

IMPLEMENTASI DAN EVALUASI PROTOKOL KEAMANAN CHATting MENGGUNAKAN CHACHA20 DAN ECDHE UNTUK PENCEGAHAN EAVESDROPPING

SKRIPSI

Oleh:

CHARLES

NIM. 221110156

CECILIA ONGSO

NIM. 221111729

JASON WILBERT

NIM. 221111572



**PROGRAM STUDI S-1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
UNIVERSITAS MIKROSKIL
MEDAN
2026**

IMPLEMENTATION AND EVALUATION OF CHATTING SECURITY PROTOCOLS USING CHACHA20 AND ECDHE TO PREVENT EAVESDROPPING

UNDERGRADUATE THESIS

By:

CHARLES

ID NUMBER. 221110156

CECILIA ONGSO

ID NUMBER. 221111729

JASON WILBERT

ID NUMBER. 221111572



**UNDERGRADUATE PROGRAM OF S-1 INFORMATICS ENGINEERING
FACULTY OF INFORMATICS
UNIVERSITAS MIKROSKIL
MEDAN
2026**

LEMBARAN PENGESAHAN

IMPLEMENTASI DAN EVALUASI PROTOKOL KEAMANAN
CHATting MENGGUNAKAN CHACHA20 DAN ECDHE
UNTUK PENCEGAHAN EAVESDROPPING

SKRIPSI

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Sarjana
Program Studi S-1 Teknik Informatika

Oleh:

CHARLES
NIM. 221110156
CECILIA ONGSO
NIM. 221111729
JASON WILBERT
NIM. 221111572

Disetujui Oleh:

Dosen Pembimbing,

Dosen Pembimbing I,



Syanti Irviantina, S.Kom., M.Kom.

Dosen Pembimbing II,



Darwin, S.Kom., M.Kom.

Medan, 22 Juli 2026

Diketahui dan Disahkan Oleh:

Ketua Program Studi
S-1 Teknik Informatika,



Charles Juliandy, S.Kom., M.Kom.

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Cecilia Ongso

NIM : 221111729

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

Judul Skripsi : Implementasi dan Evaluasi Protokol Keamanan Chatting Menggunakan ChaCha20 dan ECDHE untuk Pencegahan Eavesdropping

Tempat Penelitian : -

Alamat Tempat Penelitian : -

No. Telp. Tempat Penelitian : -

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi 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 Skripsi 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 Skripsi 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 Skripsi 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, 6 Juli 2026

Saya yang membuat pernyataan,


METRAK
TEMPEL
F7408AQX058965035
Cecilia Ongso

HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Charles

NIM : 221110156

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

Judul Skripsi : Implementasi dan Evaluasi Protokol Keamanan Chatting Menggunakan ChaCha20 dan ECDHE untuk Pencegahan Eavesdropping

Tempat Penelitian : -

Alamat Tempat Penelitian : -

No. Telp. Tempat Penelitian : -

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi 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 Skripsi 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 Skripsi 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 Skripsi 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, 6 Juli 2026

Saya yang membuat pernyataan,



HALAMAN PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Program Studi S-1 Teknik Informatika Universitas Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Jason Wilbert

NIM : 221111572

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

Judul Skripsi : Implementasi dan Evaluasi Protokol Keamanan Chatting Menggunakan ChaCha20 dan ECDHE untuk Pencegahan Eavesdropping

Tempat Penelitian : -

Alamat Tempat Penelitian : -

No. Telp. Tempat Penelitian : -

Sehubungan dengan Skripsi tersebut, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Skripsi 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 Skripsi 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 Skripsi 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 Skripsi 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, 6 Juli 2026

