Vol. 5 No. 2 Desember 2024 Hal : 335 - 355

E-ISSN: 2723-1089
P-ISSN: 2776-7779

Tinjauan Terhadap Implementasi Advanced Encryption Standard 256 Dalam Keamanan Data

Jessa Syah Putra[1)], Rian Ardianto [2)],Purwono [3)]

[1)]Prodi Jurusan Teknologi Informasi, Fakultas Sains dan Teknologi,
Universitas Harapan Bangsa
[2,3)] Prodi Informatika, Fakultas Sains dan Teknologi,
Universitas Harapan Bangsa
Coresponding Email:jessasyah72@gmail.com

Abstrak

Penelitian ini membahas bagaimana algoritma Advanced Encryption Standard (AES) 256 dapat digunakan untuk melindungi data. Keamanan data menjadi semakin penting untuk mencegah penyalahgunaan dan pencurian data, terutama dalam komunikasi digital dan penyimpanan data sensitif, berkat kemajuan teknologi informasi. Metode penelitian yang digunakan adalah penelitian literatur dengan mengacu pada berbagai literatur dan jurnal yang relevan. Hasil penelitian menunjukkan bahwa algoritma enkripsi simetris AES-256 dapat dengan efektif mendekripsi dan mengenkripsi data sambil memastikan kerahasiaan, integritas, dan keaslian data. Selain itu, studi kasus dilakukan pada aplikasi WhatsApp yang menggunakan enkripsi end-to-end untuk menunjukkan bagaimana AES-256 melindungi komunikasi pengguna.

Kata Kunci: AES 256; Enkripsi; Deskripsi; End-to-End Enkripsi; WhatsApp.

Abstract

This study discusses how the Advanced Encryption Standard (AES) 256 algorithm can be used to protect data. Data security is becoming increasingly important to prevent data abuse and theft, especially in digital communications and sensitive data storage, thanks to advances in information technology. The research method used is literary research with reference to various relevant literature and journals. The results show that the AES-256 symmetrical encryption algorithm can effectively decrypt and encrypt data while ensuring the confidentiality, integrity, and authenticity of data. In addition, a case study was conducted on a WhatsApp app that uses end-toend encryption to show how AES-256 protects user communications.

Keywords: AES 256; Encryption; Descriptions; End-to-End Encryptions; WhatsApp.

PENDAHULUAN

Perkembangan ini mengubah cara masyarakat berinteraksi satu sama lain banyak tugas dapat diselesaikan dengan cepat, akurat, dan efisien berkat kemajuan pesat dalam teknologi komputer dan telekomunikasi kontemporer.. Di masa lalu, cara konvensional untuk berkomunikasi jarak jauh seperti pengiriman surat digunakan. Namun, sekarang ada teknologi seperti internet, email, dan SMS (Short

Messaging Service), yang membuat komunikasi lebih mudah dan cepat. Selain itu, teknologi modern seperti aplikasi pesan instan, panggilan video, dan media sosial telah mempercepat pertukaran informasi, dan memperkuat hubungan sosial dan profesional di seluruh dunia. [1] melihat masa depan kemajuan teknologi komputer dan telekomunikasi, kita membutuhkan pemahaman yang lebih baik tentang kemajuan teknologi informasi saat ini. Kemampuan sebuah lembaga atau organisasi untuk menyediakan informasi yang cepat dan akurat kepada semua orang sangat penting bagi bisnis, perguruan tinggi, pemerintah (birokrasi), dan individu (swasta). Mengingat kecanggihan teknologi transmisi data dan penerapannya, serta kurangnya pengetahuan tentang keamanan data merupakan sebuah ancaman besar.Teknologi keamanan informasi membutuhkan sistem enkripsi untuk mencegah penyalahgunaan data. [2]

Latar Belakang masalah yaitu Semakin besar tingkatan teknologi komputer, maka semakin besar juga tingkat risiko yang mengancam keamanan data didalam komputer.[3] Salah satu upaya untuk mrlindungi file dengan menggunakan metode kriptografi, yang sudah banyak dipelajari dalam berbagai penelitian.[4]

