Blantika: Multidisciplinary Jornal
Volume 3 Number 7, Juni, 2025
p- ISSN 2987-758X e-ISSN 2985-4199

Enkripsi End-to-End pada Aplikasi WhatsApp Menggunakan Metode AES-256

Euis Clarita Tiara Tunas Totnay, Maria Marsela Seran, Vallient Vandem Yaved Tusala, Silverius Triyanto Mau, Hermina Loka To
Universitas Timor, Indonesia
Email author: euisclrarita@gmail.com, mariamarselaseran03@gmail.com, vandemtusala01@gmail.com, antomau322@gmail.com, herminaloka079@gmail.com

ABSTRAK

Pesatnya perkembangan komunikasi digital menuntut sistem perlindungan data yang andal untuk menjaga privasi dan keamanan informasi. WhatsApp sebagai aplikasi pesan instan terpopuler telah mengimplementasikan sistem End-to-End Encryption (E2EE) menggunakan algoritma AES-256 dan ECDH Curve25519 dalam protokol Signal. Penelitian ini bertujuan untuk menganalisis secara mendalam arsitektur keamanan E2EE WhatsApp serta mengevaluasi efektivitas dan kelemahannya dalam menghadapi ancaman siber modern. Penelitian menggunakan pendekatan deskriptif kualitatif berbasis studi literatur, dengan mengkaji dokumentasi teknis, jurnal ilmiah, dan simulasi terbatas proses enkripsi-dekripsi. Hasil analisis menunjukkan bahwa WhatsApp berhasil menggabungkan kriptografi simetris dan asimetris melalui mekanisme pertukaran kunci (Identity Key, Signed Pre Key, One-Time Pre Key) serta algoritma Double Ratchet yang menghasilkan session key unik untuk setiap pesan. Sistem ini menjamin confidentiality, integrity, dan forward secrecy, di mana pesan tidak dapat dibaca pihak ketiga, bahkan oleh server WhatsApp sendiri. Namun, kelemahan masih ditemukan pada aspek endpoint security, pengelolaan metadata, dan cadangan data yang belum sepenuhnya terlindungi E2EE. Kesimpulannya, sistem E2EE pada WhatsApp merupakan model keamanan komunikasi digital yang kuat dan adaptif, namun masih memerlukan penguatan pada sisi pengguna dan kebijakan manajemen data. Penelitian ini diharapkan menjadi referensi dalam pengembangan sistem komunikasi yang lebih aman, transparan, dan berkeadilan di era digital.
Kata Kunci: Enkripsi end-to-end, WhatsApp, AES-256, Signal Protocol, ECDH, Kriptografi

ABSTRACT

The rapid advancement of digital communication demands reliable data protection systems to safeguard privacy and information security. WhatsApp, as the most widely used instant messaging application, has implemented an End-to-End Encryption (E2EE) system using AES-256 and ECDH Curve25519 algorithms within the Signal Protocol. This study aims to analyze the security architecture of WhatsApp's E2EE and evaluate its effectiveness and limitations in addressing modern cybersecurity threats. A descriptive qualitative approach was employed through a literature study, examining technical documentation, scientific journals, and limited encryption-decryption simulations. The analysis reveals that WhatsApp successfully integrates symmetric and asymmetric cryptography through a key exchange mechanism (Identity Key, Signed Pre Key, One-Time Pre Key) and the Double Ratchet Algorithm, which generates unique session keys for each message. This system ensures confidentiality, integrity, and forward secrecy, meaning that no third party; including WhatsApp servers—can read the message contents. However, vulnerabilities still exist in endpoint security, metadata management, and backup systems that are not fully protected by E2EE. In conclusion, WhatsApp's E2EE system is a robust and adaptive model for secure digital communication, though it still requires reinforcement in user-end protection and data management policies. This research is expected to serve as a reference for developing more secure, transparent, and equitable communication systems in the digital age.
Keywords: *End-to-end encryption, WhatsApp, AES-256, Signal Protocol, ECDH, Cryptography*

