



**IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION*
STANDARD UNTUK KEAMANAN DATA FILE TEKS
DENGAN METODE *LEAST SIGNIFICANT BIT INSERTION*
PADA VIDIO AVI**

SKRIPSI

Ifan Alriansyah

1610511068

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”

JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2020



**IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION*
STANDARD UNTUK KEAMANAN DATA FILE TEKS
DENGAN METODE *LEAST SIGNIFICANT BIT INSERTION*
PADA VIDEO AVI**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh
Gelar Sarjana Komputer**

Ifan Alriansyah

1610511068

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”

JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2020

PERNYATAAN ORISINALITAS PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Ifan Alriansyah

NIM : 1610511068

Tanggal : 16-08-2020

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 16-08-2020

Yang Menvatakan



(Ifan Alriansyah)

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta,
Saya yang bertanda tangan dibawah ini:

Nama : Ifan Alriansyah

NIM : 160511068

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah Saya yang berjudul:

**IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION
STANDARD UNTUK KEAMANAN DATA FILE TEKS DENGAN
METODE LEAST SIGNIFICANT BIT INSERTION PADA VIDIO AVI**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan *data (database)*, merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Jakarta

Pada Tanggal: 16 Agustus 2020

Yang menyatakan,



(Ifan Alriansyah)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama : Ifan Alriansyah
NIM : 1610511080
Program Studi : Informatika
Judul Tugas Akhir : Implementasi Algoritma *Advanced Encryption Standard*
Untuk Keamanan Data File Teks Dengan Metode *Least Significant Bit Insertion* Pada Vidio AVI.

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Yuni Widiastiwi, S.Kom., M.Si.

Penguji I



Henki Bayu Seta, S.Kom., M.TI.

Pembimbing I



Dr. Ermatita, M. Kom.

Dekan

Ditetapkan di : Jakarta

Tanggal Pengesahan : 15 Juli 2020



Mayanda Mega Santoni, S.Kom., M.Kom.

Penguji II



Iin Ernawati, S.Kom., M.Si

Pembimbing II



Anita Muliawati, S.Kom., M.TI.

Ketua Program Studi



**IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD*
UNTUK KEAMANAN DATA FILE TEKS DENGAN METODE *LEAST
SIGNIFICANT BIT INSERTION* PADA VIDIO AVI**

Ifan Alriansyah

ABSTRAK

Banyak sekali kejahatan pencurian data penting yang terjadi di dunia maya. Hal ini terjadi dikarenakan lemahnya keamanan dalam proses pengiriman data. Akibatnya data yang dikirim dapat dicuri atau dimodifikasi oleh pihak luar yang tidak bertanggung jawab. Berawal dari masalah tersebut dibutuhkan suatu alat yang mampu memberikan keamanan tambahan kepada pengguna yang mengirimkan datanya. Berdasarkan hal tersebut tujuan penelitian ini dilakukan guna mencegah terjadinya pencurian data oleh pihak luar. Dengan menggunakan *Advanced Encryption Standard* untuk mengenkripsi pesan serta metode *Significant Bit Insertion* untuk menyisipkan hasil dari enkripsi kedalam Vidio agar tidak menimbulkan kecurigaan yang diprogram menggunakan *Matlab* guna membantu proses enkripsi. Dalam penerapan yang dilakukan penulis yaitu tahapan pengujian sistem, algoritma *AES* dapat menenkripsi dan mendenkripsi data *file text* serta metode *LSB* dapat menyisipkan dan mengambil *file text* yang terenkripsi dari Vidio AVI.

Kata Kunci: Pencurian, Enkripsi, *Advanced Encryption Standard*, *Significant Bit Insertion*, *MATLAB*

**IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD
ALGORITHM FOR TEXT FILE SECURITY USING LEAST SIGNIFICANT
BIT INSERTION METHOD IN AVI VIDIO**

Abstract

Lots of important data theft crimes that occur in cyberspace. This happens due to weak security in the process of sending data. As a result the data sent can be stolen or modified by outsiders who are not responsible. Starting from this problem we need a tool that is able to provide additional security to users who send data. Based on this the purpose of this study was conducted to prevent data theft by outsiders. By using the Advanced Encryption Standard to encrypt messages and the Significant Bit Insertion method to insert the results of encryption into the Vidio so as not to arouse suspicion that is programmed using Matlab to help the encryption process. In the application by the author, namely the system testing stage, the AES algorithm can decrypt and decrypt text file data and the LSB method can insert and retrieve encrypted text files from AVI Vidios.

