# KRIPTOGRAFI *SYMMETRIC-KEY* DENGAN METODE AES *(ADVANCED ENCRYPTION STANDARD)* 256 *BIT*

**SKRIPSI**

*Diajukan sebagai salah satu persyaratan guna memperoleh gelar*

*Sarjana Sains*


**OLEH :**

**SILVIA YOLLA**
**NIM 16030084**

**PROGRAM STUDI MATEMATIKA**

**JURUSAN MATEMATIKA**

**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**

**UNIVERSITAS NEGERI PADANG**


**2022**

# PERSETUJUAN SKRIPSI

| | |
|---|---|
| Judul | : Kriptografi *Symmetric-Key* dengan Metode AES (*Advanced Encryption Standard*) 256 Bit |
| Nama | : Silvia Yolla |
| NIM / TM | : 16030084/2016 |
| Program Studi | : Matematika |
| Departemen | : Matematika |
| Fakultas | : Matematika dan Ilmu Pengetahuan Alam |

Padang, 4 Januari 2022

Disetujui Oleh

Pembimbing

Muhammad Subhan, S.Si, M.Si
NIP. 19701126 199903 1 002

## HALAMAN PENGESAHAN LULUS UJIAN SKRIPSI

| | |
|---|---|
| Nama | : Silvia Yolla |
| NIM / TM | : 16030084/2016 |
| Program Studi | : Matematika |
| Departemen | : Matematika |
| Fakultas | : Matematika dan Ilmu Pengetahuan Alam |

Dengan Judul Skripsi

**Kriptografi *Symmetric-Key* dengan Metode AES*(Advanced Encryption Standard)* 256 *Bit***

Dinyatakan lulus setelah dipertahankan di depan Tim Penguji Skripsi
Program Studi Matematika Departemen Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Negeri Padang

Padang, 4 Januari 2022

Tim Penguji

| | Nama | Tanda Tangan |
|---|---|---|
| Ketua | : Muhammad Subhan, S.Si, M.Si | |
| Anggota | : Defri Ahmad, S.Pd, M.Si | |
| Anggota | : Drs. Yusmet Rizal, M.Si | |

# SURAT PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

| | |
|---|---|
| Nama | : Silvia Yolla |
| NIM | : 16030084 |
| Program Studi | : Matematika |
| Departemen | : Matematika |
| Fakultas | : Matematika dan Ilmu Pengetahuan Alam |

Dengan ini menyatakan, bahwa skripsi saya dengan judul "Kriptografi *Symmetric-Key* dengan Metode AES *(Advanced Encryption Standard)* 256 Bit" adalah benar merupakan hasil karya saya dan bukan merupakan plagiat dari karya orang lain atau pengutipan dengan cara-cara yang tidak sesuai dengan etika yang berlaku dalam tradisi keilmuan. Apabila suatu saat terbukti saya melakukan plagiat maka saya bersedia diproses dan menerima sanksi akademis maupun hukum sesuai dengan hukum dan ketentuan yang berlaku, baik di institusi UNP maupun di masyarakat dan negara.

Demikianlah pernyataan ini saya buat dengan penuh kesadaran dan rasa tanggung jawab sebagai anggota masyarakat ilmiah.

Padang, 4 januari 2022

Diketahui oleh,
Ketua Departemen Matematika,

Dra. Media Rosha, M.Si
NIP. 19620815 199703 2 004

Saya yang menyatakan,


Silvia yolla
NIM. 16030084

# Kriptografi *Symmetric-Key* dengan Metode AES *(Advanced Encryption Standard)* 256 *bit*

**Silvia Yolla**

## ABSTRAK

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan keamanan informasi. Dalam penerapannya, kriptografi merupakan suatu metode enkripsi atau penyandian data yang hanya diketahui oleh sekelompok pengguna tertentu. Tujuan penelitian ini yaitu untuk mendeskripsikan proses enkripsi dan dekripsi pada pesan teks dengan metode AES 256 bit.

Metode yang digunakan adalah metode deskriptif yaitu membahas permasalahan yang berlandaskan tinjauan pustaka. Penelitian ini dimulai dengan mencari key schedule, setelah itu dilakukan proses enkripsi dan proses dekripsi. Algoritma Rijndael memiliki karakteristik istimewa karena setiap ronde mengalami proses *AddRoundKey, SubBytes, ShiftRows,* dan *MixColumns.*

Pada pembahasan dibuktikan bahwa teks yang di enkripsi akan menjadi bilangan heksadesimal yang kalau diubah ke dalam bentuk karakter akan menjadi simbol-simbol tidak jelas dan jika di dekripsikan dengan kunci yang sama akan kembali ke bentuk teks awal. AES dengan kunci 256 yang melakukan putaran sebanyak 14 round sehingga ekspansi kunci semakin besar dan semakin sulit untuk dipecahkan.

