

**Pengamanan Password dan Pesan Pada Aplikasi Chat Messenger  
Berbasis Web Dengan Algoritma AES dan SHA-256**

**Skripsi Sarjana Informatika**

Oleh

Amalia Cahya Putri Alam

183112706470306



**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA  
UNIVERSITAS NASIONAL  
2024**

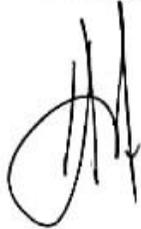
HALAMAN PENGESAHAN  
TUGAS AKHIR

**PENGAMANAN PASSWORD DAN PESAN PADA APLIKASI CHAT  
MESSENGER BERBASIS WEB DENGAN ALGORITMA AES DAN SIA-256**



Amalia Cahya Putri Alam  
183112706470306

Pembimbing 1



Dr. Agung Triayudi, S.Kom., M.Kom  
NIDN. 0419068604

Pembimbing 2



Gatot Soepriyono, S.Si., M.S.M.  
NIDN. 0317047803

## PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa Tugas Akhir dengan judul :

### **PENGAMANAN PASSWORD DAN PESAN PADA APLIKASI CHAT MESSENGER BERBASIS WEB DENGAN ALGORITMA AES DAN SHA-256**

Yang dibuat untuk melengkapi salah satu persyaratan menjadi Sarjana Komputer pada Program Studi Informatika Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional, sebagaimana yang saya ketahui adalah bukan merupakan tiruan atau publikasi dari Tugas Akhir yang pernah diajukan atau dipakai untuk mendapatkan gelar di lingkungan Universitas Nasional maupun perguruan tinggi atau instansi lainnya, kecuali pada bagian – bagian tertentu yang menjadi sumber informasi atau acuan yang dicantumkan sebagaimana mestinya.



