

**PENGAMANAN *BIG DATA* DENGAN *ADVANCED*  
*ENCRYPTION STANDARD-256* DAN KUNCI *HASHING*  
*SECURE HASH ALGORITHM-256***

**SKRIPSI**

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar  
Sarjana Matematika



Oleh

Tatyana Citra Diantari

NIM 1905050

**PROGRAM STUDI MATEMATIKA  
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
UNIVERSITAS PENDIDIKAN INDONESIA**

**2024**

# **Pengamana *Big Data* dengan *Advanced Encryption Standard-256* dan Kunci Hashing *Secure Hash Algorithm-256***

Oleh  
Tatyana Citra Diantari

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

© Tatyana Citra Diantari 2024  
Universitas Pendidikan Indonesia  
April 2024

Hak Cipta dilindungi undang-undang.  
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,  
dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

**LEMBAR PENGESAHAN**

Tatyana Citra Diantari  
1905050

**PENGAMANAN BIG DATA DENGAN *ADVANCED*  
*ENCRYPTION STANDARD-256* DAN KUNCI *HASHING*  
*SECURE HASH ALGORITHM-256***

Disetujui dan disahkan oleh pembimbing :

Pembimbing I,



Dra. Hj. Rini Marwati, M.S.  
NIP. 196606251990012001

Pembimbing II,



Ririn Sispiyati, S.Si., M.Si.  
NIP. 198106282005012001

Mengetahui,

Ketua Program Studi Matematika



Dr. Kartika Yulianti, S.Pd., M.Si  
NIP. 198207282005012001

## ABSTRAK

Teknologi yang semakin berkembang dengan pesat telah menghasilkan jumlah data yang sangat besar, yang biasa dikenal sebagai big data. Diperlukan tempat penyimpanan modern yang sangat aman untuk menyimpan big data tersebut. Keamanan data di dunia digital menjadi salah satu tantangan kritis yang dihadapi saat ini. Salah satu solusi dalam hal ini adalah mengimplementasikan kriptografi untuk pengamanan *big data*, sehingga data tersebut menjadi samar dan sulit dipahami oleh pihak yang tidak berhak. Penelitian ini membahas tentang pengamanan big data menggunakan algoritma kriptografi *Advanced Encryption Standard-256* dan kunci *hashing Secure Hash Algorithm-256*. AES-256 merupakan salah satu algoritma andalan dengan kekuatan enkripsi yang tinggi, sedangkan SHA-256 merupakan algoritma kriptografi satu arah yang hingga saat ini tidak ditemukannya kolisi. Sebuah program aplikasi berbasis *python* dikonstruksikan untuk mengamankan *file* csv berukuran besar. Kunci yang diinput pada program akan dienkripsi menggunakan algoritma SHA-256 sehingga didapatkan *message digestnya*. *Message digest* tersebut akan diolah kembali menjadi kunci yang akan digunakan pada proses enkripsi *file* csv menggunakan algoritma AES-256 hingga dihasilkan sebuah *file* enkripsi dengan format \*.aes. *File* enkripsi tersebut dapat didekripsi kembali hingga menghasilkan *file* CSV asli.

**Kata kunci:** Kriptografi, Pengamanan Data, *File* CSV, AES, SHA.

## ABSTRACT

*The rapidly advancing technology has resulted in a massive amount of data, commonly known as big data. A highly secure modern storage space is required to store this big data. Data security in the digital world has become one of the critical challenges faced today. One solution in this regard is to implement cryptography for securing big data, making the data obscure and difficult to comprehend for unauthorized parties. This research discusses the security of big data using the Advanced Encryption Standard-256 cryptography algorithm and the Secure Hash Algorithm-256 hashing key. AES-256 is one of the flagship algorithms known for its high encryption strength, while SHA-256 is a one-way cryptographic algorithm that, to date, has not encountered collisions. A python-based application program is constructed to secure large-sized CSV files. The key input into the program will be encrypted using the SHA-256 algorithm to obtain its message digest. This message digest will then be processed again to create a key for use in the AES-256 file encryption process, resulting in an encrypted file in \*.aes format. This encrypted file can be decrypted back to produce the original CSV file.*