Dengan pesatnya kemajuan teknologi dan banyaknya digitalisasi yang terjadi di berbagai bidang kehidupan manusia, penting untuk memastikan bahwa privasi dan keamanan data tetap terjaga.[5] Pencurian data saat ini sering ditemukan pada platform media sosial seperti Instagram, Facebook, WhatsApp, dan lainnya. Pengguna harus lebih berhati-hati saat menggunakan media media yang menyimpan data sensitif seperti data diri, foto, atau jenis data lainnya yang berkaitan dengan pribadi. Oleh karena itu, keamanan data sangat penting saat ini. Pengembangan pengamanan yang ketat terus dikembangkan untuk mencegah data pribadi bocor.[6] Melindungi kerahasiaan file di komputer sangat penting untuk mencegah perusakan, pencurian, atau penyalahgunaan data oleh pihak yang tidak berwenang melalui jaringan komputer.[1] Penelitian ini bertujuan untuk mempelajari dan menganalisis penggunaan Advanced Encryption Standard (AES-

256) dalam hal keamanan data. Penelitian ini secara khusus berkonsentrasi Selama proses enkripsi dan dekripsi algoritma AES-256 digunakan.

METODE PENELITIAN

Penulis menggunakan referensi dari berbagai jurnal yang berfokus pada penggunaan Advanced Encryption Standard (AES) 256. Selain itu, penelitian ini melakukan analisis menyeluruh terhadap teknik yang akan digunakan, serta analisis berbagai sumber data, termasuk buku, jurnal, dan karya ilmiah lainnya yang terkait dengan topik utama penelitian. Penelitian ini berfokus pada kriptografi, terutama algoritma AES-256, yang sangat aman. Tujuannya adalah untuk memberi penulis dasar yang kuat dan akurat untuk memilih metode AES-256 terbaik.

STUDI PUSTAKA dan PENELITIAN TERDAHULU

Tabel 1 : Review dari beberapa refrensi jurnal

NO	Judul Penelitian	Penulis	kelebihan	Kekurangan	Kesimpulan
1	Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy [7]	Berita Estu Widodo, Sidiq Purnomo	Kecepatan proses enkripsi dan dekripsi yang tinggi, terutama untuk file berukuran besar, menunjukkan efisiensi algoritma AES dalam aplikasi nyata. Ini sangat menguntungkan dalam situasi di mana pemrosesan data harus dilakukan dengan cepat. Algoritma AES meningkatkan keamanan secara signifikan, terutama dalam melindungi source code dan file dokumen. Ini menjadi pilihan yang tepat sebagai pencegahan akses tidak sah ke data penting. Aplikasi kriptografi	Meskipun algoritma AES efisien, implementasinya dapat menjadi kompleks dan memerlukan pengetahuan teknis yang mendalam. Ini bisa menjadi tantangan bagi para user yang memiliki latar belakang teknis yang lemah. Meskipun prosesnya cepat, waktu enkripsi dan dekripsi dapat meningkat secara signifikan dengan bertambahnya ukuran file. Hal ini mungkin menjadi batasan dalam beberapa kasus, terutama ketika berhadapan dengan data	Penelitian ini menunjukkan bahwa implementasi algoritma Advanced Encryption Standard (AES) efektif dalam meningkatkan keamanan data dan informasi, terutama dalam konteks enkripsi dan dekripsi file dokumen. Proses yang cepat dan efisien, serta fleksibilitas penggunaan, menjadikan AES sebagai solusi yang kuat untuk berbagai kebutuhan kriptografi. Namun, kompleksitas implementasi dan ketergantungan pada manajemen kunci yang baik harus diperhatikan untuk

E-ISSN: 2723-1089
P-ISSN: 2776-7779

					memastikan keamanan data yang optimal.

			berbasis AES dapat digunakan baik secara online maupun offline, memberikan fleksibilitas kepada pengguna dalam berbagai situasi, memungkinkan pengguna mengamankan data tanpa terbatas dengan koneksi internet.	dalam jumlah besar. Keamanan data sangat tergantung pada manajemen kunci enkripsi yang efektif. Jika kunci bocor atau hilang, data tetap berisiko. Oleh karena itu, manajemen kunci yang baik sangat penting untuk memastikan keamanan yang optimal.	