Saya yang membuat pernyataan,



Jason
Wilbert

IMPLEMENTASI DAN EVALUASI PROTOKOL KEAMANAN CHATTING MENGGUNAKAN CHACHA20 DAN ECDHE UNTUK PENCEGAHAN EAVESDROPPING

Abstrak

Aplikasi chatting berbasis web menghadapi tantangan serius terkait keamanan komunikasi, yaitu serangan eavesdropping. Untuk melindungi kerahasiaan komunikasi, berbagai aplikasi chatting modern telah menerapkan konsep End-to-End Encryption (E2EE), di mana proses enkripsi dan dekripsi pesan dilakukan langsung pada sisi pengirim dan penerima. Pada penelitian ini, akan dievaluasi efektivitas kombinasi algoritma ChaCha20 dan Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) dalam mencegah serangan eavesdropping pada skenario komunikasi chatting berbasis web. Metode yang digunakan dalam penelitian ini adalah metode Waterfall. Hasil evaluasi menunjukkan bahwa metode ChaCha20 dapat diterapkan secara praktis dalam aplikasi chatting karena memiliki waktu eksekusi yang cepat. Selain itu, metode ECDHE juga mampu mendeteksi adanya perubahan baik terhadap nilai kunci publik ataupun nilai hash dari user penerima, sehingga proses komunikasi akan langsung dihentikan apabila terdeteksi adanya perubahan data tersebut. Percobaan dekripsi dengan menyadap data kunci publik dan beberapa ciphertext juga akan sulit berhasil, karena tidak adanya korelasi antara beberapa ciphertext yang dihasilkan tersebut, walaupun ciphertext dihasilkan dengan menggunakan pesan dan shared key yang sama. Dari hasil pengujian juga terbukti bahwa aplikasi chatting dengan menggunakan metode ChaCha20 dan ECDHE mampu melakukan pencegahan terhadap eavesdropping.

Kata Kunci: *chatting, protokol keamanan, metode ChaCha20, metode ECDHE, eavesdropping*

Abstract

Web-based chat applications face a significant security challenge in the form of eavesdropping attacks. To protect communication confidentiality, many modern messaging applications implement End-to-End Encryption (E2EE), where message encryption and decryption are performed only on the sender's and receiver's devices. This study evaluates the effectiveness of combining the ChaCha20 algorithm and Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) in preventing eavesdropping in a web-based chat application. The research adopts the Waterfall development methodology. The evaluation results show that ChaCha20 is practical for chat applications due to its fast execution time. In addition, ECDHE can detect any modification to the recipient's public key or hash value, causing the communication process to terminate immediately if such changes are detected. Decryption attempts through intercepted public keys and ciphertexts are also unlikely to succeed because no correlation exists among the generated ciphertexts, even when they are produced from the same plaintext and shared key. The experimental results demonstrate that the integration of ChaCha20 and ECDHE effectively prevents eavesdropping attacks in web-based chat applications.

Keywords: *chatting, security protocol, ChaCha20 method, ECDHE method, eavesdropping*

KATA PENGANTAR

Ucapan syukur kepada Tuhan Yang Maha Esa, penulis ingin mengucapkan terima kasih atas berkat dan karunia-Nya yang telah memungkinkan penulis menyelesaikan Tugas Akhir ini dengan judul **“IMPLEMENTASI DAN EVALUASI PROTOKOL KEAMANAN CHATTING MENGGUNAKAN CHACHA20 DAN ECDHE UNTUK PENCEGAHAN EAVESDROPPING”**.

Tugas Akhir ini disusun sebagai bagian dari persyaratan untuk meraih gelar Sarjana Strata Satu (S1) pada Program Studi Teknik Informatika Universitas Mikroskil Medan.

Dalam proses penulisan Tugas Akhir ini, penulis telah berupaya untuk mencapai hasil yang terbaik. Keberhasilan ini tidak lepas dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih kepada:

1. Ibu Syanti Irviantina, S.Kom, M.Kom, selaku Dosen Pembimbing I.
2. Bapak Darwin, S.Kom, M.Kom, selaku Dosen Pembimbing II.
3. Bapak Hardy, S.Kom, M.Sc., Ph.D., selaku Rektor Universitas Mikroskil Medan.
4. Bapak Sunaryo Winardi, S.Kom, M.T., selaku Dekan Fakultas Informatika Universitas Mikroskil Medan.
5. Bapak Carles Juliandy, S.Kom, M.Kom, selaku Ketua Program Studi S-1 Teknik Informatika Fakultas Informatika Universitas Mikroskil Medan.
6. Orang tua dan keluarga yang selalu memberikan doa, dukungan, motivasi pada penulis selama penyusunan Tugas Akhir.
7. Seluruh teman-teman seperjuangan yang telah membantu penulis dalam bentuk doa dan dukungan, serta pihak-pihak yang memberi masukan dalam Tugas Akhir.

Penulis menyadari Tugas Akhir ini tidak lepas dari kekurangan dan jauh dari kesempurnaan karena keterbatasan pengetahuan dan pengalaman penulis. Oleh karena itu, kritik dan saran dari pembaca sangat diharapkan agar Tugas Akhir ini dapat memberikan manfaat untuk pembaca dan bagi pihak-pihak yang membutuhkan.