Jakarta, 27 Agustus 2024



Amalia Cahya Putri Alam  
NPM: 183112706470306

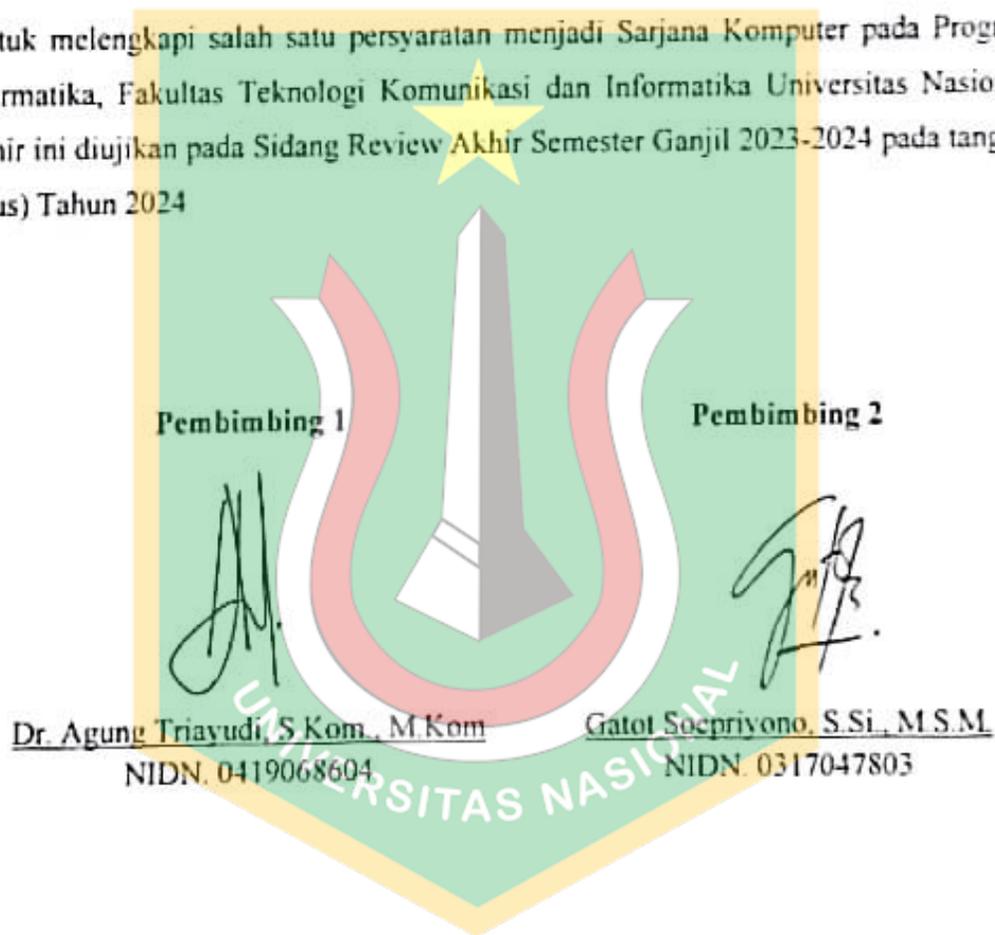


## LEMBAR PERSETUJUAN REVIEW AKHIR

Tugas Akhir dengan judul :

### **PENGAMANAN PASSWORD DAN PESAN PADA APLIKASI CHAT MESSENGER BERBASIS WEB DENGAN ALGORITMA AES DAN SIKA-256**

Dibuat untuk melengkapi salah satu persyaratan menjadi Sarjana Komputer pada Program Studi Informatika, Fakultas Teknologi Komunikasi dan Informatika Universitas Nasional. Tugas Akhir ini diujikan pada Sidang Review Akhir Semester Ganjil 2023-2024 pada tanggal (21 Agustus) Tahun 2024



**Ketua Program Studi**



Ratih Titi Komala Sari, ST., MM., MMSI  
NIDN. 0301038302

**LEMBAR PERSETUJUAN JUDUL YANG TIDAK ATAU YANG DIREVISI**

Nama : Amalia Cahya Putri Alam  
NPM : 183112706470306  
Fakultas/Akademi : Fakultas Teknologi Komunikasi dan Informatika  
Program Studi : Informatika  
Tanggal Sidang : 21 Agustus 2024

JUDUL DALAM BAHASA INDONESIA :

**PENGAMANAN PASSWORD DAN PESAN PADA APLIKASI CHAT  
MESSENGER BERBASIS WEB DENGAN ALGORITMA AES DAN SHA-256**

JUDUL DALAM BAHASA INGGRIS :

**SECURING PASSWORDS AND MESSAGES IN WEB-BASED CHAT  
MESSENGER APPLICATIONS WITH AES AND SHA-256 ALGORITHMS**

**TANDA TANGAN DAN TANGGAL**

<b>Pembimbing 1</b>	<b>Ka. Prodi</b>	<b>Mahasiswa</b>
TGL : 27 Agustus 2024	TGL : 27 Agustus 2024	TGL : 27 Agustus 2024
		

**LEMBAR PERSETUJUAN JUDUL YANG TIDAK ATAU YANG DIREVISI**

Nama : Amalia Cahya Putri Alam  
NPM : 183112706470306  
Fakultas/Akademi : Fakultas Teknologi Komunikasi dan Informatika  
Program Studi : Informatika  
Tanggal Sidang : 21 Agustus 2024

JUDUL DALAM BAHASA INDONESIA :

**PENGAMANAN PASSWORD DAN PESAN PADA APLIKASI CHAT  
MESSENGER BERBASIS WEB DENGAN ALGORITMA AES DAN SHA-256**

JUDUL DALAM BAHASA INGGRIS :