Keywords: Pencurian, Enkripsi, Advanced Encryption Standard, Significant Bit Insertion, MATLAB

KATA PENGANTAR

Dengan memanjatkan puji dan syukur ke hadirat Allah SWT atas segala karunia-Nya, atas segala rahmat dan hidayah-Nya, shalawat dan salam tak lupa tercurahkan kepada Nabi Muhammad SAW beserta keluarga dan sahabatnya, sehingga penulis dapat menyelesaikan skripsi ini yang berjudul **“IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* UNTUK KEAMANAN DATA FILE TEKS DENGAN METODE *LEAST SIGNIFICANT BIT INSERTION* PADA VIDEO AVI”**. Rasa terimakasih tak lupa penulis ucapkan kepada :

1. Kedua Orang tua Yeni Pertiwi Noer (Ibu) dan Candra Wijaya (Ayah) yang telah memberikan dukungan, kepercayaan serta doa yang tiada hentinya kepada penulis dalam menyelesaikan skripsi ini.
2. Kedua Tante Yulia Pusparini Noer dan Yuni Perdani Noer yang telah membantu saya agar bisa kuliah.
3. Abang Rafi Adriansyah yang telah memberikan dukungan materiil.
4. Bapak Henki Bayu Seta, S.Kom., M.Si dan ibu Iin Ernawati, S.Kom., M.Si selaku dosen pembimbing 1 dan 2 yang selalu memberikan dorongan kepada saya agar dapat menyelesaikan skripsi ini.
5. Ibu Dr. Ermatita, M.Kom selaku Dekan Fakultas Ilmu Komputer.
6. Ibu Anita Muliawati, S.Kom., MTI. selaku Kepala program Studi Informatika.
7. Teman-teman Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

Akhir kata, semoga skripsi yang telah dibuat ini dapat bermanfaat dan dikembangkan bagi para pembaca.

Jakarta, 16 Agustus 2020

Penulis



(Ifan Alriansyah)

DAFTAR ISI

IMPLEMENTASI ALGORITMA <i>ADVANCED ENCRYPTION STANDARD</i> UNTUK KEAMANAN DATA FILE TEKS DENGAN METODE <i>LEAST SIGNIFICANT BIT INSERTION</i> PADA VIDIO AVI	i
IMPLEMENTASI ALGORITMA <i>ADVANCED ENCRYPTION STANDARD</i> UNTUK KEAMANAN DATA FILE TEKS DENGAN METODE <i>LEAST SIGNIFICANT BIT INSERTION</i> PADA VIDIO AVI	i
PERNYATAAN ORISINALITAS	ii
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	iii
LEMBAR PENGESAHAN	iv
ABSTRAK	v
Abstract	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR	xii
DAFTAR LAMPIRAN.....	xiii
BAB 1 PENDAHULUAN	14
1.1 Latar Belakang	14
1.2 Rumusan Masalah	15
1.3 Tujuan Penelitian.....	15
1.4 Manfaat Penelitian.....	15
1.5 Luaran yang diharapkan	15
1.7 Ruang Lingkup	15
1.8 Sistematika Penulisan.....	16
BAB 2 TINJAUAN PUSTAKA	17
2.1 Kejahatan Siber	17
2.1.1 Modus Operandi Kejahatan Siber	17
2.2 Kriptografi	19
2.3 Enkripsi dan Dekripsi	20
2.4 Advance Encryption Standard.....	20
2.5 Steganografi.....	22

2.6	Least Significant Bit	23
2.7	Audio Video Interleave (AVI).....	23
2.8	File.....	24
2.9	Penelitian Relevan	24
2.9.1	Penelitian Asri Prameshwari, Nyoman Putra Sastra	24
2.9.2	Penelitian Nizirwan Anwar, 2018	25
2.9.3	Penelitian Marto Sihombing, Juliana Naftali Sitompul, Tia Anggia Putri,2019.....	25
2.9.4	Penelitian Dedy Abdullah, Doni Nugroho Saputro	25
2.9.5	Penelitian Rizky Maynarda, Ahmad Setiadi, Pas Mahyu Akhirianto, Marianus Lase, Agus Junaidi.....	25
BAB 3 METODE PENELITIAN.....		27
3.1	Kerangka Berfikir	27
3.2	Identifikasi Masalah	28
3.3	Studi Literatur.....	28
3.4	Pra Proses	28
3.5	Proses Enkripsi dan Penyisipan Data	29
3.6	Proses Dekripsi dan Ekstrasi Data.....	30
3.7	Alat yang digunakan.....	31
3.8	Tempat dan Waktu Pelaksanaan.....	32
BAB 4 HASIL DAN PEMBAHASAN.....		33
4.1	Data	33
4.2	Praproses	33
4.2.1	Inisiasi <i>AES</i>	34
4.2.2	Key Expansion	35
4.3	Proses.....	39
4.4	Perhitungan Enkripsi <i>AES</i>	39
4.5	Least Significant bit Insertion	48
4.7	Least Significant bit Extraction	52
4.6.1	Perhitungan Dekripsi <i>AES</i>	54
4.8	Evaluasi	50
BAB 5 PENUTUP		51
5.1	Kesimpulan.....	51
5.2	Saran	51