2	Penerapan Algoritma Aes-128 Untuk Pengamanan File Pada Smk Pgri 31 Legok[8]	Kaliyana Tantri Rukmana, Pipin Farida Ariyani	Kelebihan aplikasi ini adalah kemampuan untuk mengenkripsi dan mendekripsi berbagai jenis file dokumen dengan cepat dan efisien. Proses enkripsi meningkatkan ukuran file sekitar 25%, yang masih dalam batas wajar dan tidak mengganggu integritas file asli. Selain itu, fitur notifikasi aplikasi ini sangat ramah pengguna. Fiturfitur ini membantu pengguna memasukkan password dan file yang tepat dan memungkinkan pengguna berbagi file terenkripsi dengan pengguna lain.	Meskipun aplikasi ini memiliki banyak kelebihan, ada beberapa kekurangan. Jenis file tertentu seperti Word, Excel, dan PDF hanya dapat dienkripsi oleh aplikasi ini, tetapi file jenis lain seperti gambar tidak dapat. Selain itu, ada batasan ukuran file yang dapat dienkripsi, yaitu hingga 3 MB, yang mungkin menjadi kendala bagi pengguna yang perlu mengamankan file dengan ukuran lebih besar. Waktu enkripsi dan dekripsi juga bervariasi tergantung pada ukuran file, yang bisa menjadi masalah untuk	Secara keseluruhan, aplikasi pengaman file merupakan cara yang efektif dan efisien untuk mengamankan file dokumen dengan enkripsi. Hasil pengujian menunjukkan bahwa aplikasi ini dapat mengenkripsi dan mendekripsi file dengan cepat serta mengembalikan ukuran file ke kondisi semula setelah dekripsi. Kelebihan utama aplikasi ini adalah kemudahan penggunaan dan kemampuan untuk mengelola file terenkripsi. Namun, perlu diperhatikan bahwa aplikasi ini memiliki keterbat. Namun, aplikasi ini tetap menjadi alat yang bermanfaat untuk meningkatkan

			Hal ini membuatnya lebih aman dan mudah digunakan dalam kehidupan sehari-hari.	file yang sangat besar.	perlindungan data pengguna.
3	Implementasi Metode Advanced Encryption Standard (Aes) Dan Message Digest 5 (Md5) Pada Enkripsi Dokumen (Studi Kasus Lpse Unib)[9]	Gilang Gumira P.U.K. , Ernawati , Aan Erlanshari.	Keunggulan dari penelitian ini adalah kemampuan algoritma AES dengan panjang kunci 256 bit untuk mengenkripsi isi file secara efektif, yang memungkinkan pengaman file. Penggunaan algoritma MD5 sebagai penghasil nilai hash membuat proses enkripsi dan dekripsi dokumen lebih sulit, terutama jika sandi yang digunakan rumit. Aplikasi yang dibuat menggunakan UML dan dibangun dengan Adobe Dreamweaver CS6 menunjukkan kinerja yang baik dalam mencegah dokumen penting dari akses publik	Kerugian dari penelitian ini adalah ukuran file yang dihasilkan dari enkripsi menjadi dua kali lipat atau lebih besar dari ukuran file asli; hal ini dapat menyebabkan masalah dalam penyimpanan dan pengiriman file. Administrator juga dapat mendekripsi dokumen dan aplikasi tanpa harus memasukkan password yang sesuai dengan kunci dokumen. Karena semua data dokumen dapat diambil dengan mudah tanpa mencari kunci yang tepat, ini meningkatkan kemungkinan bobol akun admin.	Studi ini menunjukkan bahwa menggabungkan algoritma AES dan MD5 menjamin keamanan dokumen berbasis web. Hasil enkripsi melindungi data dengan baik, meskipun ukuran file hasilnya lebih besar. Namun demikian, perlu ada peningkatan dalam manajemen kunci dokumen untuk mengurangi kemungkinan bobol akun admin. Studi lebih lanjut disarankan untuk menyelesaikan masalah manajemen kunci dokumen yang lebih efisien bagi admin dan pengguna.

			yang tidak diinginkan.		
4	Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper	Achmad Nugrahantoro1 , Abdul Fadlil2 , Imam Riadi3	Kelebihan dari penelitian ini adalah metodologinya yang jelas, hasil uji yang menyeluruh dengan kecepatan ratarata yang baik	Pengaruh lalu lintas jaringan yang signifikan terhadap waktu eksekusi, risiko penggunaan simbol dan angka yang perlu	Kesimpulannya, algoritma modifikasi AES mode CBC ini menunjukkan kinerja yang baik dalam hal kecepatan dan ketahanan terhadap serangan melalui

				diwaspadai, dan perlunya	
	Block Chaining (CBC) [10]		pada berbagai ukuran blok, dan aplikasinya yang praktis pada sistem web dan mobile, yang menunjukkan kegunaan dan fleksibilitasnya dalam proses login dan pembuatan API.	pengujian tambahan dengan karakter yang lebih panjang untuk gambaran kinerja yang lebih akurat adalah kekurangan dari penelitian ini.	pembacaan karakter. Ini juga memiliki kemampuan untuk memberikan lapisan keamanan tambahan yang efektif untuk menjaga keabsahan data pada sistem web dan perangkat seluler. Namun, diperlukan pengujian lebih lanjut dengan skenario yang lebih kompleks dan mempertimbangkan variabel-variabel jaringan yang dapat mempengaruhi kinerja algoritma.

