Inovan Publisher

Orbit: Jurnal Ilmu Multidisplin Nusantara

| ISSN (Online) 3064-5883 |

DOI: 10.63217/orbit.v2i1.194

Teknologi Enkripsi untuk Komunikasi Aman

Achmad Fauzi[1], Bungaran Saing[2], Elly Nurkhayati[3], Murni Nur Aulia[4], Sabikah Ophelia[5], Salma Ahmad[6]
[1]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[2]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, bungaran.saing@dsn.ubharajaya.ac.id
[3]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, ellynurkhayati3@gmail.com
[4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, murninuraulia28@gmail.com
[5]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, sabikahophelia27.7g@gmail.com
[6]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, salmahhmd2908@gmail.com

Corresponding Author: achmad.fauzi@dsn.ubharajaya.ac.id[1]

Abstract: *This study aims to analyze the role of encryption technology in maintaining digital communication security, especially in the context of increasing threats of data leaks and cyber attacks in the modern era. This study uses a literature review method by examining various journals, books, and relevant publications on symmetric encryption, asymmetric encryption, end-to-end encryption, zero-trust encryption, and the application of security protocols such as SSL/TLS, PGP, and S/MIME. The results of this study show that each type of encryption has different characteristics and functions but complement each other, especially in maintaining data confidentiality, integrity, and authentication. This study confirms that encryption technology is a fundamental component in building secure digital communications, especially for the government sector, companies, and general users.*

Keywords: *Encryption, Secure Communication, E2EE, Zero-Trust, SSL/TLS, PGP, S/MIME.*

Abstrak: Penelitian ini bertujuan untuk menganalisis peran teknologi enkripsi dalam menjaga keamanan komunikasi digital, terutama pada konteks meningkatnya ancaman kebocoran data dan serangan siber di era modern. Penelitian ini menggunakan metode studi literatur dengan mengkaji berbagai jurnal, buku, dan publikasi yang relevan mengenai enkripsi simetris, asimetris, end-to-end encryption, zero-trust encryption, serta penerapan protokol keamanan seperti SSL/TLS, PGP, dan S/MIME. Hasil penelitian menunjukkan bahwa setiap jenis enkripsi memiliki karakteristik dan fungsi berbeda tetapi saling melengkapi, terutama dalam menjaga kerahasiaan, integritas, dan autentikasi data. Penelitian ini menegaskan bahwa teknologi enkripsi merupakan komponen fundamental dalam membangun komunikasi digital yang aman, terutama bagi sektor pemerintahan, perusahaan, hingga pengguna umum.

Kata Kunci: Enkripsi, Komunikasi Keamanan, *E2EE, Zero-Trust, SSL/TLS, PGP, S/MIME*.

PENDAHULUAN

Di era digital saat ini, keamanan tidak hanya berkaitan dengan perlindungan terhadap aset fisik, tetapi juga terhadap informasi yang tersimpan dan dipertukarkan secara elektronik. Data yang tersimpan dalam sistem digital khususnya dalam database memiliki nilai yang sangat penting, baik dalam sektor bisnis, pendidikan, maupun pemerintahan. Oleh karena itu, data harus dijaga kerahasiaan, integritas, dan ketersediaannya agar tidak mengalami kebocoran ataupun penyalahgunaan.

Meningkatnya kasus kebocoran data di Indonesia menunjukkan bahwa perlindungan data digital masih menghadapi banyak tantangan. Kebocoran tersebut tidak hanya berdampak pada aspek privasi, tetapi juga menurunkan kepercayaan publik terhadap layanan digital dan berpotensi menimbulkan kerugian ekonomi. Salah satu cara utama untuk meminimalkan risiko tersebut adalah melalui penerapan teknologi enkripsi.

Enkripsi merupakan proses mengubah data asli (*plaintext*) menjadi bentuk kode yang tidak dapat dipahami oleh pihak yang tidak berwenang (*ciphertext*). Dengan menggunakan algoritma tertentu, enkripsi memastikan bahwa hanya pihak yang memiliki kunci yang sah yang dapat mengembalikan data tersebut ke bentuk semula. Secara umum, enkripsi terbagi menjadi dua jenis utama, yaitu enkripsi simetris yang menggunakan satu kunci yang sama, dan enkripsi asimetris yang menggunakan pasangan kunci publik dan privat.

Penerapan enkripsi kini menjadi fondasi utama dalam berbagai platform digital. Salah satu bentuk implementasinya adalah *End-to-End Encryption* (E2EE) yang digunakan pada aplikasi WhatsApp untuk memastikan pesan hanya dapat dibaca oleh pengirim dan penerima. Selain itu, protokol SSL/TLS digunakan pada situs web untuk mengamankan komunikasi antara browser dan server melalui jalur terenkripsi. Teknologi enkripsi juga menjadi dasar pada keamanan email melalui dua protokol, yaitu PGP dan S/MIME, yang keduanya menyediakan kerahasiaan, autentikasi, serta perlindungan integritas pesan.

