IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128, BASE 64 DAN HASHING BCRYPT DALAM MENGAMANKAN PESAN RAHASIA BERBASIS ANDROID

SKRIPSI

Diajukan sebagai Salah Satu Syarat Untuk Memperoleh Kelulusan
Jenjang Strata Satu pada Program Studi Teknik Informatika

Oleh
Wahyu Albara
2155201105

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH BENGKULU
2025

LEMBAR PERSETUJUAN

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128, BASE 64 DAN HASHING BCRYPT DALAM MENGAMANKAN PESAN RAHASIA BERBASIS ANDROID

Oleh
Wahyu Albara
2155201105

Tugas Akhir Ini Telah Diterima dan Disahkan
untuk Memenuhi Persyaratan Mencapai Gelar
SARJANA KOMPUTER(S.Kom)

Pada
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK UNIVERSITAS MUHAMMADIYAH BENGKULU

Bengkulu, 4 Agustus 2025
Disetujui Oleh

Ketua Program Studi,	Dosen Pembimbing,
Ardi Wijaya, S.Kom., M.Kom	Gunawan, S.Kom., M.Kom
NP. 198805112014081181	NIDN. 0203078903

LEMBAR PERSETUJUAN HASIL REVISI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128, BASE 64 DAN HASHING BCRYPT DALAM MENGAMANKAN PESAN RAHASIA BERBASIS ANDROID

Oleh
Wahyu Albara
2155201105

Telah Melakukan Revisi Sesuai dengan Perubahan
dan Perbaikan yang Diminta Pada Saat Sidang Tugas Akhir

Bengkulu, 4 Agustus 2025
Menyetujui

No	Nama Dosen	Keterangan	Tanda Tangan
1	Harry Witriyono, S.P., M.Kom	Ketua Penguji	
2	Muhammad Imanullah, S.Kom., M.Kom	Penguji 1	
3	Gunawan, S.Kom., M.Kom	Penguji 2	

Mengetahui
Ketua Program Studi Teknik Informatika

Ardi Wijaya, S.Kom., M.Kom
NP. 198895112014081181

LEMBAR PENGESAHAN

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128, BASE 64 DAN HASHING BCRYPT DALAM MENGAMANKAN PESAN RAHASIA BERBASIS ANDROID

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Kelulusan
Jenjang Strata Satu Pada Program Studi Teknik Informatika

Oleh
Wahyu Albara
2155201105

Bengkulu, 4 Agustus 2025

No	Nama Dosen	Keterangan	Tanda Tangan
1	Harry Witriyono, S.P., M.Kom	Ketua Penguji	
2	Muhammad Imanullah, S.Kom., M.Kom	Penguji 1	
3	Gunawan, S.Kom., M.Kom	Penguji 2	

Mengesahkan
Dekan Fakultas Teknik

RG Guntur Alam, M.Kom,. Ph.D
NP. 19730101 200004 1 040

SURAT PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	:Wahyu Albara
NPM	:2155201105
Program Studi	:Teknik Informatika
Fakultas	:Teknik

Dengan ini saya menyatakan bahwa Skripsi yang saya tulis dengan judul **"IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128, BASE 64 DAN HASHING BCRYPT DALAM MENGAMANKAN PESAN RAHASIA BERBASIS ANDROID"** merupakan hasil karya saya sendiri bukan plagiat dan skripsi orang lain kecuali kutipan yang sumbernya dicantumkan. Apabila dikemudian hari pernyataan saya ini tidak benar, maka saya bersedia menerima sanksi akademis yang berlaku (di cabut predikat kelulusan dan kesarjanaanya). Demikian Surat Pernyataan ini saya buat dengan sebenarnya, tanpa paksaan dari pihak manapun.