Manuscript accepted: 27-05-2025 Revised: 15-06-2025 Date of publication: 30-06-2025

PENDAHULUAN

Perkembangan teknologi komunikasi digital telah membawa perubahan besar dalam cara manusia berinteraksi dan bertukar informasi. Kemudahan akses internet, meluasnya penggunaan perangkat pintar, serta munculnya berbagai aplikasi pesan instan telah menjadikan komunikasi daring sebagai kebutuhan primer di era modern (Siregar & Sundari, 2016). WhatsApp, sebagai salah satu aplikasi pesan instan terbesar di dunia dengan lebih dari dua miliar pengguna aktif, memainkan peran sentral dalam transformasi ini.

Namun, seiring dengan meningkatnya intensitas pertukaran data melalui kanal digital, muncul pula ancaman-ancaman serius terhadap keamanan dan privasi informasi yang dikirimkan. Isu seperti penyadapan, pencurian identitas, manipulasi data, hingga penyalahgunaan informasi pribadi semakin menjadi perhatian utama, baik di kalangan pengguna individu maupun institusi. Oleh karena itu, dibutuhkan sistem perlindungan data yang tidak hanya andal secara teknis, tetapi juga tahan terhadap berbagai jenis serangan siber yang kompleks (Aska et al., 2024).

Sebagai respons terhadap tantangan tersebut, sejak tahun 2016 WhatsApp telah mengimplementasikan sistem End-to-End Encryption (E2EE) secara menyeluruh (Liander, 2022). Teknologi ini memastikan bahwa hanya pengirim dan penerima yang dapat membaca isi pesan, bahkan pihak WhatsApp sendiri tidak memiliki akses ke pesan tersebut. Dengan kata lain, server hanya bertindak sebagai perantara pengiriman data tanpa kemampuan untuk melakukan dekripsi, sehingga keamanan pesan tidak bergantung pada kepercayaan terhadap pihak penyedia layanan.

Implementasi sistem E2EE pada WhatsApp didasarkan pada kombinasi kriptografi kunci asimetris dan simetris (Ridhoi, 2023). Untuk proses pertukaran kunci, digunakan algoritma Elliptic Curve Diffie-Hellman (ECDH), khususnya dengan kurva Curve25519 yang dikenal akan efisiensi dan keamanannya. Setelah proses pertukaran kunci berhasil, pesan dienkripsi menggunakan algoritma Advanced Encryption Standard (AES) 256-bit dalam mode CBC (Cipher Block Chaining) yang dilengkapi dengan HMAC-SHA256 untuk menjamin integritas data.

Sistem ini tidak hanya dirancang untuk mencegah pihak ketiga dari membaca isi pesan, tetapi juga untuk memberikan *forward secrecy*, yaitu kemampuan agar kunci yang digunakan untuk satu pesan tidak bisa digunakan untuk mendekripsi pesan lainnya (Leman & Rahman, 2020). Dengan demikian, bahkan jika suatu kunci berhasil diretas, pesan-pesan sebelumnya tetap aman.

Pendekatan arsitektur keamanan ini menjadikan WhatsApp sebagai salah satu pionir dalam penerapan sistem E2EE berskala global. Namun, tantangan tetap ada, seperti serangan pada perangkat pengguna (endpoint), kelemahan dalam pengelolaan kunci cadangan (backup), serta risiko metadata yang tidak terenkripsi. Oleh karena itu, penting untuk memahami secara mendalam bagaimana teknologi ini bekerja, serta mengevaluasi kelebihan dan keterbatasannya agar dapat dijadikan rujukan dalam pengembangan sistem komunikasi digital yang aman dan terpercaya.