Secara keseluruhan, teknologi enkripsi memiliki peran yang sangat vital dalam menghadapi ancaman siber dan menjaga keamanan komunikasi digital. Dengan kemampuannya melindungi data dari akses pihak yang tidak berwenang, enkripsi menjadi pilar utama dalam membangun ekosistem digital yang aman, terpercaya, dan berkelanjutan.

Berdasarkan uraian pada pendahuluan, penelitian ini berfokus pada tiga pokok masalah utama. Pertama, bagaimana konsep dasar *Zero-Trust Encryption* diterapkan sebagai mekanisme perlindungan data digital dengan mengacu pada berbagai sumber penelitian terdahulu yang membahas teknologi enkripsi dalam komunikasi digital dan protokol keamanan seperti SSL/TLS, PGP, dan S/MIME.

METODE

Penelitian ini menggunakan metode Studi Literatur, yaitu menganalisis berbagai sumber ilmiah seperti jurnal nasional dan internasional, buku, artikel ilmiah, dan publikasi digital terkait enkripsi, keamanan data, dan komunikasi digital. Peneliti mengumpulkan data sekunder berupa teori, studi kasus, dan hasil penelitian terdahulu. Literatur dipilih berdasarkan relevansi dengan topik keamanan komunikasi dan penerapan teknologi enkripsi. Setelah pengumpulan data, peneliti melakukan analisis komparatif untuk mengidentifikasi konsep utama, kelebihan dan kelemahan enkripsi, serta implementasinya dalam berbagai platform digital. Hasil analisis kemudian disintesis menjadi pembahasan yang komprehensif mengenai pentingnya enkripsi dalam menjaga keamanan komunikasi.

Tabel 1. Penelitian Terdahulu

No	Penelitian Terdahulu	Tujuan Penelitian	Persamaan Jurnal	Perbedaan Jurnal	Hasil Penelitian
1	"Analisa Keamanan pada Aplikasi WhatsApp Menggunakan Enkripsi End to End." Oleh Ananda Aufa R dkk.	Pada penelitian ini bertujuan untuk membahas penggunaan aplikasi chatting seperti WhatsApp yang melindungi data privasi pengguna dengan menggunakan teknik enkripsi end to end, dengan metodologi kualitatif dan pendekatan studi literatur	Sama-sama membahas keamanan data digital dan bagaimana enkripsi digunakan sebagai perlindungan kerahasiaan komunikasi. Menekankan pentingnya E2EE untuk mencegah penyadapan dan mengamanka n pesan pengguna. Berada dalam ranah keamanan informasi dan kriptografi modern.	Fokus utama pada analisis E2EE pada WhatsApp sebagai objek tunggal. Menggunakan pendekatan kualitatif berbasis studi literatur tanpa pengujian teknis. Pembahasan lebih banyak pada aspek praktis penggunaan enkripsi pada aplikasi pesan instan.	Hasil dari penelitian ini adalah Enkripsi end-to-end pada WhatsApp terbukti sangat efektif dalam melindungi keamanan serta privasi data penggunanya. Selain itu, Enkripsi end to end pada WhatsApp memberikan perlindungan seperti pengelolaan kunci, penggunaan generator dengan pilihan kode-kode acak dan algoritma kriptografi yang kuat, sehingga pesan tetap aman dari upaya peretasan maupun penyadapan selama proses pengiriman.
2	"Melindungi Data Di Dunia Digital: Peran Strategis Enkripsi dalam Keamanan Data." Oleh Alisa Almadira dkk.	Bertujuan membahas ancaman keamanan digital dan pentingnya enkripsi sebagai alat utama untuk melindungi data pribadi terutama pada efektivitasan	Sama-sama menyoroti pentingnya enkripsi sebagai alat untuk melindungi data dari akses tidak sah. Mengkaji peran enkripsi dalam menjaga *confidentiality , integrity,* dan	Membahas berbagai algoritma (AES, RSA, SSL/TLS, E2EE) dalam banyak sektor seperti perbankan, kesehatan dan pemerintahan. Memiliki cakupan lebih luas dibanding jurnal	Hasil penelitian bahwa enkripsi sangat penting Untuk melindungi data agar tidak diakses oleh pihak yang tidak berwenang. Metode seperti AES, RSA, enkripsi end-to-end, dan