**Keywords:** *Cryptography, Data Security, CSV File, AES, SHA.*

## DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI .....	i
SURAT PERNYATAAN.....	ii
KATA PENGANTAR .....	iii
UCAPAN TERIMA KASIH.....	iv
ABSTRAK .....	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR .....	xi
DAFTAR TABEL.....	xiii
 BAB I PENDAHULUAN .....	 1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	5
1.3. Tujuan Penelitian.....	5
1.4. Batasan Masalah.....	5
1.5. Manfaat Penelitian.....	5
 BAB II LANDASAN TEORI .....	 7
2.1. Logika Matematika.....	7
2.2. Exclusive OR (XOR).....	7
2.3. Galois <i>Field</i> .....	8
2.4. Aritmatika Galois <i>Field</i> .....	9
2.4.1. Penjumlahan dan Pengurangannya .....	9
2.4.2. Perkalian dan Inversnya .....	9
2.5. Kriptografi .....	10

2.5.1.	Pengertian Kriptografi.....	10
2.5.2.	Kriptografi Kunci Simetri .....	14
2.5.3.	Kriptografi Kunci Asimetri.....	14
2.6.	Advanced Encryption Standard.....	15
2.6.1.	Algoritma Rijndael.....	16
2.6.2.	Enkripsi Algoritma Rijndael .....	16
2.6.3.	Dekripsi Algoritma Rijndael .....	27
2.7.	Fungsi <i>Hash Secure Hash Algorithm-256</i> .....	28
2.7.1.	Padding Pesan .....	29
2.7.2.	Parsing Pesan .....	31
2.7.3.	Set Initial Hash Value .....	32
2.7.4.	Persiapkan <i>Message Schedule</i> .....	33
2.7.5.	Inisialisasi Variabel.....	34
2.7.6.	Menjumlahkan Variabel.....	36
2.7.7.	Output.....	37
2.8.	Bahasa Pemrograman <i>Python</i> .....	37
BAB III METODE PENELITIAN.....		39
3.1.	Identifikasi Masalah .....	39
3.2.	Model Dasar .....	39
3.2.1.	AES-256.....	39
3.2.2.	SHA-256 .....	41
3.3.	Pengembangan Model .....	42
3.4.	Konstruksi Program.....	43
3.4.1.	Input dan Output .....	43
3.4.2.	Rancangan Tampilan.....	44

3.5.	Algoritma Deskriptif .....	45
3.6.	Coding <i>Python</i> .....	46
3.7.	Proses Validasi .....	46
3.8.	Pengambilan Kesimpulan .....	47
BAB IV HASIL DAN PEMBAHASAN .....		48
4.1.	Skema Program Pengamanan <i>Big Data</i> dengan AES-256 dan Kunci <i>Hashing</i> SHA-256 .....	48
4.2.	Algoritma Program Pengamanan Data dengan AES-256 dan Kunci <i>Hashing</i> SHA-256 .....	49
4.2.1.	Enkripsi .....	49
4.2.2.	Dekripsi .....	50
4.3.	Tampilan Program Pengamanan Data dengan AES-256 dan Kunci <i>Hashing</i> SHA-256 .....	51
4.3.1.	Menu Utama .....	52
4.3.2.	Menu Enkripsi .....	52
4.3.3.	Menu Dekripsi .....	55
4.4.	Validasi .....	56
BAB V KESIMPULAN DAN SARAN .....		60
5.1.	Kesimpulan .....	60
5.2.	Saran .....	61
DAFTAR PUSTAKA .....		62
LAMPIRAN .....		64