Di era digital saat ini, perlindungan terhadap data dan privasi menjadi kebutuhan mendesak yang tidak dapat diabaikan (Ardiansyah & Ardiana, 2023). Meningkatnya pertukaran informasi melalui platform komunikasi daring, seperti WhatsApp, telah memperluas potensi ancaman keamanan data, mulai dari penyadapan hingga manipulasi informasi oleh pihak tidak bertanggung jawab. Implementasi sistem End-to-End Encryption (E2EE) oleh WhatsApp menjadi salah satu langkah penting dalam menjawab tantangan ini. Namun, seiring berkembangnya teknik serangan siber dan eksploitasi celah keamanan pada perangkat pengguna (endpoint), pemahaman yang lebih mendalam terhadap arsitektur keamanan E2EE serta evaluasi atas efektivitasnya sangat dibutuhkan, baik dari sisi teknis maupun implementatif. Meskipun banyak studi telah membahas struktur teknis E2EE dan

keunggulan kriptografinya, masih terbatas penelitian yang secara komprehensif mengkaji penerapan sistem E2EE pada WhatsApp dengan fokus integratif pada keamanan pesan, manajemen kunci, risiko metadata, dan kelemahan endpoint secara bersamaan. Penelitian sebelumnya cenderung terfragmentasi dan hanya meninjau satu aspek. Selain itu, belum banyak kajian akademik yang mengevaluasi bagaimana pendekatan sistem WhatsApp dapat dijadikan rujukan untuk perancangan sistem komunikasi digital yang aman dan adaptif di luar aplikasi komersial.

Sejumlah penelitian sebelumnya telah membahas efektivitas sistem E2EE. Santria & Arsoetar, (2017) mengkaji arsitektur kunci publik yang digunakan WhatsApp dalam protokol Signal, termasuk Identity Key, Signed Pre Key, dan One-Time Pre Key. Mediana & Fadhli, (2023) menyoroti efektivitas kombinasi algoritma kriptografi simetris dan asimetris dalam mencegah serangan Man-in-the-Middle. Sementara itu, Mundzir & Wirawan, (2024) menggarisbawahi keberhasilan AES-256 dalam menjaga integritas dan kerahasiaan data, serta tantangan pada aspek keamanan perangkat pengguna.

Kebaruan dari penelitian ini terletak pada pendekatan holistik yang menggabungkan analisis teknis algoritma kriptografi (ECDH Curve25519, AES-256, HMAC-SHA256), evaluasi terhadap manajemen kunci dan rotasi dinamis melalui Double Ratchet Algorithm, serta peninjauan tantangan aktual seperti endpoint security dan metadata leakage. Penelitian ini tidak hanya mendeskripsikan mekanisme E2EE, tetapi juga menilai kelayakan sistem sebagai model keamanan digital yang dapat diadaptasi untuk kebutuhan aplikasi komunikasi lainnya di sektor publik maupun privat.

Penelitian ini bertujuan untuk menganalisis secara mendalam sistem End-to-End Encryption pada WhatsApp yang berbasis protokol Signal, dengan meninjau kombinasi kriptografi asimetris dan simetris yang digunakan, mengidentifikasi keunggulan serta potensi kelemahannya, dan mengevaluasi sejauh mana sistem ini mampu menjamin keamanan komunikasi digital dalam konteks ancaman siber yang kompleks. Secara teoritis, penelitian ini memberikan kontribusi terhadap pengembangan literatur di bidang kriptografi modern dan sistem keamanan komunikasi digital. Bagi praktisi keamanan siber dan pengembang aplikasi, penelitian ini dapat menjadi acuan dalam merancang sistem perlindungan data berbasis E2EE yang aman dan efisien. Sementara itu, bagi masyarakat umum dan pengguna teknologi, penelitian ini meningkatkan kesadaran mengenai pentingnya perlindungan data pribadi serta memberikan pemahaman teknis tentang bagaimana sistem keamanan bekerja dalam aplikasi sehari-hari seperti WhatsApp.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur sebagai kerangka utama untuk menggali dan menganalisis penerapan sistem End-to-End Encryption (E2EE) menggunakan algoritma AES-256 dalam aplikasi WhatsApp. Studi literatur dipilih karena pendekatan ini memungkinkan peneliti untuk memperoleh pemahaman yang mendalam, menyeluruh, dan teoritis mengenai objek penelitian berdasarkan data sekunder yang relevan dan terverifikasi secara akademik.