		algoritma enkripsi populer, yaitu AES (*Advanced Encryption Standard*) dan RSA (*Rivest–Shamir–Adleman*), dalam mengamankan data baik yang disimpan maupun yang dikirimkan di berbagai sektor seperti keuangan, kesehatan, dan pemerintahan.	*availability*. Relevan dalam pembahasan keamanan data digital lintas sektor.	lain yang fokus pada WhatsApp atau email. Mengangkat isu masa depan seperti *Post-Quantum Cryptography*.	SSL/TLS. Selain enkripsi sebagai keamanan perlu adanya pengembangan lebih mendalam terkait Kriptografi Pasca-Kuantum dan *Zero-Knowledge Protocol* agar perlindungan data tetap kuat di masa depan.
3	"Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi." Oleh Basri.	Bertujuan membahas mengenai pentingnya keamanan data dalam perusahaan dan bagaimana metode kriptografi dapat digunakan untuk menjaga kerahasiaan serta integritas informasi. Dengan masalah utama yang dikaji adalah bagaimana memastikan data tetap aman saat dikirim agar tidak dapat diakses oleh pihak yang tidak berwenang.	Sama-sama mengkaji algoritma enkripsi dalam menjaga keamanan komunikasi data. Membahas peran kriptografi sebagai mekanisme pengamanan informasi sensitif. Mengulas konteks keamanan digital serta ancaman data	Fokus pada analisis teoretis dan komputasional kriptografi simetris vs asimetris. Menilai kecepatan, efisiensi, dan kompleksitas algoritma. Tidak mengambil studi kasus aplikasi tertentu seperti WhatsApp.	Penelitian ini memiliki Hasil penelitian menunjukkan Bahwa kedua metode memiliki tingkat keakuratan yang sama, namun kriptografi asimetris memiliki proses yang lebih kompleks dan membutuhkan waktu lebih lama. Meski demikian, metode asimetris memberikan tingkat keamanan yang lebih tinggi dibandingkan metode simetris.

HASIL DAN PEMBAHASAN

Aktivitas digital seperti berkomunikasi meningkatkan resiko kebocoran data dan ancaman keamanan siber. Dalam kondisi ini komunikasi keamanan menjadi aspek yang krusial dan perlu perhatian penuh. Salah satu cara menjaga keamanan digital adalah dengan proses enkripsi, yang di mana proses enkripsi mengubah bentuk asli *plain-text* menjadi sebuah kode acak atau *cipher-text*. Dalam konsep komunikasi keamanan enkripsi berperan sebagai "pelindung" untuk data informasi pribadi, pesan, dan data lainnya meskipun ia berada dalam jangkauan digital yaitu internet.

Dalam pembahasan mengenai teknologi enkripsi dalam komunikasi keamanan, hal yang

perlu dipahami terlebih dahulu adalah bahwa keamanan komunikasi merupakan elemen kunci bagi seluruh aktivitas digital modern. Komunikasi yang dilakukan melalui jaringan internet rentan terhadap penyadapan, manipulasi, dan pencurian informasi sensitif, sehingga teknologi enkripsi menjadi pondasi utama yang menjaga kerahasiaan, integritas, dan autentikasi data. Enkripsi memastikan bahwa pesan, data pribadi, maupun transaksi digital dapat dikirim dengan aman tanpa dapat dibaca oleh pihak yang tidak berwenang. Dengan demikian, enkripsi tidak hanya menjadi fitur tambahan dalam dunia digital saja, tetapi telah menjadi kebutuhan mutlak dalam menjaga keamanan komunikasi di jaman sekarang.

Melihat dari penelitian terdahulu oleh Almira dkk. Ia menyatakan enkripsi adalah teknologi yang strategis dalam menjaga keamanan, kerahasiaan, integritas. Data yang dilindungi cukup beragam, seperti dalam sektor perbankan, kesehatan, dan pemerintahan. Proses enkripsi adalah fondasi keamanan komunikasi digital. Enkripsi sendiri memiliki dua bentuk utama, yaitu enkripsi simetris dan asimetris.

Enkripsi simetris menggunakan metode satu kunci yang sama untuk proses enkripsi dan deskripsi, dengan sistem yang lebih cepat sehingga cocok untuk mengamankan data dalam jumlah yang besar. Namun, dalam penggunaannya enkripsi simetris memiliki tantangan tersendiri, yaitu proses distribusi satu kunci yang menyebar. Kunci yang sama ini dibagikan ke banyak pengguna sehingga dapat beresiko mengancam keamanan komunikasi. Sedangkan enkripsi asimetris menggunakan dua kunci berbeda, yaitu kunci publik dan kunci privat, maka dikatakan pesan yang dienkripsikan dengan kunci publik hanya dapat di deskripsi menggunakan kunci privat yang dimiliki oleh penerima. Berdasarkan penelitian terdahulu oleh Basri, enkripsi simetris dan asimetri keduanya memiliki kelebihan dan kekurangannya sendiri, apabila mereka berdua digabungkan hal ini akan menciptakan komunikasi yang lebih cepat seperti protokol SSL/TLS dan sistem E2EE.

