KRIPTOGRAFI AES DAN AUTENTIKASI HMAC UNTUK SISTEM PENGAMANAN PESAN TEKS BERBASIS ANDROID

Diajukan Sebagai Syarat Untuk Menyelesaikan Pendidikan

Program Strata-1 Pada Jurusan Teknik Informatika

Oleh :

Agung Dwi Paradisafa

NIM : 09021282025053

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN SKRIPSI

KRIPTOGRAFI AES DAN AUTENTIKASI HMAC UNTUK SISTEM PENGAMANAN PESAN TEKS BERBASIS ANDROID

Oleh:

Agung Dwi Paradisafa
NIM: 09021282025053

Palembang, 26 Desember 2023

Pembimbing I	Pembimbing II
Osvari Arsalan, S.Kom., M.T.	Kanda Januar Miraswan, M.T.
NIP. 198806282018031001	NIP. 199001092019031012

Mengetahui,

Ketua Jurusan Teknik Informatika

Alyi Syahrini Utami, M.Kom.

NIP. 197812222006042003

TANDA LULUS UJIAN KOMPREHENSIF

Pada hari Jumat tanggal 22 Desember 2023 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Agung Dwi Paradisafa
NIM : 09021282025053
Judul : Kriptografi AES dan Autentikasi HMAC Untuk Sistem Pengamanan Pesan Teks Berbasis Android

Dan dinyatakan **LULUS.**

1. Ketua Penguji

   Desty Rodiah, M.T. .....
   NIP. 198912212020122011

2. Penguji

   Mastura Diana Marieska, M.T. .....
   NIP. 198603212018032001

3. Pembimbing I

   Osvari Arsalan, S.Kom., M.T. .....
   NIP. 198806282018031001

4. Pembimbing II

   Kanda Januar Miraswan, M.T. .....
   NIP. 199001092019031012

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syharini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Agung Dwi Paradisafa
NIM	: 09021282025053
Program Studi	: Teknik Informatika
Judul Skripsi	: Kriptografi AES dan Autentikasi HMAC untuk Sistem Pengamanan Pesan Teks Berbasis Android
Hasil Pengecekan Software *iThenticate/Turnitin*	: 11%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan siapapun.

Inderalaya,04 Desember 2023

Agung Dwi Paradisafa

NIM: 09021282025053

MOTTO DAN PERSEMBAHAN

“Apa yang melewatkanku tidak akan pernah menjadi takdirku, dan apa yang ditakdirkan untukku tidak akan pernah melewatkanku.”

-Umar Bin Khattab-

“Manusia Hanya Budak Untuk Yang dicintainya”

-Seseorang-

“Fus Ro Dah!”

-Dragonborn-

Kupersembahkan Karya tulis ini kepada:

- Kedua orang tua dan keluargaku
- Sahabat dan Teman Sepejuanganku
- Fakultas Ilmu Komputer
- Universitas Sriwijaya

Cryptography AES and HMAC Authentication for Text Message Security System Based on Android

By:
Agung Dwi Paradisafa
09021282025053

ABSTRACT

In the rapidly evolving communication era, the security of text messages has become crucial. The use of efficient and secure cryptographic algorithms, considering the limitations of device resources, is an urgent step to protect user information from unauthorized parties. This research focuses on the integration of the AES cryptographic scheme and HMAC authentication. The goal is to effectively secure text messages in terms of security and authenticity with minimal resources. The study involves texts ranging from 10-100 characters, and the test results indicate that the combination of AES cryptography and HMAC authentication is considered effective as it complies with the Strict Avalanche Effect standard. The addition of authentication also enhances message security without a significant increase in processing time, with average encryption and decryption times of 0.64 ms and 0.45 ms, respectively, compared to using AES cryptography alone, which has times of 0.55 ms and 0.39 ms.

Keywords: message security, text messages, AES, HMAC, Avalanche Effect, Android.

Kriptografi AES dan Autentikasi HMAC untuk Sistem Pengamanan Pesan Teks Berbasis Android.

Oleh:
Agung Dwi Paradisafa
09021282025053

ABSTRAK

Dalam era komunikasi yang berkembang pesat, keamanan pesan teks menjadi krusial. Penggunaan algoritma kriptografi adalah langkah mendesak untuk melindungi informasi pengguna dari pihak yang tidak berwenang, penelitian ini fokus pada penggabungan skema kriptografi AES dan autentikasi HMAC. Tujuannya adalah mengamankan pesan teks secara efektif dari segi keamanan dan keaslian dengan sumber daya yang sedikit. Penelitian menggunakan teks berpanjang 10-100 karakter, dan hasil pengujian menunjukkan bahwa kombinasi kriptografi AES dan autentikasi HMAC dinilai baik karena sesuai dengan standar *Strict Avalanche Effect*. Penambahan autentikasi juga meningkatkan keamanan pesan tanpa peningkatan waktu yang signifikan pada waktu proses enkripsi dan dekripsi, dengan rata-rata waktu enkripsi dan dekripsi yaitu 0,64 ms dan 0,45 ms dibandingkan dengan menggunakan kriptografi AES saja 0,55 ms dan 0.39 ms.