Bengkulu, 4 Agustus 2025

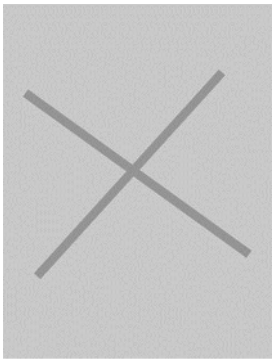
Menyatakan,

WAHYU ALBARA

NPM. 2155201105

DAFTAR RIWAYAT HIDUP

1. Data Pribadi



Nama	:	Wahyu Albara
TTL	:	Palembang, 29 November 2002
Agama	:	Islam
Anak ke	:	1 / Tunggal
Alamat	:	JL, Iskandar Baksir

2. Identitas Orang Tua

Nama Ayah	:	Yudison
Pekerjaan	:	Wiraswasta
Nama Ibu	:	Neni
Pekerjaan	:	Wiraswasta

3. Riwayat Pendidikan

1.	SD N 18 Bengkulu Selatan	:	2008-2014
2.	SMP Negeri 1 Bengkulu Selatan	:	2014-2017
3.	SMK Negeri 1 Bengkulu Selatan	:	2017-2020
4.	Universitas Muhammadiyah Bengkulu	:	2021-2025

MOTTO DAN PERSEMBAHAN

MOTTO

"Apapun yang terjadi pulanglah sebagai Sarjana"

PERSEMBAHAN

Skripsi ini saya persembahkan kepada:

ABSTRAK

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128, BASE 64 DAN HASHING BCRYPT DALAM MENGAMANKAN PESAN RAHASIA BERBASIS ANDROID

NAMA : Wahyu Albara

NPM : 2155201105

PEMBIMBING : Gunawan, S.Kom,. M.Kom

Dalam era digital yang terus berkembang, keamanan data menjadi aspek yang sangat penting, terutama dalam pengiriman pesan melalui perangkat mobile. Komunikasi yang tidak aman dapat menyebabkan kebocoran informasi, penyalahgunaan data, dan pelanggaran privasi. Oleh karena itu, dibutuhkan sistem yang mampu melindungi isi pesan dari akses pihak yang tidak berwenang. Penelitian ini bertujuan untuk mengimplementasikan tiga metode pengamanan data digital, yaitu algoritma kriptografi AES-128, encoding Base64, dan hashing Bcrypt dalam satu aplikasi Android. Algoritma **AES-128** digunakan untuk melakukan enkripsi isi pesan sehingga tidak dapat dibaca oleh pihak lain tanpa kunci enkripsi yang sesuai. Hasil enkripsi kemudian dikonversi ke dalam format teks menggunakan **Base64 encoding**, agar lebih kompatibel untuk ditransmisikan dan disimpan dalam sistem. Selain itu, pesan yang telah dienkripsi juga diproses melalui **hashing Bcrypt** guna menjamin integritas dan keaslian data, serta mencegah terjadinya manipulasi isi pesan tanpa izin. Metode yang digunakan dalam penelitian ini adalah rekayasa perangkat lunak, dengan pendekatan pengembangan aplikasi Android menggunakan framework tertentu. Pengujian dilakukan melalui simulasi proses enkripsi, dekripsi, encoding, dan hashing terhadap pesan teks dalam aplikasi. Hasil implementasi menunjukkan bahwa ketiga teknik tersebut dapat bekerja secara terpadu untuk menjaga kerahasiaan, integritas, dan keamanan pesan. Dengan pendekatan ini, pesan tidak hanya dienkripsi, tetapi juga dijamin tidak mengalami perubahan isi saat dikirimkan. Aplikasi yang dibangun diharapkan dapat menjadi solusi praktis dalam menjaga privasi komunikasi digital pengguna, serta dapat dijadikan referensi bagi pengembangan sistem keamanan informasi lainnya pada platform Android.

Kata Kunci: Kriptografi, AES-128, Base64, Bcrypt, Android, Keamanan Pesan

ABSTRACT

Implementation of AES-128 Cryptographic Algorithm, Base64, and Bcrypt Hashing for Securing Confidential Messages on Android-Based Applications