Penerapan enkripsi E2EE atau *End to End Encryption* ini berguna untuk memastikan bahwa pesan hanya dapat dibaca oleh pihak yang bersangkutan, yaitu pihak pengirim dan pihak penerima saja. Dalam penelitian terdahulu oleh Ananda Aufa dkk serta penelitian oleh Totnay Clarita dkk, menunjukan bahwa aplikasi *chatting* seperti WhatsApp menggunakan keamanan yang kompleks seperti *Identity Key, Signed Pre-Key,* dan *Double Ratchet Algorithm*. Dengan adanya sistem keamanan seperti ini tentu saja dapat melindungi privasi pengguna WhatsApp, yang di mana pesan terenkripsi oleh algoritma kriptografi dan berubah menjadi deretan kode acak, dan akan kembali kebentuk awal pesan apabila diterima oleh penerima pesan yang sah. Dalam konteks komunikasi keamanan, E2EE berperan penting karena individu pada era saat ini sering bertukar informasi penting tanpa sadar, seperti data pribadi, nomor pin, lokasi dan sebagainya. Dengan adanya E2EE inilah yang dapat melindungi pengguna dari tindakan perentas. Selailn itu pada perkembangan teknologi digital menghadirkan konsep baru dari enkripsi, yaitu konsep *Zero-Trust Encryption*.

Konsep *Zero-Trust Encryption* memiliki prinsip bahwa "*Never Trust, Always Verify.*" yang di mana jangan mudah percaya pada jaringan sistem yang dianggap aman. Konsep *Zero-Trust Encryption* mengharuskan setiap pengguna untuk verifikasi data secara berulang sebelum meminta akses atau mengizinkan akses, seperti yang dikatakan dalam penelitian terdahulu oleh Toorpu Arvind Reddy, ia menekankan bahwa *Zero-Trust* sangat efektif untuk migrasi database, penyimpanan *cloud*, dan perlindungan dalam lingkungan perusahaan besar. Sistem ini membantu mencegah kebocoran data jika salah satu bagian sistem disusupi. Hal ini tentunya berkaitan dengan komunikasi keamanan dan sangat relevan dalam kategori pekerjaan di jaman sekarang yang bisa di akses dan dimuat di mana saja hanya melalui berbagai perangkat dan jaringan yang tidak selalu aman.

Sebagai jembatan antara konsep dan praktik, penting dicatat bahwa prinsip *Zero-Trust* "*Never Trust, Always Verify*" tidak hanya bersifat teoretis tetapi harus diseimbangi oleh mekanisme

enkripsi nyata pada protokol dan layanan sehari-hari. Selain itu prinsip *Zero-Trust* ini juga menegaskan pentingnya enkripsi dan verifikasi yang berlapis pada setiap titik komunikasi digital, dengan menerapkan enkripsi *end-to-end*, sertifikat digital, dan manajemen kunci yang ketat pada lapisan komunikasi. Seperti contohnya pada protokol standar TLS/SSL untuk web, PGP atau S/MIME untuk email. Banyak organisasi atau perusahaan yang sudah menerapkan verifikasi berulang dan pembatasan akses yang dimana ini menjadi inti dari *Zero-Trust*. Oleh karena itu, pembahasan mengenai protokol-protokol standar seperti TSL/SSL, PGP dan S/MIME yang menjadi titik utama pada keamanan komunikasi.

Penerapan enkripsi terlihat jelas pada berbagai protokol standar yang digunakan dalam kehidupan digital sehari-hari. Salah satu yang paling umum adalah SSL/TLS, yang digunakan pada koneksi HTTPS untuk melindungi komunikasi antara browser dan server. Protokol ini melakukan proses *handshake*, pertukaran sertifikat digital, dan validasi identitas server sehingga pengguna dapat memastikan bahwa mereka berkomunikasi dengan pihak yang benar. Dengan perlindungan SSL/TLS, data sensitif seperti kata sandi, informasi bank, atau identitas pribadi dapat dikirim melalui internet tanpa mudah disadap. Penggunaan protokol ini sangat penting bagi layanan keuangan, *e-commerce*, dan situs web pemerintah yang menangani banyak data sensitif masyarakat.

Selain komunikasi web, komunikasi melalui email juga membutuhkan tingkat keamanan tinggi. Dua protokol utama yang digunakan dalam pengamanan email adalah PGP dan S/MIME. PGP menggabungkan enkripsi simetris dan asimetris untuk mengamankan pesan dan file digital. Sistem ini juga memiliki mekanisme *web-of-trust* yang memungkinkan pengguna untuk memverifikasi keaslian kunci publik satu sama lain. Dalam penelitian Fahrudin Azis dan Zaida, menunjukkan bahwa PGP dapat membantu penyelidikan apabila kunci privat berhasil ditemukan, sehingga konten terenkripsi dapat dianalisis untuk keperluan hukum. Sementara itu, S/MIME bekerja menggunakan sertifikat digital yang dikeluarkan oleh *Certificate Authority,* memberikan tingkat kepercayaan yang tinggi terhadap identitas pengirim email. Hal ini menjadikan S/MIME banyak digunakan oleh instansi pemerintah dan organisasi besar yang membutuhkan standar keamanan dan autentikasi yang lebih ketat.

