang membahas penerapan kriptografi pada aplikasi digital modern.

| 7

Proses analisis dilakukan melalui beberapa tahap, yaitu pengumpulan data literatur, reduksi dan klasifikasi data berdasarkan variabel penerapan algoritma, sintesis mekanisme kerja teknis, serta penarikan kesimpulan deskriptif mendalam mengenai peran kriptografi dalam perlindungan data harian.

HASIL DAN PEMBAHASAN

Penggunaan algoritma kriptografi dalam kehidupan sehari-hari merupakan bukti konkret dari penerapan ilmu matematika mutakhir untuk menjawab kebutuhan keamanan di era digital. Salah satu contoh penerapan paling nyata dapat ditemukan pada aplikasi perpesanan instan populer seperti WhatsApp dan Signal. Platform-platform ini mengimplementasikan protokol *End-to-End Encryption* (E2EE) berbasis enkripsi asimetris dan simetris secara hybrid. Dalam mekanisme E2EE, pesan dienkripsi secara langsung pada perangkat pengirim dan hanya dapat didekripsi pada perangkat penerima. Penyedia layanan aplikasi maupun peretas yang mencegat data di tengah jalan hanya akan melihat deretan *ciphertext* acak yang tidak dapat dibaca.

Penerapan krusial lainnya berada pada sektor perbankan digital dan sistem transaksi *e-commerce*. Saat pengguna melakukan transfer dana via *mobile banking* atau pembayaran belanja *online*, data finansial sensitif seperti nomor kartu, PIN, dan kode CVV dilindungi menggunakan algoritma enkripsi standar industri seperti *Advanced Encryption Standard* (AES-256). Algoritma simetris berkecepatan tinggi ini memastikan bahwa data finansial yang mentransit jaringan publik terlindungi rapat dari kejahatan *sniffing* atau penyadapan.

Di dunia *web browsing*, protokol *Hypertext Transfer Protocol Secure* (HTTPS) menjadi standar wajib untuk menjamin keamanan interaksi *online*. Ketika pengguna mengakses alamat situs web HTTPS, koneksi antara browser dan server web diamankan menggunakan protokol *Transport Layer Security* (TLS/SSL). Protokol TLS memfasilitasi pertukaran kunci aman (*handshake*) dengan mengandalkan algoritma asimetris seperti RSA atau ECC. Proses ini memastikan bahwa seluruh aktivitas navigasi, data *form*, dan *session cookie* pengguna tersandi secara rahasia.

Aspek penting lainnya dari kriptografi harian adalah pada sistem penyimpanan kata sandi (*password storage*). Sistem database modern yang kredibel tidak pernah menyimpan *password* pengguna dalam format teks biasa (*plaintext*). Sebaliknya, sistem memanfaatkan fungsi *hash* kriptografi satu arah seperti SHA-256. Ketika pengguna

membuat *password*, sistem akan mengonversinya menjadi nilai *hash digest* acak. Saat proses login dilakukan, sistem hanya membandingkan nilai *hash* dari input yang dimasukkan dengan nilai *hash* di database. Hal ini menjaga agar kata sandi asli tetap aman meskipun database mengalami kebocoran.

Teknologi kartu finansial seperti kartu ATM dan kartu kredit berteknologi cip (EMV standard) juga mengandalkan algoritma kriptografi secara intensif. Cip pintar pada kartu memuat kunci kriptografi rahasia dan mikroprosesor yang mampu melakukan komunikasi enkripsi dengan mesin EDC atau ATM. Setiap kali transaksi berlangsung, cip menghasilkan kode autentikasi dinamis yang unik. Mekanisme ini membendung potensi penggandaan kartu (*card cloning*) dan menjamin keaslian identitas pemegang kartu.

| 8

Secara mekanis, proses perlindungan privasi oleh kriptografi diawali dari proses transformasi dasar. Data mentah (*plaintext*) diproses oleh algoritma enkripsi matematika bersama dengan sebuah kunci (*key*) untuk menghasilkan *ciphertext*. Hanya penerima sah yang memiliki kunci dekripsi yang relevan yang dapat merekonstruksi *ciphertext* tersebut kembali menjadi *plaintext*. Pada skema kunci simetris, kunci enkripsi dan dekripsi bersifat identik, sedangkan pada kunci asimetris, pengirim menggunakan *public key* penerima dan penerima menggunakan *private key* miliknya yang bersifat rahasia.