Name : Wahyu Albara

NPM : 2155201105

Advisor : Gunawan, S.Kom,. M.Kom

In the rapidly evolving digital era, data security has become a critical concern, especially in message transmission through mobile devices. Unsecured communication may lead to information leakage, data misuse, and violations of user privacy. Therefore, it is essential to design a system capable of protecting message content from unauthorized access. This study aims to implement three different digital data protection methods—AES-128 encryption, Base64 encoding, and Bcrypt hashing—into a single Android-based application. The ***AES-128 algorithm*** *is used to encrypt the message content so that it cannot be read without the appropriate encryption key. The encrypted data is then converted into readable text format using* ***Base64 encoding*** *to ensure compatibility for transmission and storage within the system. Additionally, the encrypted message is hashed using* ***Bcrypt*** *to verify the integrity and authenticity of the message, ensuring that no unauthorized modifications have occurred. The research method used is software engineering with a mobile application development approach. Testing was carried out through simulation of encryption, decryption, encoding, and hashing processes on text messages within the application. The results demonstrate that the integration of these three cryptographic techniques is effective in maintaining the confidentiality, integrity, and overall security of messages. This layered security approach ensures that the message is not only encrypted but also remains unchanged throughout transmission. The developed application is expected to serve as a practical solution for maintaining user privacy in digital communication and may also serve as a reference for the development of other information security systems on the Android platform.*

Keywords: *Cryptography, AES-128, Base64, Bcrypt, Android, Message Security*

KATA PENGANTAR

Assalamu'alaikum Warohmatullahi Wabarokatuh.

Puji syukur penulis ucapkan kehadirat Allah Subhanahu Wa Ta'ala, atas berkat, rahmat, ridho dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Algoritma Kriptografi Aes-128, Base 64 Dan Hashing Bcrypt Dalam Mengamankan Pesan Rahasia Berbasis Android" Pada kesempatan ini penulis mengucapkan rasa terima kasih yang sebesar-besarnya kepada :

1. Bapak RG Guntur Alam, M.Kom.,Ph.D selaku Dekan Fakultas Teknik Universitas Muhammadiyah Bengkulu
2. Bapak Ardi Wijaya, S. Kom,. M. Kom selaku Ketua Program Studi Teknik Informatika Universitas Muhammadiyah Bengkulu
3. Bapak Gunawan, S.Kom,. M.Kom. selaku Dosen Pembimbing dalam penyusunan skripsi
4. Keluarga tercinta yang telah memberikan dukungan moral maupun materi.
5. Sahabat dan teman-teman seperjuangan Teknik Informatika yang selalu memberikan inspirasi, motivasi dan selalu meluangkan waktunya ketika penulis dalam kesulitan.

Penulis menyadari bahwa dalam penyusunan skripsi ini jauh dari kata sempurna Untuk itu saran dan kritik yang bersifat membangun penulis sangat harapkan demi penyempurnaan di masa yang akan datang.

Semoga skripsi ini bermanfaat bagi penulis dan pembaca sekalian. Aamiin.

Wassalamu'alaikum Warohmatullahi Wabarokatuh.

Bengkulu, 4 Agustus 2025

Wahyu Albara

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang pesat di era digital saat ini telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam bidang pendidikan, komunikasi, industri, dan layanan publik. Inovasi seperti internet, kecerdasan buatan, dan perangkat mobile telah mempermudah akses informasi serta meningkatkan efisiensi kerja. Kemajuan ini juga mendorong masyarakat untuk terus beradaptasi dengan teknologi agar tidak tertinggal, sehingga peran teknologi menjadi sangat penting dalam mendukung kemajuan peradaban dan peningkatan kualitas hidup manusia.

Kemajuan di bidang komunikasi data dan jaringan komputer telah memungkinkan ribuan orang untuk melakukan komunikasi dengan beragam teknologi perangkat keras dan perangkat lunak. Di sisi lain terdapat ancaman yang membayangi kemajuan tersebut, yaitu aspek keamanan data dan informasi. Sistem keamanan data diperlukan untuk melindungi data dan informasi yang ditransmisikan melalui jaringan komunikasi. Salah satu mekanisme untuk menyediakan layanan keamanan data adalah teknik kriptografi. Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya

tulisanKriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi Dalam kriptografi, data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa dengan teknik enkripsi sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak.(Amin, 2020) Data yang akan dikirimkan dan belum mengalami penyandian dikenal dengan istilah plaintext, dan setelah disamarkan dengan suatu cara penyandian, maka plaintext ini akan berubah menjadi ciphertext. Sebelum adanya komputer, kriptografi dilakukan dengan algoritma berbasis karakter. Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi, algoritma-algoritma tersebut sering diistilahkan dengan algoritma kriptografi klasik. Pada penelitian ini diimplementasikan kriptografi klasik sebagai metode untuk melakukan proses enkripsi dan dekripsi data teks yang dikirimkan melalui aplikasi chat. Dari proses pengujian diperoleh bahwa proses enkripsi dan dekripsi dapat menjaga kerahasiaan data.(Eril Obeit Choiri, 2020)

Dalam pengamanan data digital, algoritma kriptografi seperti AES-128, Base64 encoding, dan hashing Bcrypt telah menjadi komponen penting dalam mengamankan pesan pada platform mobile. AES-128 menawarkan metode enkripsi simetris yang kuat dengan efisiensi tinggi untuk perangkat terbatas seperti smartphone. Sementara itu, Base64 digunakan untuk memastikan kompatibilitas data terenkripsi saat dikirim melalui media berbasis teks, dan Bcrypt berfungsi memperkuat keamanan autentikasi pengguna dengan teknik hashing yang tahan

terhadap serangan brute force. Studi terbaru menunjukkan bahwa kombinasi teknik ini mampu meningkatkan tingkat keamanan data, meskipun implementasi pada perangkat bergerak harus memperhatikan optimasi performa agar tidak membebani sistem (Al Farissi; Arya Pradata; Kanda Miraswan, 2020)

1.2 Pertanyaan Penelitian

Bagaimana cara mengimplementasikan algoritma kriptografi AES-128, encoding Base64, dan hashing Bcrypt, dalam mengamankan pesan rahasia berbasis Android ?

1.3 Tujuan Penelitian

1. Untuk mengimplementasikan ketiga algoritma, yaitu algoritma AES-128, algoritma Base64, serta algoritma hashing Bcrypt untuk enkripsi dan dekripsi pesan guna meningkatkan keamanan pesan rahasia secara terpisah ke dalam fitur-fitur yang berbeda dalam satu aplikasi Android.
2. Untuk membangun aplikasi Android yang mampu mengamankan pengiriman pesan rahasia dengan menggunakan pendekatan kriptografi tersebut

1.4 Kerangka Kerja Penelitian

FASE	Uraian Kegiatan	Input	Output
1	Analisis Kebutuhan	Observasi, Studi Pustaka, Spesifikasi system	1. berbagai jenis pesan teks yang umumnya digunakan dalam komunikasi sehari-hari di aplikasi whatssapp. 2. Beberapa jurnal atau penelitian terkait kriptografi 3. Laptop Lenovo Thinkpad X1 Carbon dengan prosesor Intel Core i5 dan RAM 8GB

2	Desain Sistem	Merancang antarmuka pengguna (UI) dan pengalaman pengguna (UX) menggunakan ionic untuk aplikasi berbasis Android.	Halaman depan atau dashboard pada Aplikasi
3	Implementasi	Rancangan sistem, algoritma kriptografi (AES, Base64, Bcrypt)	Aplikasi Android versi awal dengan 3 fitur keamanan terpisah.yang dimana screen pertama akan berisi dashboard, screen kedua implementasi Algoritma AES 128, screen ketiga implementasi Algoritma Base64, dan keempat implementasi algoritma hashing Bcrypt
4	Pengujian	Aplikasi hasil implementasi, skenario pengujian.	Setelah proses implementasi selesai, dilakukan pengujian terhadap aplikasi enkripsi pesan berbasis Android yang telah dibuat menggunakan platform Kodular. Pengujian dilakukan untuk memastikan bahwa algoritma dapat bekerja dengan baik dalam (enkripsi) dan mengembalikan (dekripsi) pesan ke bentuk aslinya.
5	Pemeliharaan	Melakukan perbaikan jika ada bug serta pembaruan versi jika diperlukan.	Aplikasi lebih stabil dan siap dikembangkan lebih lanjut.

1. 1 Tabel Kerangka Kerja Penelitian