Walaupun enkripsi telah memberikan perlindungan yang kuat, teknologi ini tidak bebas dari tantangan dan ancaman. Kesalahan implementasi dapat menyebabkan celah keamanan yang dapat dimanfaatkan oleh penyerang, seperti serangan EFAIL yang menargetkan PGP dan S/MIME melalui manipulasi HTML pada email. Selain itu, enkripsi berpotensi disalahgunakan oleh kelompok kriminal untuk menyembunyikan aktivitas ilegal sehingga menyulitkan proses penyelidikan digital. Tantangan lain mencakup manajemen kunci yang kompleks terutama pada sistem berskala besar, serta ancaman masa depan dari komputasi kuantum yang memiliki kemampuan memecahkan algoritma enkripsi tradisional dengan kecepatan lebih tinggi. Oleh karena itu, pengembangan teknologi enkripsi harus dilakukan secara berkelanjutan agar tetap mampu menghadapi risiko dan ancaman yang terus berkembang.

Di Indonesia sendiri isu keamanan digital menjadi semakin menonjol seiring meningkatnya kasus kebocoran data yang berdampak pada masyarakat. Seperti kebocoran data KTP, NPWP, melalui banyaknya insiden tersebut menunjukkan bahwa sistem keamanan yang digunakan oleh berbagai penyedia layanan di indonesia masih belum optimal, terutama dalam teknologi enkripsi. Maka untuk mengatasi hal ini, penting bagi instansi pemerintah, perusahaan swasta, sektor perbankan, dan lembaga pendidikan untuk meningkatkan penerapan teknologi enkripsi pada setiap sistem digital yang mereka gunakan. Penggunaan SSL/TLS pada situs web resmi, pemanfaatan E2EE pada aplikasi komunikasi, serta penggunaan PGP atau S/MIME pada email instansi adalah langkah strategis yang dapat meningkatkan keamanan digital nasional. Dengan implementasi enkripsi yang lebih konsisten, tingkat kepercayaan masyarakat terhadap layanan

digital juga akan meningkat, sekaligus menciptakan ekosistem komunikasi yang lebih aman dan tidak mudah untuk terkena ancaman siber.

Dari keseluruhan pembahasan, terlihat jelas bahwa enkripsi merupakan satu elemen krusial dalam menjaga keamanan komunikasi digital. Enkripsi simetris, asimetris, *end-to-end encryption*, dan model *zero-trust* memberikan perlindungan penting yang mencegah penyadapan dan manipulasi data. Sementara itu, protokol seperti SSL/TLS, PGP, dan S/MIME memperkuat keamanan pada komunikasi web dan email. Meskipun dalam implementasinya enkripsi menghadapi tantangan dan ancaman teknologi, manfaatnya tetap sangat besar bagi perlindungan data dan privasi pengguna. Oleh karena itu, penerapan teknologi enkripsi harus terus menerus ditingkatkan agar mampu menjawab tantangan komunikasi digital modern, baik itu secara global maupun dalam secara lokal.

KESIMPULAN

Enkripsi merupakan suatu komponen yang fundamental dalam menjaga keamanan komunikasi digital. Di tengah meningkatnya aktivitas komunikasi melalui internet dan besarnya risiko kebocoran data, enkripsi berfungsi sebagai pelindung utama yang memastikan kerahasiaan, integritas, dan autentikasi informasi tetap terjaga. Enkripsi simetris, asimetris, *End-to-End Encryption*, dan konsep *Zero-Trust Encryption* menyediakan mekanisme perlindungan yang saling melengkapi. Mulai dari pengamanan pesan, pertukaran kunci, hingga validasi identitas pengguna. Selain itu, protokol seperti SSL/TLS, PGP, dan S/MIME juga memperkuat keamanan pada komunikasi web dan email, terutama pada sektor yang menangani informasi sensitif seperti layanan keuangan, pemerintahan, dan instansi besar lainnya.