Data dikumpulkan dari berbagai sumber, termasuk:

1. Jurnal ilmiah yang membahas enkripsi, kriptografi, dan keamanan data.
2. Dokumentasi teknis resmi dari WhatsApp dan Signal Foundation mengenai protokol Signal dan implementasi sistem E2EE.
3. White papers dan spesifikasi teknis dari pengembang kriptografi seperti Open Whisper Systems.
4. Sumber akademik dan non-akademik lain seperti prosiding seminar, buku referensi, dan artikel teknologi terapan.

Langkah-langkah metodologis dalam penelitian ini dirancang secara sistematis untuk mengkaji struktur dan efektivitas E2EE dalam WhatsApp. Adapun tahapan penelitian secara rinci adalah sebagai berikut:

1. Pengumpulan Literatur
   Proses pengumpulan data dilakukan dengan menyaring referensi yang berkaitan langsung dengan teknologi enkripsi simetris AES-256, pertukaran kunci ECDH Curve25519, dan protokol Signal. Literatur dipilih berdasarkan kredibilitas, relevansi, dan tahun publikasi (minimal 2019–2024) untuk memastikan konteks yang mutakhir. Proses seleksi ini juga mengikuti pendekatan Systematic Literature Review (SLR) guna menghindari bias interpretatif.
2. Analisis Arsitektur Keamanan WhatsApp
   Peneliti melakukan eksplorasi terhadap arsitektur sistem WhatsApp yang mengadopsi protokol Signal. Analisis ini mencakup:
   a. Struktur pertukaran kunci (Identity Key, Signed Pre Key, One-Time Pre Key).
   b. Proses pembentukan sesi komunikasi (session initialization).
   c. Mekanisme pembangkitan session key (Root Key, Chain Key, dan Message Key).
   d. Integrasi algoritma AES-256 dan HMAC-SHA256 untuk enkripsi dan validasi integritas pesan.

   Analisis ini bertujuan untuk membedah bagaimana WhatsApp membangun sistem keamanan berlapis guna menjamin kerahasiaan dan integritas data pengguna.
3. Simulasi Enkripsi-Dekripsi
   Untuk memperkuat validitas teknis, dilakukan simulasi terbatas terhadap proses enkripsi dan dekripsi pesan berbasis AES-256. Simulasi ini mencakup:
   a. Pembuatan cipher dari plaintext menggunakan kunci 256-bit.
   b. Implementasi mode operasi Cipher Block Chaining (CBC) dan penambahan IV (Initialization Vector).
   c. Validasi autentikasi dan integritas menggunakan HMAC-SHA256.

   Di sisi pertukaran kunci, simulasi pendek dilakukan terhadap cara kerja ECDH Curve25519 untuk menghasilkan shared secret sebagai dasar pembentukan session key.
4. Evaluasi Kekuatan dan Kelemahan Implementasi
   Penelitian ini juga melakukan evaluasi terhadap potensi kekuatan dan kelemahan implementasi sistem keamanan WhatsApp. Evaluasi dilakukan berdasarkan skenario serangan umum, seperti:
   a. Man-in-the-Middle Attack (MitM).
   b. Serangan brute-force pada AES.
   c. Eksploitasi perangkat endpoint (melalui malware, phishing, atau social engineering).
   d. Pencurian metadata dan pengelolaan backup cloud.

   Aspek yang menjadi perhatian utama dalam evaluasi ini meliputi confidentiality, integrity, forward secrecy, dan resilience terhadap serangan kontemporer.