5.	Analisis Penggunaan Enkripsi End To End Pada Aplikasi Whatsapp Messengger[11]	Gellysa Urva	Studi ini menemukan bahwa algoritma Curve25519, yang digunakan dalam WhatsApp Messenger untuk enkripsi end-toend, memiliki beberapa keuntungan. Algoritma ini menunjukkan kecepatan yang sangat tinggi (Extremely High Speed) pada beberapa PC. Selain itu, Curve25519 tidak terpengaruh oleh serangan timing, serangan hyperthreading, dan serangan cache timing (No Time Variability). Penggunaan kunci publik dan rahasia yang pendek—masing-masing sebesar 32 byte—dan kunci	Namun, penelitian ini memiliki kekurangan. Meskipun algoritma Curve25519 sangat cepat dan efektif, penyerang sering menggunakanny a di sistem keamanan seperti WhatsApp Messenger. Selain itu, bagi pengembang aplikasi yang kurang berpengalaman, kompleksitas teknis algoritma ini mungkin menghalangi mereka untuk menerapkan kriptografi tingkat lanjut. Selain itu, penelitian ini tidak memeriksa kelemahan tambahan yang mungkin muncul dari menggabungkan	Secara keseluruhan, penelitian ini menemukan bahwa algoritma Curve25519 cocok untuk sistem enkripsi end-to-end seperti WhatsApp Messenger. Curve25519 adalah pilihan yang bagus untuk menyimpan data komunikasi karena cepat dan tahan terhadap banyak serangan. Namun, perlu diperhatikan bahwa penggunaan algoritma harus dilakukan dengan hati-hati untuk mencegah penyerang yang semakin mahir menggunakan kelemahan keamanan.

			rahasia membuatnya efektif dalam penggunaan memori dan kecepatan proses enkripsi.	Curve25519 dengan algoritma lain atau dalam berbagai situasi serangan dunia nyata.	

HASIL DAN PEMBAHASAN

Kriptografi adalah bahasa dan teknik untuk menyandi dan menyembunyikan informasi untuk menjaga kerahasiaan, keautentikan, integritas, dan keabsahan data saat dikirim atau disimpan dalam sistem komunikasi atau penyimpanan. Cryptography berfungsi untuk menjaga kerahasiaan pesan dari orang lain dengan mengubah pesan asli menjadi bentuk yang tidak dapat dipahami tanpa pengetahuan kunci atau algoritma khusus . Selain itu, Cryptography juga bertujuan untuk memastikan bahwa pesan tidak diubah oleh pihak yang tidak berwenang selama transmisi dan untuk memverifikasi identitas pengirim dan penerima pesan untuk memastikan bahwa komunikasi dilakukan dengan aman. Dalam era digital saat ini, Cryptography sangat penting untuk melindungi informasi di berbagai platform, seperti komunikasi online, sistem keuangan, dan pengelolaan data pribadi. Teknik Kriptografi terus berkembang untuk mengatasi masalah keamanan yang semakin kompleks dan meningkatkan standar keamanan dalam pertukaran dan penyimpanan data sensitif.[7] Teknik kriptografi seperti Caesar Cipher, Affine, Monoalphabetic, Polyalphabetic, Vigenere, dan Transposition dapat digunakan untuk mengenkripsi pesan atau informasi yang ingin disembunyikan.[6]

Bahasa Yunani "crypto" berarti rahasia dan "graphia" berarti menulis (teks). Kriptografi adalah bidang studi tentang cara menyembunyikan pesan. Kriptografi digunakan dalam aplikasinya untuk mengenkripsi atau menyandi data sehingga

hanya dapat dibaca oleh pihak yang berwenang atau pengguna tertentu yang relevan.[7]

Gambar 1 Ilustrasi penerapan algoritma kriptografi pada sistem

Gambar 1 di atas menunjukkan bagaimana algoritma kriptografi digunakan. Data pesanan dienkripsi, dan kemudian disimpan ke database sebagai chipertext, atau data yang sudah tersandi.