Meskipun memiliki manfaat yang signifikan, teknologi enkripsi juga menghadapi tantangan seperti kerentanan implementasi seperti kasus EFAIL penyalahgunaan oleh pihak kriminal, manajemen kunci yang kompleks, dan ancaman masa depan dari komputasi kuantum. Hal ini menunjukkan bahwa enkripsi membutuhkan pengembangan berkelanjutan agar tetap adaptif terhadap ancaman siber yang terus berkembang. Dalam konteks Indonesia, penerapan enkripsi memiliki urgensi tinggi mengingat maraknya kebocoran data yang memengaruhi masyarakat. Implementasi enkripsi yang konsisten, mulai dari penggunaan SSL/TLS pada situs pemerintah, E2EE pada aplikasi komunikasi, hingga PGP/S/MIME pada layanan email instansi, merupakan langkah penting untuk memperkuat keamanan nasional dan membangun kepercayaan publik terhadap layanan digital.

Secara keseluruhan, enkripsi bukan hanya teknologi pendukung, tetapi elemen krusial dalam menciptakan komunikasi digital yang aman, terlindungi, dan terpercaya, sekaligus menjadi fondasi penting bagi penguatan keamanan informasi di Indonesia. Melalui pemahaman tentang berbagai bentuk enkripsi, protokol keamanan, serta tantangan yang mengiringinya, penelitian ini diharapkan dapat menjadi landasan bagi pengembangan sistem komunikasi yang lebih aman dan andal.

DAFTAR PUSTAKA

Abidde, W N, et al. “CIA TRIAD: A REVIEW OF THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF DATA IN A SYSTEM OF CONNECTED NETWORKS.” *Www.Irjmets.Com @International Research Journal of Modernization in Engineering*, vol. 7, no. 3, Mar. 2025, https://doi.org/10.56726/IRJMETS68704.

AhmadZadeh Raji, Mehrdad, et al. “A New Secure Email Scheme Using Digital Signature with S/MIME.” *International Journal of Computer Networks and Communications Security*, vol. 4, no. 3, Mar. 2016, pp. 56–62, www.ijcncs.org.

Alamsyah. *IMPLEMENTASI KEAMANAN E-MAIL DENGAN MENGGUNAKAN PGPTRAY*. Almadira,

Alisa, et al. "MELINDUNGI DATA DI DUNIA DIGITAL: PERAN SRTATEGIS ENKRIPSI DALAM KEAMANAN DATA." *Journal of Scientech Research and Development*, vol. 6, no. 2, 2024, https://idm.or.id/JSCR/index.php/JSCR.

Arif, Zaenul, and Akhmad Nurokhman. "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi." *JTSI*, vol. 4, no. 2, Oct. 2023, pp. 394–405.

Bagies, Taghreed. "Classifying Software Security Requirements into Confidentiality, Integrity, and Availability Using Machine Learning Approaches." *PeerJ Computer Science*, vol. 10, Nov. 2024, pp. 1–20, https://doi.org/10.7717/peerj-cs.2554.

Basri. "KRIPTOGRAFI SIMETRIS DAN ASIMETRIS DALAM PERSPEKTIF KEAMANAN DATA DAN KOMPLEKSITAS KOMPUTASI." *Jurnal Ilmiah Ilmu Komputer*, vol. 2, Sept. 2016, http://ejournal.fikom-unasman.ac.id.

Clarita Tiara Tunas Totnay, Euis, et al. "Enkripsi End-to-End Pada Aplikasi WhatsApp Menggunakan Metode AES-256." *Blantika: Multidisciplinary Jornal*, vol. 3, pp. 2025–2025, https://blantika.publikasiku.id/.

Cyberhub.id. (n.d.). *Manfaat enkripsi data*. Cyberhub.id. https://cyberhub.id/pengetahuan-dasar/manfaat-enkripsi-data

Davis Don. *Defective Sign & Encryptin S/MIME PKCS#7, MOSS, PEM, PGP, and XML*. 2001.

Dicoding. (n.d.). *Enkripsi untuk keamanan data*. Dicoding.com. https://www.dicoding.com/blog/enkripsi-untuk-keamanan-data/

Dechand, Sergej, et al. *In Encryption We Don't Trust: The Effect of End-To-End Encryption to the Masses on User Perception*.

Dharmawan, Nathanael, et al. "ANALISIS KEAMANAN JARINGAN UNIVERSITAS KRISTEN DUTA WACANA DENGAN SERANGAN SSL/TLS." *Jurnal Terapan Teknologi Informasi*, vol. 6, no. 2, Oct. 2022, pp. 121–30, https://doi.org/10.21460/jutei.2022.62.214.

Diaz Ramiro Daniel and B.S.E. *S/MIME Client with Wireless Key Passing for Android*. Dec. 2015.

Diniyatullah, Ledi, and Kurniati Bunga Rindu. "Crisis Management and Recovery Strategies After a Data Leak: Equifax Case Study." *JOISTECH: Journal of Information System and Technology*, vol. 01, Dec. 2024, pp. 76–81.

Dobeš, Zdeněk. *S/MIME Email Security in Roundcube*. http://excel.fit.vutbr.cz.