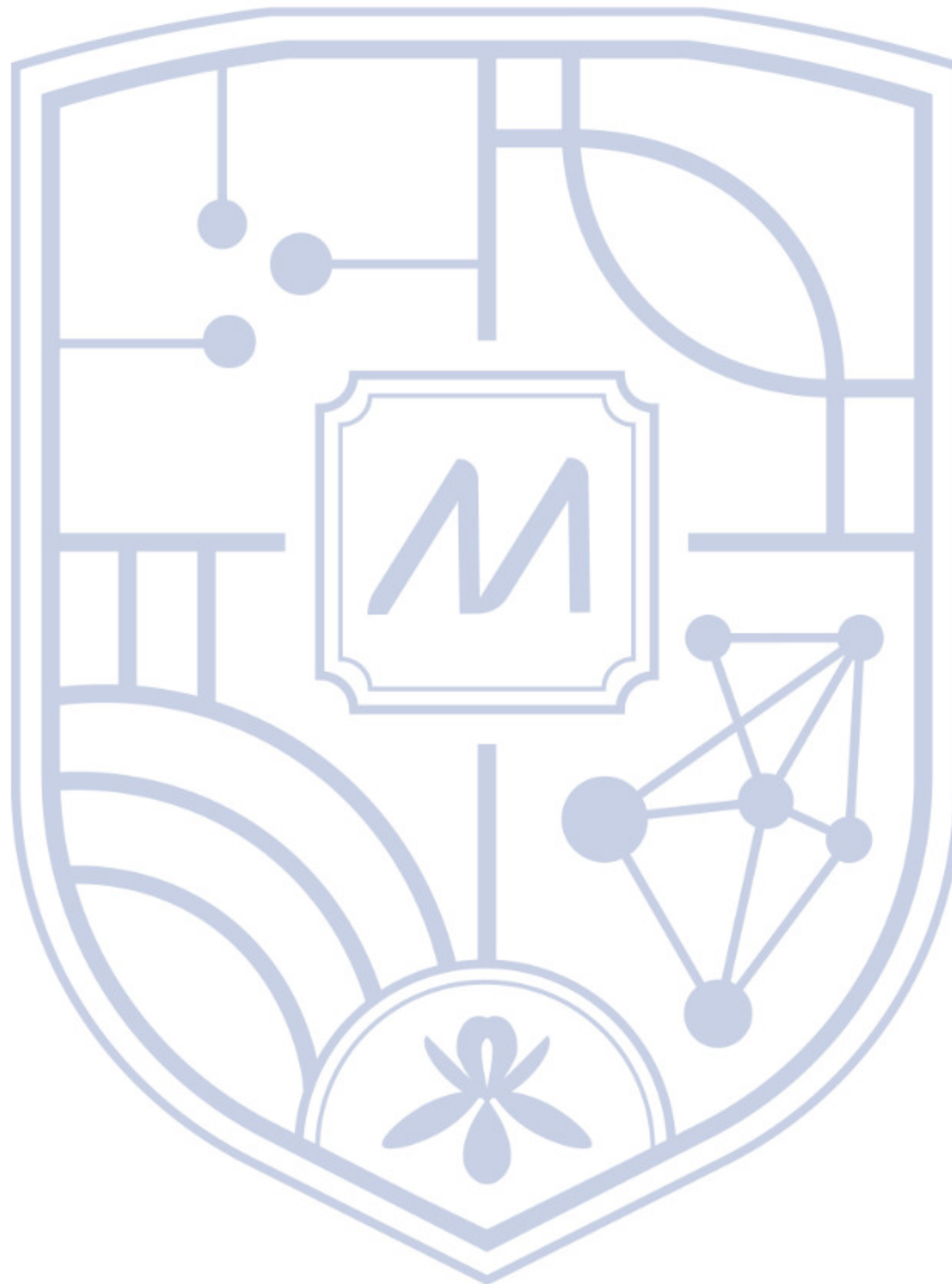
Medan, 01 Juli 2026

Penulis,

Charles

Cecilia Ongso

Jason Wilbert



DAFTAR ISI

Abstrak.....	i
Abstract.....	i
KATA PENGANTAR	ii
DAFTAR ISI	iv
DAFTAR GAMBAR.....	vi
DAFTAR TABEL	viii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan	3
1.4 Manfaat	3
1.5 Ruang Lingkup.....	3
BAB II KAJIAN LITERATUR.....	5
2.1 Keamanan Data	5
2.2 Kriptografi.....	6
2.2.1 Kriptografi Simetris	9
2.2.2 Kriptografi Asimetris.....	9
2.2.3 Kriptografi Hibrid.....	10
2.3 End-to-End Encryption (E2EE)	11
2.4 Metode ChaCha20.....	12
2.5 Metode Elliptic Curve Diffie-Hellman Ephemeral.....	16
2.5.1 Metode Elliptic Curve Diffie-Hellman.....	16
2.5.2 Prosedur Kerja dari Metode Elliptic Curve Diffie-Hellman Ephemeral.....	19
2.6 Metode SHA-256	21
2.6.1 Fungsi Hash.....	21
2.6.2 Algoritma SHA-256	23
2.7 Aplikasi <i>Chatting</i>	27
2.8 Eavesdropping.....	27
2.8.1 Model Serangan <i>Eavesdropping</i>	28
2.8.2 Pencegahan Eavesdropping dengan Kriptografi Hibrid	28
2.9 Model Keamanan Sistem	29
2.10 Kerangka Pemikiran.....	30
2.11 Penelitian Terdahulu	31

BAB III TAHAPAN PELAKSANAAN	34
3.1 Metode Penelitian	34
3.2 Analisis.....	35
3.2.1 Analisis Proses.....	35
3.2.2 Analisis Kebutuhan Fungsional.....	54
3.2.3 Analisis Kebutuhan Non-Fungsional	62
3.3 Perancangan	63
3.3.1 Rancangan Tampilan	63
3.3.2 Rancangan Basis Data	68
BAB IV HASIL DAN PEMBAHASAN	69
4.1 Hasil	69
4.1.1 Tampilan Utama	69
4.1.2 Tampilan Pengujian Performa	72
4.1.3 Tampilan Pengujian Keamanan.....	73
4.2 Pembahasan.....	74
4.2.1 Pengujian Performa	75
4.2.2 Pengujian Keamanan	79
4.2.3 Pengujian Pencegahan Eavesdropping	87
BAB V PENUTUP	90
5.1 Kesimpulan	90
5.2 Saran.....	90