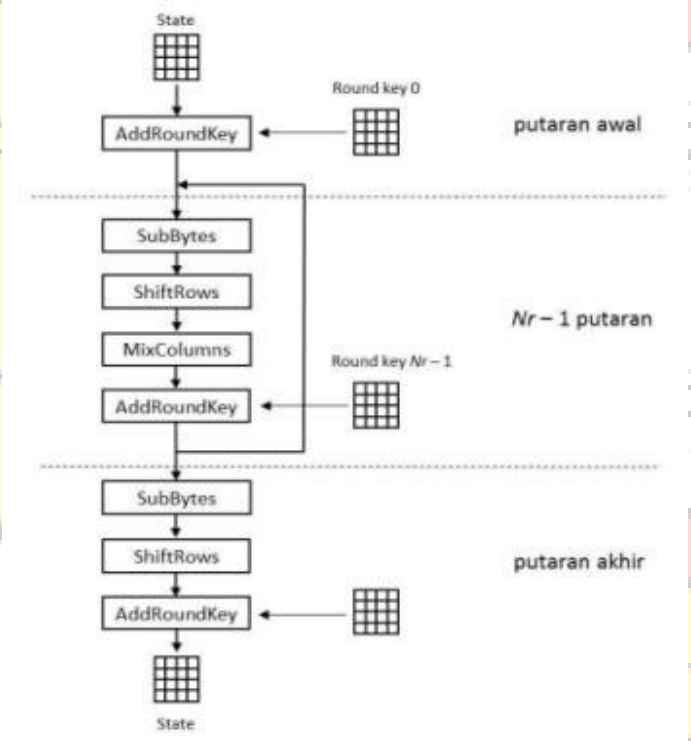
- Advanced Encryption Standard (AES)

  Advanced Encryption Standard (AES) diciptakan pada tahun 2001 oleh NIST (National Institute of Standards and Technology) sebagai pengembangan dari algoritma enkripsi DES tradisional yang menggunakan prosedur berulang yang disebut ronde. Digunakan untuk melindungi data atau informasi rahasia dengan menggunakan kunci simetris selama proses enkripsi dan dekripsi (NIST, 2001).[8][12] Panjang kunci yang digunakan menentukan jumlah putaran (rounds) yang digunakan dalam AES. NIST (National Institute of Standards and Technology) menetapkan algoritma AES sebagai standar enkripsi federal AS karena kinerjanya. Tiga versi panjang kunci AES: 128 bit, 192 bit, dan 256 bit. [13][14][15]

  Algoritma ini menggunakan fungsi permutasi dan substitusi. Metode enkripsi AES 128, AES 192, dan AES 256 hampir sama, kecuali bahwa AES 256 melakukan 14 permutasi per round. Metode algoritma Advanced Encryption Standard (AES) yang sudah digunakan dapat mengurangi risiko kejahatan keamanan data karena pesan atau file dan dokumen terlindungi.[16]

- Proses Enskripsi

Enkripsi adalah proses mengacak data atau informasi dalam aplikasi dengan menggunakan algoritma enkripsi AES 256 yang digunakan dengan satu kunci[3]. Empat jenis transformasi byte digunakan dalam proses ini: SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Pada tahap pertama, input diubah menjadi byte AddRoundKey. Kemudian state mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey selama jumlah Nr putaran. Dalam algoritma AES, rangkaian ini disebut sebagai "fungsi putaran", dengan putaran terakhir memiliki fitur yang berbeda dari putaran pertama. Namun, dalam proses dekripsi, algoritma AES menggunakan transformasi invers untuk setiap transformasi dasarnya.[17].

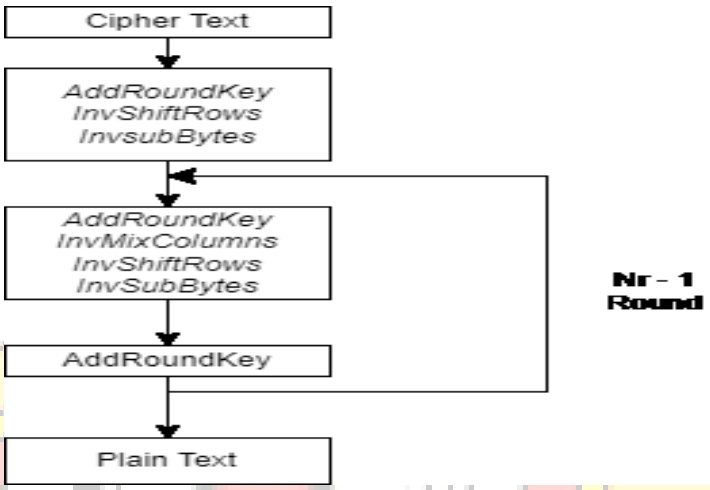


Gambar 3 Proses Enskripsi

- Proses Deskripsi

Dalam proses dekripsi, algoritma simetris AES 256 mengubah data acak (cipher) yang telah dienkripsi menjadi data asli (plain). Untuk membuat cipher invers yang sesuai dengan algoritma AES, transformasi cipher dapat dibalik dan diterapkan dalam berbagai urutan selama fase dekripsi. Cipher