**Kata Kunci :** Kriptografi, AES (Advanced Encryption Standard), Enkripsi, Dekripsi, Rijndael.

**Kriptografi *Symmetric-Key* dengan Metode AES *(Advanced Encryption Standard)* 256 *bit***

**Silvia Yolla**

## ABSTRACT

Cryptography is a mathematical study that has a relationship with information security. In its application, cryptography is a method of encrypting or encoding data that is only known by a certain group of users. The purpose of this study is to describe the process of encryption and decryption of text messages using the AES 256 bit method.

The method used is a descriptive method, namely discussing problems based on a literature review. This research begins by looking for the key schedule, after that the encryption and decryption processes are carried out. Rijndael's algorithm has special characteristics because each round undergoes AddRoundKey, SubBytes, ShiftRows, and MixColumns processes.

In the discussion, it is proven that the encrypted text will be a hexadecimal number which if converted into character form will become unclear symbols and if it is decrypted with the same key it will return to the initial text form. AES with 256 keys that do 14 rounds so that the key expansion gets bigger and more difficult to solve.

**Keywords** : Cryptography, AES (Advanced Encryption Standard), Encryption, Decryption, Rijndael.

# KATA PENGANTAR

Segala puji hanya milik Allah SWT, atas segala karunia, rahmat, taufik serta hidayat-Nya sehingga penulis dapat menyelesaikan Skripsi yang berjudul **"Kriptografi *Symmetric-Key* dengan metode AES *(Advanced Encryption Standard)* 256 *bit*"** dengan baik. Shalawat beriringan salam penulis sampaikan kepada Rasulullah, Nabi Muhammad SAW sebagai suri teladan bagi umat manusia.

Skripsi ini disusun guna memenuhi syarat memperoleh gelar Sarjana Sains Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Padang. Dalam penyusunan skripsi ini, penulis banyak mendapatkan bantuan dan dukungan berupa dorongan semangat, nasihat, bimbingan, dan kerja keras dari berbagai pihak, oleh sebab itu penulis ingin mengucapkan terimakasih kepada :

1. Bapak Muhammad Subhan, S.Si, M.Si sebagai Dosen Pembimbing sekaligus Penasehat Akademik.
2. Bapak Defri Ahmad, S.Pd, M.Si sebagai Dosen Penguji.
3. Bapak Drs. Yusmet Rizal, M.Si sebagai Dosen Penguji.
4. Ibu Dra. Media Rosha, M.Si sebagai Ketua Jurusan Matematika dan Ketua Program Studi Matematika FMIPA UNP.
5. Bapak dan Ibu Dosen Matematika yang telah memberikan ilmu kepada penulis.
6. Segenap Karyawan dan Laboran Jurusan Matematika FMIPA UNP.
7. Mama, Papa, dan Keluarga Besar yang telah mendoakan, memberi semangat, nasehat, materi dalam menyelesaikan skripsi ini.
8. Sahabat dan rekan-rekan semua yang turut membantu dan mendukung dalam penyelesaian skripsi ini.

Semoga segala bantuan, bimbingan, dan masukan yang telah diberikan kepada penulis menjadi amal ibadah dan mendapatkan balasan dari Allah SWT.

Semoga skripsi ini dapat bermanfaat bagi para pembaca umumnya. Akhir kata penulis ucapkan terimakasih. Wassalamu'alaikum.

Padang, November 2021

Silvia Yolla

# DAFTAR ISI

# DAFTAR TABEL

Tabel Halaman

# DAFTAR GAMBAR

Gambar Halaman

# DAFTAR LAMPIRAN

Lampiran Halaman

# BAB I

# PENDAHULUAN

## A. Latar Belakang

Perkembangan teknologi merupakan aspek yang penting dalam kehidupan manusia, termasuk kemajuan teknologi dalam bidang telekomunikasi. Dahulu masyarakat berkomunikasi melalui surat menyurat tetapi dengan seiring berkembangnya teknologi masyarakat dapat berkomunikasi dengan mengirimkan pesan dari jarak jauh dengan cepat dan mudah menggunakan jaringan internet, gelombang radio maupun media lain. Dibalik perkembangan dan pemanfaatan internet yang demikian pesat, ternyata ada bahaya yang mengancam penggunanya, apalagi yang kurang memahami tentang keamanan data. Untuk meminimalkan kemungkinan terjadinya tindak kejahatan di internet inilah diperlukan teknologi keamanan informasi, khususnya sistem enkripsi (penyandian). Enkripsi merupakan bagian dari cabang kriptografi, dimana algoritma kriptografi untuk penyandian telah mengalami perkembangan dan perbaikan dari masa ke masa. Sehingga proses tersebut menghasilkan algoritma yang memuaskan, misalnya DES, IDEA, RSA, dan lain-lain. Salah satu algoritma yang populer dan kuat sehingga tidak mudah dipecahkan pada tahun 80-an yaitu DES (Dony, 2005).

