LEMBAR PENGESAHAN

Skripsi yang berjudul **"IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) 128 BIT UNTUK PROSES ENKRIPSI DAN DESKRIPSI PESAN TEKS"**

()

Oleh

FITRI ASIALI
NIM. 412418027

Program Studi Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam

Telah dipertahankan di depan dewan penguji

Hari, tanggal	:	**Selasa, 20 Desember 2022**
Waktu	:	**12.30-14.00 WITA**
Tempat	:	**Ruang Sidang Matematika**

	Dewan Penguji		**Tanda Tangan**
1.	**Dra. Lailany Yahya, M. Si** NIP. 196812191994032001	Penguji Utama	(.....)
2.	**Asriadi, S.Pd., M.Si** NIP. 198910282020121015	Anggota	(.....)
3.	**Nurwan, S.Pd., M.Si** NIP. 198105102006041002	Anggota	(.....)
4.	**Djihad Wungguli, S.Pd., M.Si** NIP. 198906122019031018	Anggota	(.....)
5.	**Nisky Imansyah Yahya, S.Pd., M.Si** NIP. 199107302020121008	Anggota	(.....)

Mengetahui,
Dekan Fakultas Matematika dan IPA

Prof. Dr. Astin Lukum, M.Si
NIP. 196303271988032002

Dipindai dengan CamScanner

ABSTRAK

FITRI ASIALI, 2022. *IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) 128 BIT UNTUK PROSES ENKRIPSI DAN DESKRIPSI PESAN TEKS ().* **SKRIPSI.** Gorontalo. Program Studi Matematika. Jurusan Matematika. Fakultas Matematika dan Ilmu Pengetahuan Alam. Universitas Negeri Gorontalo.
Pembimbing : **(1) Dra. Lailany Yahya, M.Si, (2) Asriadi, S.Pd., M.Si**

AES merupakan algoritma yang memiliki kemampuan untuk menangani 128 bit (16 byte) sebagai ukuran blok plaintext. 16 byte ini membentuk matriks yang berukuran 4x4. Adaupun fitur penting yang ada di AES terletak pada nomor dari putaran, dimana panjang kunci bergantung pada jumlah putaran. Variasi panjang kunci yang digunakan dalam proses enkripsi dan deskripsi algoritma ini terdiri dari 128 bit, 192 bit, dan 256 bit. Kunci 128 bit memerlukan 10 putaran, 192 bit memerlukan 12 putaran, dan kunci 256 bit memerlukan 14 kali putaran. Penelitian ini bertujuan untuk Mengimplementasikan *Algoritma Advanced Encryption Standard* (AES) terkait tentang kemanan dan kerahasiaan pesan teks dengan menggunakan panjang kunci 128 bit pada aplikasi *visual studio code*. Terkait dengan masalah yang ada dan pentingnya tentang pengamanan pesan teks, maka dalam penelitian ini akan direncanakan untuk mengimplementasikan konsep pengamanan isi pesan teks untuk melindungi pesan dan informasi penting agar tidak mudah dibaca dan demi menjaga kerahasiaan pesan teks tersebut. Pada penelitian ini, akan membahas keamanan dan kerahasiaan pesan menggunakan algoritma AES dengan panjang kunci 128 bit. Dimana pada proses enkripsi dan deskripsi pada penelitian ini menggunakan proses software pada *visual studio code*. Berdasarkan hasil penelitian menunjukkan bahwa algoritma AES dapat digunakan dalam menjaga kerahasiaan pesan teks.

Kata Kunci: *Kriptografi, Algoritma AES, Visual Studio Code*

Dipindai dengan CamScanner

ABSTRACT

FITRI ASIALI, 2022. *CRYPTOGRAPHY IMPLEMENTATION USING 128 BIT ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM FOR TEXT MESSAGE ENCRYPTION AND DESCRIPTION ().* **UNDERGRADUATE THESIS.** Gorontalo. Study Program of Mathematics. Department of Mathematics. Faculty of Mathematics and Natural Sciences. Universitas Negeri Gorontalo.
The Principal Supervisor: **Dra. Lailany Yahya, M.Si,** the Co-supervisor: **Asriadi, S.Pd., M.Si**

AES is an algorithm that has the ability to handle 128 bits (16 bytes) as a plaintext block size. These 16 bytes form a 4X4 matrix. The important feature of AES lies in the number of rounds, where the key length depends on the number of rounds. Variations in the key length used in the encryption process and description of this algorithm consist of 128 bits, 192 bits, and 256 bits. A 128 bit key requires 10 rounds, a 192 bit key requires 12 rounds, and a 256 bit key requires 14 rounds. This study aimed to implement the Advanced Encryption Standard (AES) algorithm in regard to the security and confidentiality of text messages using a 128-bit key length in the visual studio code application. In regards to the existing problems and the importance of securing text messages, in this research, it was planned that the concept of security for text messages to protect important messages and information would be implemented so that they would not be easy to be read and for the sake of maintaining the confidentiality of these text messages. In this study, we discussed the security and confidentiality of messages using the AES algorithm with a key length of 128 bits. The process of encryption and description in this study used the software process in visual studio code. Based on the results of the research, it was shown that the AES algorithm could be used to maintain the confidentiality of text messages.

Keywords: *Cryptography, AES Algorithm, Visual Studio Code*

UPT. BAHASA

Dipindai dengan CamScanner