INTEGRASI ECDHE CURVE25519, RSASSA-PSS, DAN AES-256 UNTUK PENINGKATAN PROTOKOL PERTUKARAN KUNCI PRIVATEDH DALAM KOMUNIKASI *END-TO-END*

TESIS

Oleh:

ARDI SAPUTRA
NIM. 241231060

PROGRAM STUDI S-2 TEKNOLOGI INFORMASI
FAKULTAS INFORMATIKA
UNIVERSITAS MIKROSKIL
MEDAN
2025

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

INTEGRATION OF ECDHE CURVE25519, RSASSA-PSS, AND AES-256 FOR ENHANCED PRIVATEDH KEY EXCHANGE PROTOCOL IN END-TO-END COMMUNICATION

THESIS

By:

ARDI SAPUTRA
ID NUMBER. 241231060

MAJOR OF S-2 INFORMATION TECHNOLOGY
FACULTY OF INFORMATICS
UNIVERSITAS MIKROSKIL
MEDAN
2025

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

LEMBARAN PENGESAHAN

INTEGRASI ECDHE CURVE25519, RSASSA-PSS, DAN AES-256 UNTUK PENINGKATAN PROTOKOL PERTUKARAN KUNCI PRIVATEDH DALAM KOMUNIKASI *END-TO-END*

TESIS

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Magister
Program Studi S-2 Teknologi Informasi

Oleh:

ARDI SAPUTRA
NIM. 241231060

Disetujui Oleh:

Dosen Pembimbing,

Dr. Ronsen Purba, M.Sc.

Medan, 03 September 2025
Diketahui dan Disahkan Oleh:

Ketua Program Studi
S-2 Teknologi Informasi,

Ir. Erwin Setiawan Panjaitan, M.M.S.I., Ph.D.

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-2 Teknologi Informasi Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Ardi Saputra
NIM : 241231060

Saya telah melaksanakan penelitian dan penulisan Tesis dengan judul dan tempat penelitian sebagai berikut:

Judul Tesis : Integrasi ECDHE Curve25519, RSASSA-PSS, dan AES-256 Untuk Peningkatan Protokol Pertukaran Kunci Privatedh Dalam Komunikasi *End-To-End*
Tempat Penelitian : -
Alamat Tempat Penelitian : -
No. Telp. Tempat Penelitian : -

Sehubungan dengan Tesis tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Tesis tersebut merupakan hasil karya saya sendiri (tidak menyuruh orang lain yang mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar. Bila di kemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya (membuatnya), maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh Universitas Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada Universitas Mikroskil Medan Hak Bebas Royalti Non-eksklusif (Non-exclusive Royalty Free Right) atas Tesis saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, Universitas Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Tesis saya, secara keseluruhan atau hanya sebagian atau hanya ringkasannya saja dalam bentuk format tercetak dan/atau elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Tesis saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak/sistem informasi.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 20 Juni 2025
Saya yang membuat pernyataan,

Ardi Saputra

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

INTEGRASI ECDHE CURVE25519, RSASSA-PSS, DAN AES-256 UNTUK PENINGKATAN PROTOKOL PERTUKARAN KUNCI PRIVATEDH DALAM KOMUNIKASI *END-TO-END*

Abstrak

Meningkatnya permintaan untuk komunikasi digital yang aman membutuhkan protokol kriptografi yang tidak hanya efisien tetapi juga mampu memastikan kerahasiaan, integritas, dan keaslian pesan. PrivateDH adalah salah satu protokol yang menggabungkan Diffie-Hellman, RSA, dan AES; namun, protokol ini masih memiliki beberapa kelemahan utama, termasuk tidak adanya otentikasi pengguna dan ketergantungan pada algoritma Diffie-Hellman klasik, yang secara komputasi sangat intensif dan tidak mendukung forward secrecy. Penelitian ini mengusulkan versi yang ditingkatkan dari protokol PrivateDH dengan mengintegrasikan ECDHE Curve25519 sebagai pengganti DH klasik, dan RSASSA-PSS sebagai mekanisme tanda tangan digital yang kuat untuk otentikasi pengguna. Metodologi yang digunakan mencakup implementasi dan pengujian protokol yang diusulkan dalam skenario komunikasi peer-to-peer, dengan evaluasi kinerja berdasarkan durasi handshake, penggunaan CPU dan memori, serta penilaian keamanan termasuk validasi tanda tangan digital dan forward secrecy. Hasilnya menunjukkan bahwa protokol yang ditingkatkan secara efektif mempercepat pertukaran kunci, mempertahankan efisiensi sumber daya, dan menyediakan otentikasi pengguna yang andal. Dengan demikian, protokol ini memberikan kontribusi yang berarti bagi kemajuan sistem komunikasi end-to-end yang lebih aman dan efisien, selaras dengan tuntutan lingkungan digital modern.