**SECURING PASSWORDS AND MESSAGES IN WEB-BASED CHAT  
MESSENGER APPLICATIONS WITH AES AND SHA-256 ALGORITHMS**

<b>TANDA TANGAN DAN TANGGAL</b>		
<b>Pembimbing 2</b>	<b>Ka. Prodi</b>	<b>Mahasiswa</b>
TGL : 27 Agustus 2024	TGL : 27 Agustus 2024	TGL : 27 Agustus 2024
		

**HALAMAN PENGESAHAN**

**TUGAS SARJANA**

**[ Pengamanan Password dan Pesan Pada Aplikasi Chat Messenger  
Berbasis Web Dengan Algoritma AES dan SHA-256 ]**

Oleh:

[ Amalia Cahya Putri Alam ]  
[ 183112706470306 ]

Program Studi Informatika  
Fakultas Teknologi Komunikasi dan Informatika

Disetujui pada tanggal: [23 Agustus 2024]

Pembimbing 1 Pembimbing 2

[Dr. Agung Triayudi, S.Kom., M.Kom] [Gatot Soepriyono, S.Si., M.S.M.]  
NIDN. 0419068604 NIDN. 0317047803

Penguji 1 Penguji 2

[Dr. Moh. Iwan Wahyuddin, S.T., M.T.] [Nur Hayati, S.Si., M.T.I.]  
NIDN. 0318047004 NIDN. 0316068402



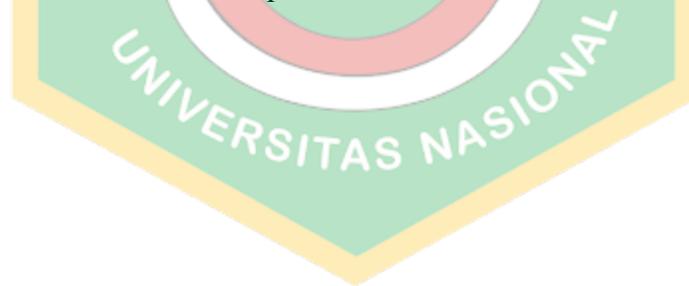
# Pengamanan Password dan Pesan Pada Aplikasi Chat Messenger Berbasis Web Dengan Algoritma AES dan SHA-256

Amalia Cahya Putri Alam – 183112706470306

## Abstrak

Penelitian ini membahas implementasi algoritma Advanced Encryption Standard (AES) dan Secure Hash Algorithm 256 (SHA-256) dalam pengamanan password dan pesan pada aplikasi chat messenger berbasis web. Di era digital saat ini, keamanan data sangat penting, terutama dalam komunikasi melalui aplikasi pesan. Metode enkripsi AES digunakan untuk melindungi pesan yang dikirimkan dari satu pengguna ke pengguna lainnya, sedangkan SHA-256 digunakan untuk mengamankan password pengguna dengan menghasilkan hash yang sulit diretas. Kombinasi kedua algoritma ini menawarkan keamanan yang kuat baik dalam hal penyimpanan maupun transmisi data. Proses enkripsi pesan menggunakan kunci yang dihasilkan secara acak, sehingga pesan tidak dapat diakses oleh pihak yang tidak berwenang. Sementara itu, proses hashing pada password menjamin bahwa password yang disimpan di server tidak dapat dibalikkan menjadi bentuk aslinya, sehingga menambah lapisan keamanan ekstra. Implementasi algoritma ini diuji pada sebuah aplikasi chat berbasis web yang memungkinkan pengguna saling berkomunikasi dengan aman. Hasil uji menunjukkan bahwa penerapan AES dan SHA-256 mampu memberikan perlindungan optimal terhadap serangan pencurian data dan brute force. Sistem ini juga tetap mempertahankan kinerja yang efisien meskipun dengan lapisan keamanan yang tinggi. Dengan demikian, kombinasi enkripsi AES dan hashing SHA-256 direkomendasikan sebagai solusi yang efektif untuk meningkatkan keamanan aplikasi chat messenger berbasis web.