Selain aspek kerahasiaan (*confidentiality*), algoritma kriptografi memainkan peran vital dalam menjaga integritas data (*data integrity*). Dalam proses pengiriman data, penggunaan fungsi *hash* seperti SHA-256 menjamin bahwa data tidak diubah, ditambah, atau dikurangi oleh pihak ketiga. Fungsi *hash* memiliki sifat yang sangat sensitif; perubahan satu bit data saja akan menghasilkan nilai *hash* (*avalanche effect*) yang jauh berbeda, sehingga manipulasi data dapat langsung terdeteksi oleh sistem.

Terakhir, aspek autentikasi dan nirpenyangkalan (*non-repudiation*) diwujudkan melalui mekanisme tanda tangan digital (*digital signature*). Dengan mengombinasikan fungsi *hash* dan kriptografi asimetris (seperti RSA atau ECC), tanda tangan digital memungkinkan penerima memverifikasi keaslian pengirim dokumen atau transaksi secara pasti. Pengirim tidak dapat menyangkal transaksi yang telah dilakukannya karena tanda tangan digital tersebut secara unik terikat pada *private key* milik pengirim. Dengan demikian, kombinasi enkripsi, *hashing*, dan tanda tangan digital membentuk sistem pertahanan holistik yang menjaga privasi dan keamanan masyarakat di ruang digital.

SIMPULAN

Berdasarkan analisis dan pembahasan yang telah dipaparkan, dapat disimpulkan bahwa algoritma kriptografi merupakan infrastruktur tak terlihat namun sangat krusial dalam menjaga ekosistem digital modern. Kriptografi tidak hanya berfungsi menyandikan data (*confidentiality*), tetapi juga menjamin keutuhan data (*integrity*), kepastian identitas (*authentication*), serta keabsahan transaksi (*non-repudiation*). Implementasi nyata kriptografi dapat dirasakan secara langsung dalam kehidupan harian, seperti pada aplikasi pesan instan E2EE, transaksi perbankan digital, komunikasi web berbasis

HTTPS, penyimpanan *password* berteknologi *hash*, serta kartu ATM cip.

Untuk menghadapi ancaman siber yang semakin kompleks di masa depan, disarankan agar masyarakat sebagai pengguna akhir (*end-user*) terus meningkatkan literasi keamanan digital, seperti menggunakan kata sandi yang kuat dan menerapkan *Two-Factor Authentication* (2FA). Sementara itu, para pengembang aplikasi dan penyedia layanan teknologi harus secara konsisten memperbarui standar algoritma kriptografi mereka sesuai dengan rekomendasi standar industri untuk menangkal teknik-teknik eksploitasi baru.

| 9

DAFTAR PUSTAKA

- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
- National Institute of Standards and Technology (NIST). (2015). *Secure Hash Standard (SHS)* (FIPS PUB 180-4). National Institute of Standards and Technology.
- Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
- Telkom University. (2023a). *Apa itu Algoritma: Pengertian, Ciri-ciri, Jenis dan Contohnya dalam Kehidupan Sehari-hari*. Diakses dari <https://telkomuniversity.ac.id/apa-itu-algoritma-pengertian-ciri-ciri-jenis-dan-contohnya-dalam-kehidupan-sehari-hari/>
- Telkom University. (2023b). *Apa itu Kriptografi: Pengertian, Jenis, dan Manfaat*. Diakses dari <https://it.telkomuniversity.ac.id/kriptografi-adalah/>
- Telkom University. (2023c). *Mengenal Kriptografi: Rahasia di Balik Enkripsi Data Digital*. Diakses dari <https://msf.telkomuniversity.ac.id/mengenal-kriptografi-rahasia-di-balik-enkripsi-data-digital/>