Kata kunci: keamanan pesan, pesan teks, AES, HMAC, *Avalanche Effect*, Android.

KATA PENGANTAR

Penulis ucapkan puji syukur kepada Allah atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir denganjudul "**Kriptografi AES dan Autentikasi HMAC untuk Sistem Pengamanan Pesan Teks Berbasis Android**" dengan baik untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada pihak pihak yang telah berperan memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung dalam menyelesaikan tugas akhir ini. Penulis ingin menyampaikan rasa terima kasih kepada:

1. Kedua orang tuaku, Wahyu Fitroh dan Nurul Hikmawati yang selalu mendoakan serta memberikan dukungan baik moril maupun materil.
2. Bapak Prof. DR. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya beserta jajarannya. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika beserta jajarannya, dan Ibu Mastura Diana Marieska, M.T. selaku Sekretaris Jurusan Teknik Informatika.
3. Bapak Osvari Arsalan, S.Kom., M.T. selaku dosen pembimbing I dan bapak Kanda Januar Miraswan, M.T. selaku pembimbing II yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir
4. Bapak Kanda Januar Miraswan, M.T. selaku dosen pembimbing akademik yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan.
5. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya
6. Mbak Septi, selaku staff administrasi Teknik Informatika Reguler, dan seluruh staff Fakultas Ilmu Komputer Universitas Sriwijaya yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.

7. Seluruh pihak yang telah membantu dalam penyusunan dan penyempurnaan tugas akhir ini yang tidak dapat disebutkan satu persatu.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Indralaya, 26 Desember 2023

Agung Dwi Paradisafa

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini, akan dijelaskan prinsip-prinsip dasar yang menjadi landasan bagi perencanaan penelitian. Aspek-aspek yang akan dibahas melibatkan latar belakang permasalahan penelitian, pembentukan pertanyaan penelitian, tujuan penelitian, dampak positif penelitian, cakupan keterbatasan penelitian, serta tata cara penyusunan laporan secara terstruktur

1.2 Latar Belakang

Dalam menghadapi tuntutan pertumbuhan pesat komunikasi pada era digital ini, perlunya keamanan pesan teks menjadi sangat mendesak. Keamanan pesan tidak hanya terbatas pada perlindungan dari akses tidak sah, tetapi juga melibatkan pencegahan terhadap perubahan atau manipulasi pesan yang dapat membahayakan keamanan informasi pengguna. Karena itulah menjadi suatu kebutuhan kritis untuk melindungi privasi dan integritas informasi terutama pesan teks pengguna. Teknologi kriptografi merupakan salah satu cara untuk melindungi data tersebut, teknologi dapat mengenkripsi pesan sehigga hanya pihak yang berwenang dapat membukanya.

Dalam konteks pengamanan pesan di lingkungan Android, solusi yang diterapkan perlu mempertimbangkan keterbatasan sumber daya perangkat. Oleh karena itu, penggunaan algoritma kriptografi yang tidak hanya efisien dalam

penggunaan sumber daya , tetapi juga baik dalam menyediakan tingkat keamanan yang diperlukan, menjadi krusial. Penerapan solusi kriptografi menjadi sarana utama dalam mengamankan pesan teks, memastikan bahwa pesan tidak dapat diakses oleh pihak yang tidak sah tetapi juga tetap utuh dan tidak mengalami perubahan yang tidak diinginkan.

Kriptografi adalah Teknik mengacak atau membuat informasi menjadi tidak dapat dipahami. Teknik ini berkaitan dengan Teknik matematika yang memiliki kaitan dengan keamanan informasi seperti kerahasiaan, integritas data, dan autentikasi data. Kriptografi sendiri merupakan teknologi yang digunakan untuk hal tersebut. Ketika pengguna menentukan masukan yang dapat berupa format apa saja termasuk teks atau gambar sederhana, lalu masukan tersebut dikonversi menjadi bentuk acak yang dikenal sebagai *cipher text* atau *cipher image.* Proses tersebut dinamakan sebagai enkripsi. Untuk mengkonversi data tersebut pengguna harus menentukan algoritma khusus. Sedangkan proses mengembalikan data asli disebut dengan deskripsi(Jeeva dkk., 2012). Oleh karena itu, kriptografi adalah teknik yang sangat bagus untuk mengamankan suatu data atau informasi.