DTE, Telkom University. (n.d.). *Enkripsi: Menjaga keamanan data dalam dunia digital*. DTE Telkom University. https://dte.telkomuniversity.ac.id/enkripsi-menjaga-keamanan-data-dalam-dunia-digital/

Egitekno. (2025, Juli). *Penggunaan teknologi enkripsi dalam .....*Egitekno. https://www.egitekno.com/2025/07/penggunaan-teknologi-enkripsi-dalam.html

Fahim Zibran, Minhaz. *Cryptographic Security for Emails: A Focus on S/MIME*.

Fahri, M, et al. "PEMANFAATAN ALGORITMA AES UNTUK KEAMANANN DATA KARYAWAN PT. TELKOM INDONESIA PEMATANGSIANTAR." *Jurnal Ilmiah Teknik Dan Ilmu Komputer*, vol. 1, no. 1, Feb. 2022, pp. 32–37.

Fahrudin, Azis, and Gufron Zaida Muflih. "ANALISIS FORENSIK DIGITAL PADA PESAN WHATSAPP YANG TERENKRIPSI DENGAN PRETTY GOOD PRIVACY (PGP) MENGGUNAKAN FRAMEWORK DFRWS." *Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 1, Feb. 2025.

Fatima, Sana, et al. "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing †." *Engineering Proceedings*, vol. 20, no. 1, July 2022, https://doi.org/10.3390/engproc2022020014.

Ferdiansyah, Salsabila, et al. *Media Hukum Indonesia (MHI) Published by Yayasan Daarul Huda Krueng Mane Peran OJK Dalam Perlindungan Konsumen Terhadap Kebocoran Data Pada Konsumen Jasa Keuangan Indonesia*. vol. 2, no. 3, Oct. 2024, pp. 301–301, https://doi.org/10.5281/zenodo.11737122.

Fry Ann, et al. *Not Sealed But Delivered: The (Un)Usability of S/MIME Today*. www.issnet.ca.

Ganesh, Rahoul, et al. "A Panoramic Survey of the Advanced Encryption Standard: From Architecture to Security Analysis, Key Management, Real-World Applications, and Post-Quantum Challenges." *International Journal of Information Security*, vol. 24, no. 5, Oct. 2025, https://doi.org/10.1007/s10207-025-01116-x.

Garfinkel, Simson L, and Robert C Miller. *Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express*. 2005.

Goyal, Prachi, et al. "The Importance of Data Encryption in Data Security." *Journal of Nonlinear Analysis and Optimization*, vol. 13, no. 01, 2022, pp. 01–11, https://doi.org/10.36893/jnao.2022.v13i02.001-011.

Hale, Britta, and Chelsea Komlo. *On End-to-End Encryption*.

Hasibuan, Mega, et al. "Perlindungan Privasi Konsumen Dalam Penggunaan Big Data Di Ekonomi Digital." *Jurnal Ekonomi Dan Bisnis*, vol. 2, no. 2, June 2023, http://jurnal.jomparnd.com/index.php/jk.

IDN.id. (n.d.). *Pentingnya enkripsi dalam dunia digital*. IDN.id. https://www.idn.id/pentingnya-enkripsi-dalam-dunia-digital/

Indra, Dedek, et al. *PERBANDINGAN ALGORITMA KRIPTOGRAFI SIMETRIS DAN ASIMETRIS*. vol. 8, June 2023, https://fe.ekasakti.org/index.php/UJIS.

Jain, Priyank, et al. "Big Data Privacy: A Technological Perspective and Review." *Journal of Big Data*, vol. 3, no. 1, Dec. 2016, https://doi.org/10.1186/s40537-016-0059-y.

Jeanita Sengkey, Dwi, et al. "Kemampuan Pemahaman Konsep Matematis: Sebuah Kajian Literatur." *Maret 2023 Journal of Mathematics Education and Application*, vol. 3, no. 1, Mar. 2023, pp. 67–67, https://mathjournal.unram.ac.id/index.php/Griya/indexGriya.

Jefry, Buala, et al. "PENYALAHGUNAAN DATA PRIBADI KONSUMEN OLEH PERUSAHAAN: KAJIAN YURIDIS DALAM PERSPEKTIF UU PERLINDUNGAN KONSUMEN DAN UU PERLINDUNGAN DATA PRIBADI." *Jurnal Pendidikan Indonesia*, vol. 6, no. 5, 2025, pp. 1–1.

Karier.mu. (n.d.). *Mengenal fungsi enkripsi dalam keamanan data*. Karier.mu. https://www.karier.mu/blog/umum/mengenal-fungsi-enkripsi-dalam-keamanan-data/

Kar, Jayaprakash, et al. "An Efficient and Lightweight Deniably Authenticated Encryption Scheme for E-Mail Security." *IEEE Access*, vol. 7, Dec. 2019, pp. 184207–20, https://doi.org/10.1109/ACCESS.2019.2960291.