DES merupakan nama dari sebuah algoritma untuk mengenkripsi data yang dikeluarkan oleh Federal Information Processing Standard (FIPS) di Amerika. Ada sedikit modifikasi dan perbaikan pada perkembangan algoritma DES yaitu algoritma Triple DES, cara ini dipakai untuk membuat

algoritma DES lebih kuat lagi. Akan tetapi algoritma yang digunakan sama, hanya saja algoritma Triple DES melakukan enkripsi algoritma DES sebanyak tiga kali dengan menggunakan dua kunci yang berbeda.

NIST (*National Institute of Standards and Technology*) yang berada di Amerika setiap lima tahun sekali mensertifikasi ulang algoritma DES sejak tahun 1977, disebabkan banyaknya kelemahan pada algoritma DES, kini NIST tidak lagi mensertifikati sejak tahun 1993(penyertifikatan terakhir untuk DES). Selanjutnya dikembangkan suatu algoritma baru yang diharapkan dapat menggantikan DES yaitu AES (*Advanced Encryption Standard*).

Algoritma AES merupakan salah satu algoritma simetris yng beroperasi pada sekumpulan *byte* data atau per blok. AES *(Advanced Encryption Standard)*yang lahir pada November 2001 dengan pencetus Rijmen dan Daemen (Rijndael) cukup mengejutkan dunia kriptografi, karena pada saat itu menyisihkan empat finalis algoritma lainnya yang cukup populer yaitu *MARS, RC6, Serpent,* dan *Twofish.* Terbukti dengan diberlakukan AES secara efektif tahun 2002, AES mendapatkan sertifikat dari NIST saja sudah mencapai 144 produk sampai bulan Mei 2004. AES memang dipersiapkan untuk penerapan *software, firmware, hardware* atau kombinasinya. Jadi, suatu hal yang cukuo wajar bila usaha pengembangannya banyak dan bervariasi (Dony, 2005). Selain keunggulan yang telah disebutkan, Algoritma AES:Rijndael juga dirancang untuk memiliki properti ketahanan terhadap semua jenis serangan yang telah diketahui, kesederhanaan rancangan, dan kekompakan kode serta kecepatan koputasi pada berbagai platform.

Rijndael *cipher* (AES:Rijndael) dapat dikategorikan sebagai *iterated block cipher* dengan panjang blok dan panjang kunci yang dapat dipilih secara *independent* sebanyak 128, 192, 256 *bit*,ukuran blok dan kunci dapat berupa kelipatan 32 bit, dengan minimum 128 dan maksimum 256 bit. Biasanya enkripsi 256 bit digunakan untuk data saat transit, atau data yang berjalan melalui jaringan atau koneksi internet. Tidak diketahui berapa banyak yang menggunakan AES 256 bit. Namun, menurut techopedia AES ini juga diterapkan untuk data sensitif dan penting seperti data keuangan, militer, atau milik pemerintah. Pemerintah AS mewajibkan semua data sensitif dan penting dienkripsi menggunakan metode enkripsi 192 atau 256 bit.

Berdasarkan latar belakang tersebut peneliti ingin melakukan penelitian yang berjudul "**Kriptografi Symmetric-Key dengan Metode AES(Advanced Encryption Standard) 256 bit"**.

## B. Rumusan Masalah

Dari latar belakang masalah, maka penulis merumuskan masalah penelitian yaitu "Bagaimana kinerja algoritma AES (*Advanced Encryption Standard*) menggunakan panjang kunci 256 bit untuk mengamankan pesan teks".

## C. Tujuan Penelitian

Berdasarkan permasalahan yang diajukan maka penelitian ini bertujuan untuk:

1. Mendeskripsikan proses enkripsi pada pesan teks dengan metode AES 256 bit.

2. Mendeskripsikan proses dekripsi pada pesan teks dengan metode AES 256 bit.

## D. Manfaat Penelitian

1. Bagi Peneliti

   Untuk menambah wawasan tentang Kriptografi Symmetric-Key dengan Metode AES (Advanced Encryption Standard) 256 bit.

2. Bagi Pembaca

   Sebagai informasi tentang Kriptografi Symmetric-Key dengan Metode AES (Advanced Encryption Standard) 256 bit.

3. Bagi Peneliti Selanjutnya

   Sebagai referensi untuk mengembangkan Kriptografi Symmetric-Key dengan Metode AES (Advanced Encryption Standard) 256 bit.