DAFTAR PUSTAKA.....	91
DAFTAR RIYAWAT HIDUP	94
DAFTAR RIYAWAT HIDUP	95
DAFTAR RIYAWAT HIDUP	96

DAFTAR GAMBAR

Gambar 2.1 Skema Enkripsi dan Dekripsi [16]	8
Gambar 2.2 Skema Algoritma Simetris [17]	9
Gambar 2.3 Skema Algoritma Asimetris [17]	10
Gambar 2.4 Konsep Dasar Enkripsi End to End [21]	12
Gambar 2.5 Fungsi Quarter-Round ChaCha20 [22]	13
Gambar 2.6 Double Round [22]	14
Gambar 2.7 Model Keamanan Komunikasi End-to-End Menggunakan ChaCha20 dan ECDHE	30
Gambar 2.8 Kerangka Penelitian	31
Gambar 3.1 Evaluasi Protokol Keamanan <i>Chatting</i> menggunakan Chacha20 dan ECDHE untuk Pencegahan <i>Eavesdropping</i>	36
Gambar 3.2 Proses Pertukaran Kunci dengan Metode ECDHE	37
Gambar 3.3 Proses Perhitungan Nilai <i>Hash</i> dengan Metode SHA-256	40
Gambar 3.4 Proses Enkripsi dengan Metode ChaCha20	48
Gambar 3.5 Proses Dekripsi dengan Metode ChaCha20	53
Gambar 3.6 <i>Use Case Diagram</i> dari Evaluasi Protokol Keamanan <i>Chatting</i> menggunakan Chacha20 dan ECDHE untuk Pencegahan <i>Eavesdropping</i>	55
Gambar 3.7 Rancangan Halaman <i>Login User</i>	64
Gambar 3.8 Rancangan Halaman Registrasi <i>User</i>	64
Gambar 3.9 Rancangan Halaman Daftar Pesan	65
Gambar 3.10 Rancangan Halaman Evaluasi Protokol Keamanan	66
Gambar 3.11 Rancangan Halaman Evaluasi Performa Sistem	67
Gambar 3.12 Rancangan Class diagram dari Sistem Usulan	68
Gambar 4.1 Halaman <i>Login User</i>	69
Gambar 4.2 Halaman Registrasi <i>User</i>	70
Gambar 4.3 Halaman Pilih <i>User</i>	70
Gambar 4.4 Halaman <i>Chatting</i>	71
Gambar 4.5 Halaman Pengujian	71
Gambar 4.6 Halaman Daftar Pengujian Performansi	72
Gambar 4.7 Halaman Pengujian Performansi	72
Gambar 4.8 Halaman Daftar Pengujian Keamanan	73