Kshetri, Naresh, et al. *algoTRIC: Symmetric and Asymmetric Encryption Algorithms for Cryptography - A Comparative Analysis in AI Era*. Dec. 2024.

Matta, Priya, et al. "A Comparative Survey on Data Encryption Techniques: Big Data Perspective." vol. 46, 2021, pp. 11035–39, https://doi.org/10.1016/j.matpr.2021.02.153.

MSF, Telkom University. (n.d.). *Apa itu enkripsi? Rahasia di balik keamanan data digital*. MSF Telkom University. https://msf.telkomuniversity.ac.id/apa-itu-enkripsi-rahasia-di-balik-keamanan-data-digital/

Muttaqin, et al. *Pengantar Ilmu Kriptografi*. Edited by Matias Julyus Fika Sirait and S.Kom. Devy Dian Pratama, Yayasan Kita Menulis, 2024, https://www.researchgate.net/publication/385936425.

Poddebniak, Damian, et al. *Efail: Breaking S/MIME and OpenPGP Email Encryption Using*

Exfiltration Channels. 2018, https://www.usenix.org/conference/usenixsecurity18/presentation/poddebniak.

Primartha Rifkie. "Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)." *Jurnal Sistem Informasi (JSI)*, vol. 3, Oct. 2011, pp. 371–87, http://ejournal.unsri.ac.id/index.php/jsi/index.

Prof. Dr. Ir. Siti Herlinda, M.Si., et al. *Buku Metodologi Penelitian. Bekal Teori Dan Petunjuk Praktis Bagi Mahasiswa Dan Peneliti Dalam Perancangan Penelitian, Serta Penulisan Artikel Ilmiah Dengan Benar Sesuai Kaidah Ilmiah*. Lembaga Penelitian Universitas Sriwijaya, 2010.

R Ananda Aufa, et al. *ANALISA KEAMANAN PADA APLIKASI WHATSAPP MENGGUNAKAN ENKRIPSI END TO END*. 2024.

Rahmadi Putra and Yunita Hilda Dwi. *IMPLEMENTASI PENGAMANAN BASIS DATA DENGAN TEKNIK ENKRIPSI (Studi Kasus: PT. Sugar Group Companies)*.

RumahCoding.co.id. (n.d.). *Pentingnya enkripsi SSL/TLS dalam keamanan web: Panduan praktis*. RumahCoding.co.id. https://rumahcoding.co.id/pentingnya-enkripsi-ssl-tls-dalam-keamanan-web-panduan-praktis/

Reuter, Adrian, et al. "Usability of End-to-End Encryption in E-Mail Communication." *Frontiers in Big Data*, vol. 4, July 2021, https://doi.org/10.3389/fdata.2021.568284.

Saputra Dwi Fajar. "LITERASI DIGITAL UNTUK PERLINDUNGAN DATA PRIBADI." *Jurnal Ilmu Kepolisian*, vol. 17, Dec. 2023.

Sari Ayumi Kartika. "Kebijakan Hukum Perlindungan Konsumen Terhadap Kebocoran Data Di Platform Fintech." *Jurnal Hukum*, vol. 6, Nov. 2025, https://journal.cattleyadf.org/index.php/Judge/index.

Simplilearn. (n.d.). *Data encryption methods*. Simplilearn. https://www-simplilearn-com.translate.goog/data-encryption-methods-article?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc

Sutarman, Buku. *Pengantar Teknologi Informasi*. 2012. Jakarta: Bumi Aksara.

Syarifuddin Syahab, Alfin, and Erik Iman Heri Ujianto. *PENGGUNAAN WIRESHARK DAN NESSUS UNTUK ANALISIS SSL/TLS PADA KEAMANAN DATA PENGGUNA WEBSITE*. May 2023. JIKA.

Tanoto, Andri. *Analisis Keamanan Pada Pretty Good Privacy (PGP)*. http://www.pgp.org. Teltics.

(n.d.). *Enkripsi data: Menjaga keamanan informasi di era digital*. Teltics.com. https://teltics.com/blog/enkripsi-data-menjaga-keamanan-informasi-di-era-digital

Thomas, Jason. *A Case Study Analysis of the Equifax Data Breach 1 A Case Study Analysis of the Equifax Data Breach*. https://doi.org/10.13140/RG.2.2.16468.76161.

Toorpu Arvind Reddy. *End-to-End Zero-Trust in Database Migration Frameworks: A Comprehensive Review*.

Ujung Adelia Marwah, et al. *PERANAN SISTEM INFORMASI MANAJEMEN DALAM MENINGKATKAN KUALITAS PENDIDIKAN*. vol. 2, Feb. 2023.