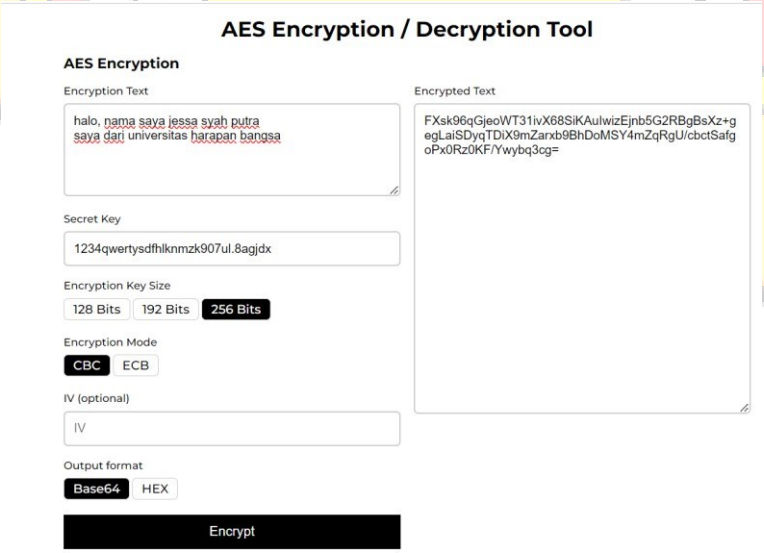
invers dapat mengembalikan byte ke bentuk aslinya dengan menggunakan transformasi InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey [15].



Gambar 4 Proses Deskripsi

- Proses Enskripsi dan Deskripsi pada AES 256
  - Proses Enskripsi AES 256

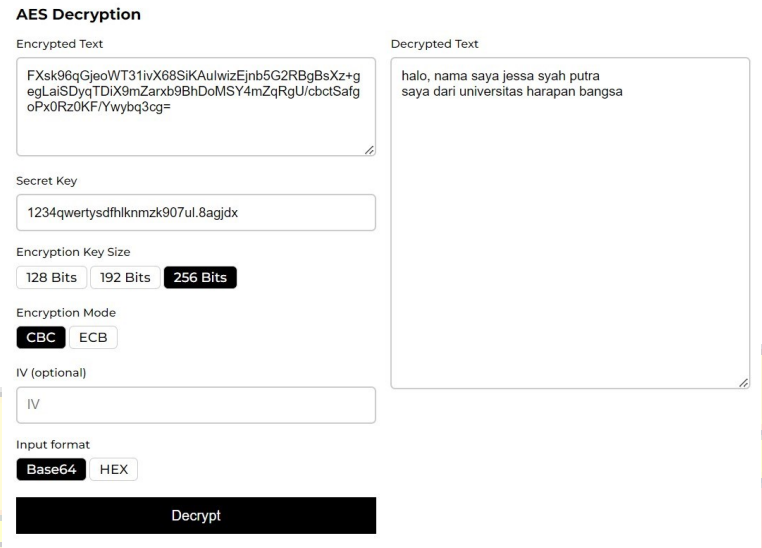
    Enkripsi AES-256 melindungi pesan atau data rahasia dari orang yang tidak dapat melihatnya.



Gambar 5 ilustrasi proses enskripsi AES 256

➢ Proses Deskripsi AES 256

Proses dekripsi pada AES-256 melibatkan beberapa langkah yang memungkinkan mengubah teks terenkripsi (ciphertext) kembali menjadi teks asli (plaintext).



Gambar 6 ilustrasi proses deskripsi AES 256

- Studi Kasus pada WhatsApp

WhatsApp Messenger adalah aplikasi pesan lintas platform yang dikembangkan oleh WhatsApp Inc. yang memungkinkan pengguna untuk bertukar pesan tanpa membayar SMS. Aplikasi ini didirikan pada tahun 2009 oleh Brian Acton dan Jan Koum. Kedua orang tersebut juga adalah karyawan senior yang pernah bekerja di Yahoo.Inspirasi awal untuk WhatsApp datang dari Jan Koum, yang ingin membuat aplikasi yang memungkinkan pengguna memposting status meskipun sedang sulit dihubungi. Sejak diluncurkan, WhatsApp telah berkembang menjadi salah satu platform komunikasi terpopuler di dunia, menawarkan berbagai fitur seperti pesan teks, panggilan suara dan video, serta berbagi media dan dokumen, yang memudahkan komunikasi global secara instan dan efisien. [18]