Tujuan utama dari metodologi ini adalah untuk memperoleh pemahaman teknis secara menyeluruh mengenai bagaimana sistem enkripsi end-to-end diterapkan dalam WhatsApp, termasuk efektivitasnya dalam menjaga kerahasiaan dan integritas komunikasi digital serta celah-celah kerentanan yang mungkin muncul dalam praktiknya. Dengan pendekatan ini, hasil analisis diharapkan dapat memberikan kontribusi ilmiah terhadap pengembangan sistem komunikasi yang lebih aman dan andal di masa depan.

HASIL DAN PEMBAHASAN

Implementasi sistem keamanan pada WhatsApp didasarkan pada arsitektur kriptografi berlapis yang mengombinasikan algoritma simetris dan asimetris untuk mencapai tingkat

proteksi maksimal terhadap komunikasi digital. WhatsApp mengadopsi Signal Protocol sebagai kerangka utama dalam menerapkan End-to-End Encryption (E2EE) (Wali et al., 2024), yang berfokus pada tiga prinsip utama: kerahasiaan, integritas**,** dan forward secrecy. Berikut adalah pembahasan rinci berdasarkan tahapan teknis implementasi sistem keamanan tersebut:

Pertukaran Kunci (Key Exchange)

Tahapan ini merupakan dasar dari proses komunikasi terenkripsi (Prianggodo, 2018; Urva, 2017). Ketika dua pengguna WhatsApp memulai komunikasi, aplikasi akan melakukan proses inisialisasi sesi melalui pertukaran sejumlah kunci publik, yaitu:

1. Identity Key (kunci jangka panjang).
2. Signed Pre Key **(**kunci jangka menengah yang ditandatangani).
3. One-Time Pre Key (kunci temporer yang hanya digunakan sekali).

Semua kunci ini berbasis Elliptic Curve Diffie-Hellman (ECDH) dengan kurva Curve25519, yang dikenal akan efisiensi dan keamanannya dalam menghasilkan shared secret. Pengirim (inisiator) menghitung master secret melalui kombinasi ECDH berikut:

makefile
SalinEdit

```
master_secret = ECDH(Ipengirim, Spreceiver) || ECDH(Epengirim, Ireceiver) ||
                ECDH(Epengirim, Spreceiver) || ECDH(Epengirim, Oreceiver)
```

Proses ini menjamin bahwa hanya pihak yang memiliki kunci privat dan publik terkait yang mampu menghasilkan shared key, sekaligus menjamin forward secrecy (jika satu kunci bocor, sesi lain tetap aman).

Pembangkitan Session Key

Dari master secret yang dihasilkan, proses dilanjutkan dengan pembentukan Root Key dan Chain Key menggunakan fungsi HMAC-based Key Derivation Function (HKDF) (Hagen, 2023; Yao et al., 2023). Sistem ini dikenal sebagai Double Ratchet Algorithm, di mana Chain Key digunakan untuk menghasilkan Message Key secara dinamis di setiap pengiriman pesan. Komposisi Message Key sebagai berikut:

1. 32 Byte: kunci enkripsi AES-256.
2. 32 Byte: kunci HMAC-SHA256 untuk verifikasi integritas.
3. 16 Byte**:** Initialization Vector (IV) untuk mode enkripsi CBC.

   Karena Message Key bersifat ephemeral (sekali pakai), sistem ini juga mendukung self-healing security—jika satu sesi terganggu, sesi berikutnya tetap aman karena menggunakan kunci baru.

Enkripsi dan Dekripsi Pesan

Setelah Message Key dibentuk, setiap pesan akan melalui proses enkripsi sebagai berikut:

1. Enkripsi dilakukan menggunakan AES-256 dalam mode CBC, sebuah mode operasi block cipher yang menambahkan keacakan melalui IV.
2. Integritas data dijamin dengan menggunakan HMAC-SHA256**,** yang menghasilkan tag autentikasi pesan dan mencegah manipulasi isi.
3. Setiap pesan yang dikirim membawa metadata terenkripsi yang menginformasikan identitas pengirim, ID sesi, dan kunci publik sementara.