## DAFTAR GAMBAR

Gambar 2.1 Alur Komunikasi dalam Kriptografi .....	12
Gambar 2.2 Skema Kriptografi Kunci Simetri .....	14
Gambar 2.3 Skema Kriptografi Kunci Asimetri .....	15
Gambar 2.4 Proses <i>AddRoundKey</i> .....	17
Gambar 2.5 Matriks Kunci.....	18
Gambar 2.6 Matriks <i>State</i> .....	18
Gambar 2.7 Proses <i>AddRoundKey</i> .....	19
Gambar 2.8 Hasil Proses <i>AddRoundKey</i> .....	19
Gambar 2.9 Proses <i>SubBytes</i> .....	20
Gambar 2.10 Proses <i>SubBytes</i> .....	21
Gambar 2.11 Proses <i>SubBytes</i> .....	21
Gambar 2.12 Matriks <i>State</i> .....	22
Gambar 2.13 Matriks <i>State</i> .....	23
Gambar 2.14 Matriks <i>State</i> .....	25
Gambar 2.15 Matriks Kunci.....	26
Gambar 2.16 Proses Ekspansi Kunci .....	26
Gambar 2.17 Proses Ekspansi Kunci .....	26
Gambar 2.18 Proses Ekspansi Kunci .....	27
Gambar 2.19 Proses Ekspansi Kunci .....	27
Gambar 2.20 Matriks <i>State</i> .....	27
Gambar 2.21 Contoh <i>Input</i> dan <i>Output</i> Fungsi Hash.....	29
Gambar 3.1 Skema Enkripsi <i>Advanced Encryption Standard</i> .....	40
Gambar 3.2 Skema Dekripsi <i>Advanced Encryption Standard</i> .....	41
Gambar 3.3 Skema Enkripsi <i>Secure Hash Algorithm-256</i> .....	42
Gambar 3.4 Skema Hasil Pengembangan Model.....	43
Gambar 3.5 Rancangan Tampilan Menu Utama.....	44
Gambar 3.6 Rancangan Tampilan Menu Enkripsi.....	44
Gambar 3.7 Rancangan Tampilan Menu Dekripsi.....	45

Gambar 4.1 Skema Program Pengamanan <i>Big Data</i> dengan AES-256 dan Kunci Hashing SHA-256.....	48
Gambar 4.2 Tampilan Menu Utama.....	52
Gambar 4.3 Tampilan Menu Enkripsi.....	52
Gambar 4.4 Tampilan <i>Window Select a File</i> .....	53
Gambar 4.5 Hasil Enkripsi <i>File Individual_incident_2000.csv</i> .....	54
Gambar 4.6 Tampilan Menu Dekripsi .....	55
Gambar 4.7 Hasil Dekripsi <i>File Ciphertext Individual_incident_2000.csv</i> .....	56
Gambar 4.8 <i>Ciphertext File Individual_incident_2003.csv</i> .....	57
Gambar 4.9 <i>Plaintext Asli dan Plaintext Hasil Dekripsi File Individual_incident_2003.csv</i> .....	57
Gambar 4.10 <i>Ciphertext File Individual_incident_2004.csv</i> .....	58
Gambar 4.11 <i>Plaintext Asli dan Plaintext Hasil Dekripsi Individual_incident_2004.csv</i> .....	58
Gambar 4.12 <i>Ciphertext File Individual_incident_2004a.csv</i> .....	59

**DAFTAR TABEL**

Tabel 2.1 Tabel Kebenaran XOR.....	8
Tabel 2.2 Tabel <i>S-box</i> .....	20
Tabel 2.3 Tabel E .....	24
Tabel 2.4 Tabel L .....	24
Tabel 2.5 Tabel Invers S-box .....	28
Tabel 2.6 Contoh Sembarang <i>Plaintext</i> dalam Biner.....	30
Tabel 2.7 <i>Plaintext</i> Setelah Penambahan Bit 0 .....	31
Tabel 2.8 <i>Plaintext</i> Setelah Penambahan Panjang <i>Append</i> .....	31
Tabel 2.9 Tabel <i>Hash Value</i> .....	33
Tabel 2.10 <i>Plaintext</i> dalam Heksadesimal .....	34
Tabel 2.11 Konstanta SHA-256 .....	35