Dalam dunia kriptografi, terdapat berbagai metode algoritma, di antaranya adalah Standar Enkripsi Lanjutan (AES). Dalam kondisi sistem yang tidak memiliki banyak sumberdaya, AES adalah algoritma yang sering digunakan(Rahman dkk., 2020). AES (*Advance Encyption Standard)* merupakan algoritma pengacakan blok atau biasa disebut *block cipher* yang bergantung pada sturktur jaringan penggantian dan permutasi blok 128 *bits* dengan tiga Panjang kunci opsional yaitu 128 *bit ,* 192 *bit,* dan 256 *bit*. AES sudah lama dikenal sebagai algoritma yang paling efisien

dalam penggunaan sumberdaya dengan kecepatan yang tinggi dan keamanan yang sangat baik(Alassaf dkk., 2017). Pesan atau informasi yang dikirimkan harus memiliki jaminan atas keasliannya dan tidak dimodifikasi. Oleh karena itu, untuk menjamin keaslian data tersebut dibutuhkan metode autentikasi seperti HMAC (*keyed-Hash Message Authentification Code)* yang akan memberikan jaminan keaslian data dengan konsumsi suberdaya yang sedikit(Khemissa & Tandjaoui, 2015).

Dengan merujuk pada konteks diatas, maka metode *Advence Encryption Standart* (AES) dan *Hash-based Messege Authentication Code* (HMAC) merupakan metode yang tepat untuk diimplementasikan pada platform Android karena waktu proses metode ini cukup cepat dan tetap menghasilkan kualitas yang baik.

1.3 Rumusan Masalah

1. Bagaimana cara mengamankan pesan teks dengan baik menggunakan kriptografi AES dan autentikasi HMAC.
2. Seberapa kuat ketahanan algoritma kriptografi AES dalam mengamankan pesan teks.
3. Seberapa efisien proses mengamankan pesan teks dengan menggunakan algoritma kriptografi AES dan autentikasi HMAC.

1.4 Tujuan Penelitian

Berikut merupakan beberapa tujuan dari penelitian ini:

1. Mengembangkan program yang menerapkan sistem keamanan dan verifikasi keaslian pesan teks menggunakan algoritma kriptografi AES serta autentikasi HMAC pada platform Android.
2. Mengukur kualitas kekuatan serta tingkat ketahanan pesan teks yang telah dilindungi oleh algoritma kriptografi AES dengan memanfaatkan Avalanche Effect.
3. Mengukur efisiensi dalam proses mengamankan pesan teks dengan menggunakan algoritma kriptografi AES dan juga autentikasi HMAC dengan memfokuskan pada pengukuran waktu proses.

1.5 Manfaat Penelitian

Berikut manfaat dari penelitian ini:

1. Menghasilkan perangkat lunak yang menerapkan metode pengaman pesan teks dengan algoritma kriptografi AES & autentikasi HMAC.
2. Mengetahui sebaik apa protokol pengaman pesan teks dengan mengimplentasikan algoritma kriptografi AES & autentikasi HMAC guna menjaga keaslian pesan teks pengguna.
3. Mengetahui efisiensi waktu proses yang dibutuhkan dalam proses mengamankan pesan teks dengan menggunakan algoritma kriptografi AES dan juga autentikasi HMAC

4. Menjadi rujukan yang berharga untuk penelitian – penelitian kriptografi selanjutnya.

1.6 Batasan Masalah

Berikut merupakan batasan - batasan masalah pada penelitian ini:

1. Metode kriptografi atau algoritma yang digunakan pada pesan teks adalah AES.
2. Metode autentikasi yang digunakan adalah HMAC dengan fungsi *hash* SHA256.
3. Pada algoritma kriptografi Advanced Encryption Standard (AES), ukuran blok yang digunakan untuk mengenkripsi data adalah sebesar 128 bit. Selain itu, ukuran kunci yang digunakan dalam enkripsi adalah 32 karakter dalam bentuk bilangan heksadesimal dan 24 karakter dalam format base64.
4. Skenario *Avalance Effect* dilakukan pada pesa teks yang hanya berbeda 1 karakter.
5. Proses enkripsi dan dekripsi dilakukan tanpa mengirimkan pesan.

1.7 Sistematika Penelitian

BAB I. PENDAHULUAN

Bab ini menguraikan konteks latar belakang studi, perumusan permasalahan, tujuan penelitian, kebermanfaatan hasil penelitian, keterbatasan lingkup penelitian, dan tata cara penyajian naskah pada riset ini.

BAB II. KAJIAN LITERATUR

Pada bab ini, akan dibahas mengenai konteks latar belakang penelitian, penentuan permasalahan penelitian, tujuan penelitian, dampak positif hasil penelitian, cakupan pembatasan penelitian, dan susunan penyajian naskah pada riset ini.