   Penerima pesan kemudian menggunakan Message Key yang sama untuk mendekripsi isi pesan. Karena tidak ada Message Key yang disimpan di server, hanya perangkat penerima sah yang dapat membuka isi pesan tersebut.

Evaluasi Keamanan

Keunggulan utama dari sistem ini meliputi:

1. Kerahasiaan (Confidentiality): Dengan tidak adanya penyimpanan kunci di server dan penggunaan ECDH + AES, tidak ada entitas lain—termasuk WhatsApp—yang dapat membaca isi pesan.

2. Integritas (Integrity): Tag HMAC memastikan pesan tidak mengalami perubahan selama transmisi. Bila terjadi perubahan, pesan akan dianggap rusak dan tidak diproses.
3. Forward Secrecy: Setiap pesan menggunakan Message Key yang berbeda (Yuliana & dan Suwadi, 2019). Artinya, kompromi pada satu kunci tidak akan memengaruhi keamanan pesan sebelumnya atau sesudahnya.

Namun, terdapat sejumlah tantangan teknis dan non-teknis, antara lain:

5. Endpoint Vulnerability: Keamanan E2EE sangat bergantung pada perangkat pengguna. Serangan seperti malware**,** keylogger, atau akses fisik dapat mengekspos pesan meskipun dienkripsi selama transmisi.
6. Pengelolaan Metadata: Meskipun isi pesan terenkripsi, informasi seperti waktu kirim, nama pengirim, dan ID perangkat masih dapat terekam oleh server dan berpotensi disalahgunakan.
7. Manajemen Sesi dan Backup: Jika pengguna memulihkan cadangan dari cloud (yang tidak terenkripsi end-to-end), sesi E2EE sebelumnya dapat terbuka. WhatsApp saat ini menawarkan backup terenkripsi, namun tidak semua pengguna mengaktifkannya.

Dengan demikian, hasil kajian ini menunjukkan bahwa sistem enkripsi yang diimplementasikan WhatsApp merupakan salah satu yang paling komprehensif dan adaptif dalam ranah komunikasi digital. Kombinasi arsitektur kriptografi hibrida dan algoritma kuat seperti AES-256 dan Curve25519 berhasil menciptakan lingkungan komunikasi yang aman. Namun, untuk mencapai tingkat keamanan ideal, perlu diimbangi dengan edukasi pengguna**,** penguatan keamanan perangkat, serta peninjauan ulang terhadap manajemen metadata dan fitur cadangan.

KESIMPULAN

Penerapan *End-to-End Encryption* (E2EE) pada WhatsApp menggunakan algoritma Advanced Encryption Standard (AES) 256-bit dan Elliptic Curve Diffie-Hellman (ECDH) dengan Curve25519 terbukti menjadi salah satu model keamanan komunikasi digital paling kuat saat ini. Sistem ini menggabungkan kriptografi simetris dan asimetris dalam kerangka Signal Protocol serta didukung oleh *Double Ratchet Algorithm*, yang memperbarui kunci sesi untuk setiap pesan guna menjamin *forward secrecy*. WhatsApp juga menerapkan *zero-knowledge architecture*, di mana pihak penyedia layanan tidak menyimpan kunci enkripsi.

Namun, efektivitas E2EE tetap menghadapi tantangan, terutama pada sisi *endpoint*, yakni perangkat pengguna. Ancaman seperti malware, *keylogger*, atau akses fisik tidak sah dapat mengekspos pesan setelah didekripsi. Selain itu, metadata seperti informasi waktu pengiriman dan identitas kontak masih rentan karena tidak terenkripsi. Celah lainnya adalah cadangan pesan di *cloud* yang seringkali tidak terlindungi oleh E2EE. Di tengah meningkatnya kesadaran masyarakat terhadap privasi digital, sistem seperti E2EE menjadi krusial, tidak hanya sebagai solusi teknis, tetapi juga sebagai bentuk perlindungan hak atas privasi dan kebebasan berekspresi. Untuk menyempurnakan sistem ini, diperlukan kolaborasi antara pengembang, pakar keamanan, regulator, dan pengguna. Langkah-langkah seperti audit terbuka, penguatan sisi perangkat, serta edukasi keamanan digital sangat penting untuk memastikan komunikasi yang aman, transparan, dan adil di era digital.