Kata kunci: *Keamanan Komunikasi; End-to-End Encryption; ECDHE Curve25519; RSASSA-PSS; AES-256.*

Abstract

The growing demand for secure digital communication calls for cryptographic protocols that are not only efficient but also capable of ensuring message confidentiality, integrity, and authenticity. PrivateDH is one such protocol that combines Diffie-Hellman, RSA, and AES; however, it still exhibits key weaknesses, including the absence of user authentication and reliance on classical Diffie-Hellman algorithms, which are computationally intensive and do not support forward secrecy. This study proposes an enhanced version of the PrivateDH protocol by integrating ECDHE Curve25519 as a replacement for classic DH, and RSASSA-PSS as a robust digital signature mechanism for user authentication. The methodology involves implementing and testing the proposed protocol within a peer-to-peer communication scenario, with performance evaluations based on handshake duration, CPU and memory usage, as well as security assessments including digital signature validation and forward secrecy. The results demonstrate that the enhanced protocol effectively accelerates key exchange, maintains resource efficiency, and provides reliable user authentication. In conclusion, this protocol contributes meaningfully to the advancement of more secure and efficient end-to-end communication systems, aligning with the demands of modern digital environments.

Keywords: *Secure Communication; End-to-End Encryption; ECDHE Curve25519; RSASSA-PSS; AES-256.*

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan tesis yang berjudul "Integrasi ECDHE Curve25519, RSASSA-PSS, dan AES-256 Untuk Peningkatan Protokol Pertukaran Kunci Privatedh Dalam Komunikasi *End-To-End*" dengan baik dan lancar.

Tesis ini disusun sebagai salah satu syarat untuk memperoleh gelar Magister pada Program Studi S-2 Teknologi Informasi, Fakultas Informatika, Universitas Mikroskil Medan. Penelitian ini dilakukan sebagai bentuk kontribusi ilmiah dalam menjawab tantangan keamanan komunikasi digital modern, khususnya pada protokol pertukaran kunci yang aman, efisien dan independen.

Penulis menyampaikan terima kasih yang sebesar-besarnya kepada berbagai pihak yang telah memberikan bimbingan, dukungan, dan bantuan selama proses penulisan tesis ini, khususnya kepada:

1. Bapak Dr. Ronsen Purba, M.Sc., selaku Dosen Pembimbing yang telah membimbing penulis dalam menyelesaikan tesis ini.
2. Bapak Hardy, S.Kom., M.Sc., Ph.D., selaku Rektor Universitas Mikroskil Medan.
3. Bapak Sunaryo Winardi, S.Kom., M.T., selaku Dekan Fakultas Informatika Universitas Mikroskil Medan.
4. Bapak Ir. Erwin Setiawan Panjaitan, M.M.S.I., Ph.D., selaku Ketua Program Studi S-2 Teknologi Informasi Fakultas Informatika Universitas Mikroskil Medan.

Ucapan terima kasih juga penulis sampaikan kepada kedua orang tua, keluarga, dan seluruh sahabat yang selalu memberikan semangat, doa, dan dukungan, baik secara moral maupun materi, selama proses penyusunan tesis ini berlangsung.

Penulis menyadari bahwa dalam penyusunan tesis ini masih terdapat kekurangan, baik dari sisi analisis maupun ruang lingkup implementasi, yang disebabkan oleh keterbatasan waktu dan sumber daya. Namun demikian, penulis berharap bahwa melalui pendekatan terpadu yang digunakan, tesis ini tetap dapat memberikan kontribusi bagi pengembangan ilmu pengetahuan di bidang keamanan komunikasi digital.

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

Akhir kata, penulis berharap tesis ini dapat bermanfaat bagi semua pihak yang membutuhkan dan menjadi dasar untuk penelitian lebih lanjut di masa yang akan datang.

Medan, 20 Juni 2025

Penulis,

Ardi Saputra

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

DAFTAR ISI

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

DAFTAR GAMBAR

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.

DAFTAR TABEL

© Karya Dilindungi UU Hak Cipta
1. Dilarang menyebarluaskan dokumen tanpa izin.
2. Dilarang melakukan plagiasi.
3. Pelanggaran diberlakukan sanksi sesuai peraturan UU Hak Cipta.