BAB III. METODE PENELITIAN

Bab ini membicarakan langkah-langkah yang dilibatkan dalam penelitian tugas akhir. Rencana tahapan penelitian diuraikan melalui struktur kerangka kerja dan pengelolaan proyek penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab ini membicarakan langkah-langkah yang terlibat dalam proses pengembangan perangkat lunak untuk sistem keamanan pesan teks yang memanfaatkan kriptografi AES dan autentikasi HMAC, dengan fokus pada implementasi pada platform Android.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab ini akan mengulas mengenai output yang dihasilkan dari pengembangan perangkat lunak. Kesimpulan yang dapat ditarik dari penelitian ini akan didasarkan pada hasil analisis yang telah dilakukan.

BAB VI. KESIMPULAN DAN SARAN

Bab ini akan mengulas rangkuman dari bab sebelumnya dan memberikan rekomendasi yang dapat bermanfaat berdasarkan temuan dalam penelitian ini.

1.8 Kesimpulan

Berdasarkan pembahasan diatas, peneliti akan mengembakan sebuah perangkat lunak pengamanan pesan teks menggunakan kriptografi AES dan autentikasi HMAC dengan fungsi hash SHA256 yang berbasis Android.

DAFTAR PUSTAKA

Alassaf, N., Alkazemi, B., & Gutub, A. (2017). APPLICABLE LIGHT-WEIGHT CRYPTOGRAPHYTOSECURE MEDICAL DATA IN IOT SYSTEMS. *Journal of Research in Engineering and Applied Sciences*, *02*(02), 50–58. https://doi.org/10.46565/jreas.2017.v02i02.002

Amin, M. M. (2017). IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS. *Pseudocode*, *3*(2), 129–136. https://doi.org/10.33369/pseudocode.3.2.129-136

Calista, D., Farissi, A., & Marieska, M. D. (2021). Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android. *JUPITER: Jurnal Penelitian Ilmu dan Teknologi Komputer*, *13*(2), 220–226. https://doi.org/10.5281/3927.jupiter.2021.10

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer*, *3*(2), 253. https://doi.org/10.14710/jtsiskom.3.2.2015.253-258

Hamouda, B. E. H. H. (2020). Comparative Study of Different Cryptographic Algorithms. *Journal of Information Security*, *11*(03), 138–148. https://doi.org/10.4236/jis.2020.113009

Hutahaean, D. J., Wardani, N. H., & Purnomo, W. (2019). Pengembangan Sistem Informasi Penyewaan Gedung Berbasis Web dengan Metode Rational Unified Process (RUP) (Studi Kasus: Wisma Rata Medan). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *3*(6), 5789–5798.

Ichwan, M., Gustian, M., & Nurjaman, N. R. (2018). Implementasi Keyed-Hash Message Authentatication Code Pada Sistem Keamanan Rumah. *MIND Journal*, *1*(1), 9. https://doi.org/10.26760/mindjournal.v1i1.9

Jeeva, A., Palanisamy, D. V., & Kanagaram, K. (2012). COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS. *International Journal of Engineering Research And*, *2*(3), 3033–3037.

Kaffah, F. M., Gerhana, Y. A., Huda, I. M., Rahman, A., Manaf, K., & Subaeki, B. (2020). E-Mail Message Encryption Using Advanced Encryption Standard (AES) and Huffman Compression Engineering. *2020 6th International Conference on Wireless and Telematics (ICWT)*, 1–6. https://doi.org/10.1109/ICWT50448.2020.9243651

Khemissa, H., & Tandjaoui, D. (2015). A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. *2015 9th*

International Conference on Next Generation Mobile Applications, Services and Technologies, 90–95. https://doi.org/10.1109/NGMAST.2015.31

Pairin, Y. B. (2018). Kode Autentikasi Hash pada Pesan Teks Berbasis Android. *Eksplora Informatika*, *8*(1), 6. https://doi.org/10.30864/eksplora.v8i1.129

Rahman, A. G. A., Pramukantoro, E. S., & Amron, K. (2020). Implementasi Mekanisme End-To-End Security Menggunakan Algoritma AES dan HMAC pada Pengiriman Data Sensor ECG Berbasis LoRa. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *4*(1), 166–173.

Windya, P. A., Suryani, V., & Wardana, A. A. (2021). Penerapan Keamanan Komunikasi pada Jaringan LoRa(Long Range) Menggunakan Algoritma Advanced Encryption Standard(AES) dan Message Authentication Code(MAC). *Jurnal Tugas Akhir Fakultas Informatika*, *8*(2), 3406.