REFERENSI

Ardiansyah, M. R., & Ardiana, R. (2023). Kewajiban Dan Tanggung Jawab Hukum Perdata Dalam Perlindungan Privasi Data Pasien Dalam Layanan Kesehatan Digital. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *1*(4), 276–287.

Aska, M. F., Putra, D. P., & Sinambela, C. J. M. (2024). Strategi Efektif Untuk Implementasi

Keamanan Siber di Era Digital. *Journal of Informatic and Information Security*, *5*(2), 187–200.

Hagen, H. K. (2023). *Authenticated Key Exchange: An analysis of low-cost protocols*. NTNU.

Leman, D., & Rahman, M. (2020). Metode Merkle Hellman Untuk Enkripsi dan Dekripsi Pesan Whatapp. *Riau Journal Of Computer Science*, *6*(1), 45–49.

Liander, G. V. (2022). Penggunaan Algoritma Elliptic Curve Diffie Hellman dan AES 256 pada Implementasi End-to-End Encryption WhatsApp. *Sumber*, *7680*(384), 15360.

Mediana, S. D., & Fadhli, M. (2023). Implementing Zero Trust Model for SSH Security with kerberos and OpenLDAP. *Sistemasi: Jurnal Sistem Informasi*, *12*(3), 981–995.

Mundzir, J. A., & Wirawan, W. (2024). Implementasi Lightweight Cryptography untuk Keamanan Data pada Sistem Komunikasi LoRa. *Jurnal Teknik ITS*, *13*(3), A236–A142.

Prianggodo, D. Y. (2018). Prototipe Pengamanan Data Pada Aplikasi Lapor Polisi Berbasis Android Dengan Algoritma Blowfish Dan Algoritma Diffie-Hellman. *JIKA (Jurnal Informatika)*, *2*(1).

Ridhoi, M. (2023). *Implementasi Algoritma Elliptic Curve Cryptography (ECC) dengan End-to-End Encryption pada Aplikasi Chat= Implementation of Elliptic Curve Cryptography (ECC) Algorithm with End-To-End Encryption in Mobile-Based Chat Application*. Universitas Hasanuddin.

Santria, U., & Arsoetar, N. (2017). *Penggunaan Enkripsi End-to-End dalam Pengamanan Pesan dan Video Call pada Whatsapp*.

Siregar, S. R. S., & Sundari, P. (2016). Rancangan Sistem Informasi Pengelolaan Data Kependudukan Desa (Studi Kasus di Kantor Desa Sangiang Kecamatan Sepatan Timur). *Jurnal Sisfotek Global*, *6*(1).

Urva, G. (2017). Analisis Penggunaan Enkripsi End To End Pada Aplikasi Whatsapp Messengger. *Jurnal Unitek*, *10*(1), 34–45.

Wali, M., Syafrizal, S., Syafrinal, S., & Fathurrahmad, F. (2024). Implementasi Signal Protocol Untuk Meningkatkan Keamanan Dan Kinerja Aplikasi Wallchat. *Jurnal Digitech*, *1*(1), 1–17.

Yao, J., Hlayhel, A., & Matusiewicz, K. (2023). Post Quantum KEM authentication in SPDM for secure session establishment. *IEEE Design & Test*.

Yuliana, M., & dan Suwadi, W. (2019). *Skema Secret Key Generation (SKG) untuk Keamanan pada Sistem Komunikasi di Lingkungan Wireless*. Institut Teknologi Sepuluh Nopember.