**Kata kunci:** AES, SHA-256, keamanan aplikasi chat



## Kata Pengantar

Puji dan syukur penulis panjatkan kepada Yang Maha Esa yang telah memberikan rahmat dan karunia sehingga penulis dapat menyelesaikan proposal penelitian tugas akhir ini dengan judul **“Pengamanan Password dan Pesan Pada Aplikasi Chat Messenger Berbasis Web Dengan Algoritma AES dan SHA-256”** sebagai salah satu syarat kelulusan program studi Sarjana Komputer Fakultas Teknologi Komunikasi dan Informatika.

Penelitian dan penulisan proposal ini tidak terlepas dari bantuan berbagai pihak, oleh karena itu penulis menyampaikan banyak terimakasih terutama kepada dosen pembimbing tugas akhir yang telah meluangkan banyak waktu, tenaga, pikiran, bimbingan, arahan, motivasi serta memaklumi segala kekurangan penulis selama penelitian tugas akhir dan penyusunan skripsi.

Karena itu dengan ketulusan dan kerendahan hati penulis mengucapkan terima kasih yang tidak terhingga kepada yang terhormat:

1. Tuhan Yang Maha Esa yang telah memberikan rahmat dan hidayah-Nya sehingga laporan dapat terlaksana dengan baik.
2. Dr. El Amry Bermawi Putera, M.A., selaku Rektor Universitas Nasional
3. Ibu Ratih Titi Komala Sari, ST., MM., MMSI, selaku ketua Program Studi Informatika Universitas Nasional.
4. Dr. Agung Triayudi, S.Kom., M.Kom. selaku Dosen Pembimbing satu Laporan Seminar Proposal yang telah meluangkan waktu dan semangatnya selama proses bimbingan.
5. Gatot Soepriyono, S.Si., M.S.M., selaku Dosen Pembimbing dua Laporan Seminar Proposal yang telah meluangkan waktu dan semangatnya selama proses bimbingan.
6. Orang tua serta keluarga yang telah memberikan dukungan dan semangat selama penulis menjalani proses penelitian ini.
7. Rekan-rekan teman yang telah memberi arahan atau koreksi pada isi laporan penulisan jika ada kekurangan di dalamnya.

Penulis menyadari bahwa proposal penelitian tugas akhir ini masih memiliki kekurangan. Karenanya penulis mengharapkan kritik dan saran yang membangun dari pembaca terutama kepada dosen pembimbing untuk perbaikan penulisan laporan di masa yang akan datang.



Jakarta, 27 maret 2023

A handwritten signature in black ink, appearing to be "Amalia Cahya Putri Alam".

Penulis,

Amalia Cahya Putri Alam

NPM. 183112706470306

## Daftar Isi

Kata Pengantar .....	2
Abstrak .....	4
BAB I .....	6
PENDAHULUAN.....	6
1.1. Latar Belakang Masalah. ....	6
1.2. Identifikasi Masalah .....	7
1.3. Rumusan Masalah.....	7
1.4. Batasan Masalah .....	7
1.5. Tujuan dan Manfaat.....	8
BAB II.....	9
Tinjauan Pustaka .....	9
2.1. Chat Messenger.....	9
2.2. Kriptografi .....	9
2.3. Kriptografi Simetris dan Asimetris.....	10
1.4. Fungsi Hash.....	10
1.5. Advanced Encryption Standard.....	11
1.6. Algoritma Cipher Block Chaining.....	14
1.7. Algoritma SHA-256 .....	14
1.8. Avalanche Effect.....	15
BAB III.....	17
Metode Penelitian.....	17
3.1. Waktu Penelitian.....	17
3.2. Fokus Penelitian .....	17
3.3. Teknik Pengumpulan Data.....	17
BAB IV .....	21
Hasil Dan Pembahasan.....	21
4.1. Penerapan algoritma SHA-256.....	23
4.2. Penerapan Algoritma AES-256.....	38
Bab V .....	46
Kesimpulan.....	46
Daftar Pustaka.....	48