Gambar 4.9 Halaman Pengujian Keamanan.....	74
Gambar 4.10 Halaman Daftar Proses Pengujian Performansi.....	77
Gambar 4.11 Halaman Daftar Proses Pengujian Performansi untuk Beberapa Ukuran <i>File</i> Berbeda.....	79
Gambar 4.12 Halaman Proses Pertukaran Kunci di Bagian <i>User</i> Pengirim (Menunggu Respon).....	80
Gambar 4.13 Halaman Proses Pertukaran Kunci di Bagian <i>User</i> Pengirim Setelah Proses Selesai.....	80
Gambar 4.14 Halaman Proses Pertukaran Kunci di Bagian <i>User</i> Penerima	81
Gambar 4.15 Proses Pengujian dengan Mengubah Data Kunci Publik Penerima	81
Gambar 4.16 Proses Pengujian dengan Mengubah Data Nilai <i>Hash</i> Penerima	82
Gambar 4.17 Proses Pengujian dengan Mengubah Data Kunci Publik dan Nilai <i>Hash</i> Penerima	83
Gambar 4.18 Skenario Normal dari Proses Enkripsi Tahapan Awal	83
Gambar 4.19 Skenario Normal dari Proses Enkripsi Tahapan Akhir.....	84
Gambar 4.20 Skenario Normal dari Proses Dekripsi Tahapan Awal.....	84
Gambar 4.21 Skenario Normal dari Proses Dekripsi Tahapan Akhir	85
Gambar 4.22 Proses Pengujian dengan Menyadap Data Kunci Publik dan Beberapa <i>Ciphertext</i>	85
Gambar 4.23 Proses Pengujian dengan Mengubah Data <i>Ciphertext</i> (Tahapan Proses Enkripsi)	86
Gambar 4.24 Proses Pengujian dengan Mengubah Data <i>Ciphertext</i>	87
Gambar 4.25 Proses Pengiriman Pesan pada Proses <i>Chatting</i>	88
Gambar 4.26 Proses Penyadapan dengan Aplikasi <i>Wireshark</i> (Tampilan Awal)	88
Gambar 4.27 Proses Penyadapan dengan Aplikasi <i>Wireshark</i> (Tampilan Lanjutan).....	89

DAFTAR TABEL

Tabel 2.1 Susunan Matriks Metode ChaCha20 [22]	13
Tabel 2.2 Parameter Curve25519 [24].....	19
Tabel 2.3 Inisialisasi Awal dalam Notasi Heksadesimal [8]	24
Tabel 2.4 Konstanta SHA-256 [28]	26
Tabel 2.5 Penelitian Terdahulu	31
Tabel 3.1 Deskripsi Aktor.....	56
Tabel 3.2 Identifikasi Use Case	56
Tabel 3.3 Narasi Use Case Melihat Status User	57
Tabel 3.4 Narasi Use Case Memverifikasi Kunci dengan Metode SHA-256	57
Tabel 3.5 Narasi Use Case Melakukan Proses Pertukaran Kunci dengan Metode ECDHE.....	58
Tabel 3.6 Narasi Use Case Mengirimkan Pesan.....	59
Tabel 3.7 Narasi Use Case Mengenkripsi Pesan dengan Metode ChaCha20	59
Tabel 3.8 Narasi Use Case Menerima Pesan	60
Tabel 3.9 Narasi Use Case Mendekripsi Ciphertext dengan Metode ChaCha20	61
Tabel 3.10 Narasi Use Case Mengevaluasi Protokol Keamanan	61
Tabel 3.11 Narasi Use Case Mengevaluasi Performa Sistem.....	62
Tabel 3.12 Struktur Tabel User	68
Tabel 3.13 Struktur Tabel Pesan.....	68
Tabel 4.1 Hasil Pengujian Performa (Pengujian 1)	75
Tabel 4.2 Hasil Pengujian Performa (Pengujian 2)	75
Tabel 4.3 Hasil Pengujian Performa (Pengujian 3)	76
Tabel 4.4 Hasil Pengujian Performa (Rata-Rata Pengujian 1 sampai 3).....	76
Tabel 4.5 Hasil Pengujian Performa untuk Ukuran File Berbeda (Pengujian 1).....	77
Tabel 4.6 Hasil Pengujian Performa untuk Ukuran File Berbeda (Pengujian 2).....	77
Tabel 4.7 Hasil Pengujian Performa untuk Ukuran File Berbeda (Pengujian 3).....	77
Tabel 4.8 Hasil Pengujian Performa untuk Ukuran File Berbeda (Rata-Rata Pengujian 1 sampai 3)	78