Salah satu fitur keamanan yang digunakan oleh aplikasi WhatsApp Messenger adalah fitur enkripsi end-to-end, juga dikenal sebagai enkripsi end-to-end. Pada dasarnya, enkripsi end-to-end adalah jenis enkripsi yang ada di sistem

komunikasi, yang berarti bahwa pesan dienkripsi sebelum dikirim oleh pengirim dan kemudian didekripsi hanya pada tujuan akhir atau penerima pesan[19] Beberapa aplikasi pesan populer telah mengadopsi enkripsi end-to-end dalam beberapa tahun terakhir, baik secara default atau sebagai fitur opsional. Akibatnya, E2EE sekarang tersedia dan digunakan oleh jutaan, jika tidak miliaran, pengguna setelah beberapa dekade hanya digunakan dalam komunitas dan aplikasi khusus.[20]

Fitur keamanan end-to-end encryption memiliki keistimewaan hanya orang yang mengirim dan menerima pesan yang dapat membaca chat. File yang dapat dibaca termasuk teks, gambar gif/JPEG, dokumen pdf/.doc, suara/musik, video, dan format lainnya. . Karena server tidak memiliki kunci penyulitan, pesan yang akan dikirim pengguna juga tidak dapat dibaca oleh server. end to end encryption, bekerja secara otomatis, tanpa mengaktifkan pengaturan tertentu.[16] Hanya orang yang mengirim dan yang menerima pesan yang dapat mengetahui pesan saat menggunakan metode ini. Berikut adalah contoh penggunaan end-to-end encryption.

Gambar 7 Penggunaan end-to-end encryption

Gambar berikut menunjukkan pengiriman pesan yang tidak dilindungi end-to-end encryption. Ini menunjukkan perbedaan antara pengiriman pesan yang dilindungi end-to-end encryption dan pengiriman pesan yang digunakan secara umum.

Gambar 8 Penggunaan tanpa end-to-end encryption

Gambar 7 dan 8 menunjukkan perbedaan bagaimana menggunakan end-to-end encryption. Pada gambar 7 dan 8, pesan yang dikirim dari client ke server dienkripsi, sehingga server tidak dapat mengetahui pesan asli dan tidak dapat mendekripsinya karena tidak memiliki kunci untuk mendekripsinya. Sebaliknya, gambar 8 menunjukkan penggunaan end-to-end encryption, sehingga pesan yang dikirim merupakan pesan yang sudah dienkripsi.

Contoh pengimplementasian end-to-end encryption

Gambar diatas adalah contoh jelasnya dari pengimplementasian pengiriman pesan tanpa end-to-end encryption.

Gambar diatas adalah contoh jelasnya dari pengimplementasian pengiriman pesan menggunakan end-toend encryption.

SIMPULAN

Algoritma Advanced Encryption Standard (AES) 256 adalah alat yang sangat baik untuk melindungi data saat disimpan dan dikomunikasikan secara digital. Penelitian ini menegaskan bahwa keamanan data sangat penting untuk mencegah penyalahgunaan dan pencurian data, yang semakin relevan dengan kemajuan teknologi informasi. Dengan menggunakan metode penelitian literatur yang merujuk pada berbagai sumber yang relevan, terbukti bahwa AES-256 dapat dengan mudah mendekripsi dan mengenkripsi data, memastikan kerahasiaan, integritas, dan keaslian data. Studi kasus yang dilakukan pada aplikasi WhatsApp yang menggunakan enkripsi end-to-end menunjukkan bagaimana AES-256 benar-benar melindungi komunikasi pengguna, peran penting algoritma ini dalam keamanan digital kontemporer.

DAFTAR PUSTAKA

Abadi Pamungkas, A. and Susilo Yuda Irawan, A. (2023) 'Analisis Penerapan Algoritma Kriptografi Rivest-Shamir-Adleman (RSA) dan Zero-Knowledge Proof Pada Aplikasi Whatsapp Mod', in *Jurnal Ilmiah Wahana Pendidikan, Juli*, pp. 81–95. Available at: https://doi.org/10.5281/zenodo.8145614.

Andriyanto, M.R. and Sukmasetya, P. (2022) 'Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace', in *Journal of Computer System and Informatics (JoSYC)*. Forum Kerjasama Pendidikan Tinggi (FKPT), pp. 179–187. Available at: https://doi.org/10.47065/josyc.v4i1.2451.