## DAFTAR PUSTAKA

- Asriyanik. (2017). Studi Terhadap *Advanced Encryption Standard* (AES) dan Algoritma *Knapsack* dalam Pengamanan Data. *Jurnal SANTIKA: Ilmiah Sains dan Teknologi*, 7(1).
- Benvenuto, C. J. (2012). Galois field in cryptography. *University of Washington*, 1(1), 1-11.
- Biham, E., & Chen, R. (2004, August). Near-collisions of SHA-0. *Annual International Cryptology Conference* (pp. 290-305). Springer, Berlin, Heidelberg.
- Damayanti, R. (2021). *Logika Matematika*. Kediri: Pernal Edukreatif.
- Davies, R. B. (2002). Exclusive OR (XOR) and hardware random number generators. Retrieved May, 31, 2013.
- Fathurrozi, A. (2021). PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-256) DENGAN MODE CBC DAN SECURE HASH ALGORITHM (SHA-256) UNTUK PENGAMANAN DATA FILE. *Journal of Informatic and Information Security*, 2(2).
- Jamil, T. (2004). *The rijndael algorithm*. *IEEE Potentials*, 23(2), 36–38. doi:10.1109/mp.2004.1289996
- Lusiana, V. (2011). Implementasi Kriptografi Pada *File* Dokumen Menggunakan Algoritma AES-128. *Dinamika Informatika: Jurnal Ilmiah Teknologi Informasi*, 3(2).
- Munir, R. (2019). *KRIPTOGRAFI*. Bandung: Informatika Bandung.
- Nainggolan, S. (2022). Implementasi Algoritma SHA-256 Pada Aplikasi Duplicate Document Scanner. *Resolusi: Rekayasa Teknik Informatika dan Informasi*, 2(5), 201-213.
- Narendra, A. P. (2015). Data besar, data analisis, dan pengembangan kompetensi pustakawan. *Record and Library Journal*, 1(2), 83-93.
- Sanner, M. F. (1999). *Python: a programming language for software integration and development*. *J Mol Graph Model*, 17(1), 57-61.
- Saputra, I., & Nasution, S. D. (2019). Analisa Algoritma SHA-256 Untuk Mendeteksi Orisinalitas Citra Digital. *Prosiding Seminar Nasional Riset Information Science (SENARIS)* (Vol. 1, pp. 164-178).
- Srinath, K. R. (2017). *Python–The Fastest Growing Programming Language*. *International Research Journal of Engineering and Technology*, 4(12), 354-357.

- Stinson, D.R. (2006). *Cryptography Theory and Practice Third Edition*. Boca Raton, FL: CRC Press.
- Stinson, D.R. & Paterson, M.B. (2019). *Cryptography Theory and Practice Fourth Edition*. Boca Raton, FL: CRC Press.
- Sutabri, T. (2012). *Konsep Sistem Informasi*. Yogyakarta: CV ANDI OFFSET.
- Vidhya, S. (2018). Network security using *python*. *2018 IJSRSET*, 4(4).
- Wibisono, S. (2008). *Matematika Diskrit*. Yogyakarta: Graha Ilmu.
- Yoshida, H., & Biryukov, A. (2006). Analysis of a SHA-256 variant. In *International Workshop on Selected Areas in Cryptography* (pp. 245-260). Springer, Berlin, Heidelberg.
- Yuniati, V., & Indriyanta, G. (2011). Enkripsi dan Dekripsi dengan algoritma AES 256 untuk semua jenis *file*. *Jurnal Informatika*, 5(1).