DAFTAR PUSTAKA	57
Lampiran	59

DAFTAR TABEL

Table 1 Tipe Algoritma AES	21
Table 2 Tempat Dan Waktu Pelaksanaan	32
Table 3 Hasil Reshape Plainteks 4x4	34
Table 4 Hasil Reshape Key 4x4	34
Table 5 Cipher Key	35
Table 6 Hasil Byte Setelah Baris 4 Bergeser	35
Table 7 Tabel S-BOX.....	36
Table 8 Hasil Matriks SubBytes	37
Table 9 Tabel Rcon	37
Table 10 Baris Pertama <i>CipherKey</i>	37
Table 11 Nilai Rcon Kolom Pertama	37
Table 12 Hasil <i>CipherKey XOR SubBytes XOR Nilai Rcon</i>	38
Table 13 Round Key 1-10	38
Table 14 Plaintext	39
Table 15 Ciphertext.....	39
Table 16 Hasil Plaintext XOR Round Key 1	46
Table 17 Hasil SubBytes	46
Table 18 Hasil ShiftRows	47
Table 19 Matriks Polynomial.....	47
Table 20 Hasil <i>MixColumns</i>	47
Table 21 Round Key 2	46
Table 22 Hasil <i>MixColumns XOR Round Key 2</i>	46
Table 23 Enkripsi Round 2 - 10	46
Table 24 CipherText	48
Table 25 Hexadecimal To Biner	48
Table 26 Nilai Piksel Berbentuk Decimal.....	49
Table 27 Nilai Piksel Berbentuk Biner	49
Table 28 Urutan Tiap Bit Pada Pesan	50
Table 29 Hasil Substitusi Nilai Binary	51
Table 30 Hasil Substitusi Yang Dirubah Menjadi Decimal	52
Table 31 Nilai Biner Layer RGB	52
Table 32 Round Key 10	54
Table 33 Hasil CipherText XOR Round Key 10	54
Table 34 Hasil InvShiftRows	55
Table 35 Tabel INV S-BOX	55
Table 36 Hasil InvSubBytes.....	57
Table 37 Round Key 9	57
Table 38 Hasil InvSubBytes XOR Round Key 9.....	57
Table 39 Inverse Matriks Polynomial	57
Table 40 InvMixColumns	47
Table 41 Hasil Dekripsi Round 2 – 10.....	47

DAFTAR GAMBAR

Gambar 1 Proses Enkripsi Dan Dekripsi	20
Gambar 2 Proses Steganografi	22
Gambar 3 Kerangka Berfikir.....	27
Gambar 4 Flowchart Enkripsi dan Penyisipan Data	29
Gambar 5 FlowChart Dekripsi dan Ekstrasi Data.....	30
Gambar 6 Size File Testing 1 Awal dan Akhir	50
Gambar 7 Size File Testing 2 Awal dan Akhir	51
Gambar 8 Size File Testing 3 Awal dan Akhir	51
Gambar 9 Size File Vidio LSB Awal dan Hasil	52
Gambar 10 Size File Vidio LSB 2 Awal dan Hasil	52
Gambar 11 Size File Vidio LSB 3 Awal dan Hasil	52
Gambar 12 Tampilan File Testing 1 Awal dan Akhir	53
Gambar 13 Tampilan File Testing 2 Awal dan Akhir	54
Gambar 14 Tampilan File Testing 3 Awal dan Akhir	54
Gambar 15 Tampilan File Vidio Awal	55
Gambar 16 Tampilan Hasil Vidio LSB.....	56
Gambar 17 Tampilan Hasil Vidio LSB 2.....	56
Gambar 18 Tampilan Hasil Vidio LSB 3.....	57
Gambar 19 Tampilan Awal.....	59
Gambar 20 Hasil Enkripsi Dari Data Teks File Yang Diambil	60
Gambar 21 Proses Penyisipan Hasil Enkripsi Kedalam Vidio	60
Gambar 22 Proses Pengambilan Hasil Enkripsi Dari Vidio	61
Gambar 23 Proses Dekripsi File Yang Telah Dienkripsi.....	62

DAFTAR LAMPIRAN

Lampiran 1	<i>GUI</i>
Lampiran 2	Hasil Turnitin