Bai, W. *et al.* (2020) 'Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study', in *Proceedings - 5th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2020*, pp. 210–219. Available at:

https://doi.org/10.1109/EuroSPW51379.2020.00036.

CANDRA, N. (2021) 'IMPLEMENTASI ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY (ECC) DENGAN END-TO-END ENCRYPTION PADA APLIKASI CHAT BERBASIS MOBILE', in *Stikespanakkukang.Ac.Id*. Available at: https://stikespanakkukang.ac.id/assets/uploads/alumni/8a827536b6809e5871a87340e2594ad8.pdf.

Febrianto, R. and Waluyo, S. (2023) 'IMPLEMENTASI ALGORITME KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-256) UNTUK MENGAMANKAN DATABASE PENILAIAN KARYAWAN PADA KJPP NDR', in, pp. 44–49.

Gumira PUK, G. and Erlanshari, A. (2016) 'IMPLEMENTASI METODE ADVANCED ENCRYPTION STANDARD (AES) DAN MESSAGE DIGEST 5 (MD5) PADA ENKRIPSI DOKUMEN (STUDI KASUS LPSE UNIB)', in *Jurnal Rekursif*.

Hulu, D., Nadeak, B. and Aripin, S. (2020) 'Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan', in. Available at: https://doi.org/10.30865/komik.v4i1.2590.

Khasanah, S. and Sutabri, T. (2023) 'Analisis Pencegahan Pencurian Data Melalui Aplikasi Whatsapp Menggunakan Metode Kriptografi', in *Jurnal Sain dan Teknik*, pp. 145–153.

Liander, G. V (2022) 'Penggunaan Algoritma Elliptic Curve Diffie Hellman dan AES 256 pada Implementasi End-to-End Encryption WhatsApp', in *Sumber*. Available at: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/Makalah2022/Makalah-II4031-Kripto-2022 (14).pdf.

Nugrahantoro, A., Fadlil, A. and Riadi, I. (2020) 'Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC)', in *Jurnal Ilmiah FIFO*. Universitas Mercu Buana, p. 12. Available at: https://doi.org/10.22441/fifo.2020.v12i1.002.

Permana, A.A. (2018) 'Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android', in *JURNAL Al-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, p. 110. Available at: https://doi.org/10.36722/sst.v4i3.280.

Prasetyo, A. and Pradana, R. (2023) 'Penerapan Algoritme Aes - 128 Untuk Pengamanan File Pada Smkn 1 Kota Tangerang Implementation of Aes-128 Algorithm for File Security At Smkn 1 Tangerang City', in *Senafti*, pp. 324–331.

Pratama, R.W. and Desyani, T. (2022) 'Analisa dan Implementasi Kriptografi File Dokumen Dengan Metode Algoritma Advanced Encryption Standard (AES) Berbasis Web', in *OKTAL: Jurnal Ilmu Komputer …*, pp. 758–762. Available at: https://journal.mediapublikasi.id/index.php/oktal/article/view/86%0Ahttps://journal.mediapublikasi.id/index.php/oktal/article/download/86/262.

Ribli, S. (no date) 'Analisis Keamanan Enkripsi End-to-end Aplikasi Whatsapp', in. Available at: https://budi.rahardjo.id/files/courses/2016/EL6115-2016-2.

Rukmana, K.T. and Ariyani, P.F. (2022) 'Penerapan Algoritma Aes-128 Untuk Pengamanan File Pada Smk Pgri 31 Legok', in *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)* , pp. 327–336.

Studi Informatika, P. and Tinggi Teknologi Dumai Jl Utama Karya Bukit Batrem Dumai, S.I. (no date) 'Gellysa Urva', in.

Widodo, B.E. and Purnomo, A.S. (2020) 'IMPLEMENTASI ADVANCED ENCRYPTION STANDARD PADA ENKRIPSI DAN DEKRIPSI DOKUMEN RAHASIA DITINTELKAM POLDA DIY', in *Jurnal Teknik Informatika (Jutif)*. Infinite Corporation, pp. 69–77. Available at: https://doi.org/10.20884/1.jutif.2020.1.2.21.

Wiharto, Y. and Irawan, A. (2018) 'ENKRIPSI DATA MENGGUNAKAN ADVANCED ENCRYPTION STANDARD 256', in.

Yuniati, V., Gani, I. and Rachmat, A. (no date) 'ENKRIPSI DAN DEKRIPSI DENGAN ALGORITMA AES 256 UNTUK SEMUA JENIS FILE', in.