# 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


Universitas Pendidikan Indonesia
April 2024

**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

# DAFTAR GAMBAR

# DAFTAR TABEL

## 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: Pemeral 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).