PENERAPAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) UNTUK ENKRIPSI DAN DEKRIPSI CITRA BERFORMAT .BMP DAN .PNG

SKRIPSI

Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Sains Bidang Studi Matematika

Oleh

YUSTI QOMAH
NIM. 08011281520093

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS SRIWIJAYA
JANUARI 2020

LEMBAR PENGESAHAN

PENERAPAN ALGORITMA
***ADVANCED ENCRYPTION STANDARD* (AES)**
UNTUK ENKRIPSI DAN DEKRIPSI CITRA
BERFORMAT .BMP DAN .PNG

SKRIPSI

Sebagai Salah Satu Syarat untuk Memperoleh Gelar
Sarjana Sains Bidang Studi Matematika

Oleh

YUSTI QOMAH
NIM 08011281520093

Indralaya, Januari 2020

Pembimbing Kedua	**Pembimbing Utama**
Drs. Ali Amran, M.T	**Anita Desiani, M.Kom**
NIP. 19661213199402 2 001	**NIP. 19771211200312 2 002**

Mengetahui
Ketua Jurusan Matematika

Drs. Sugandi Yahdin, M.M
NIP.19580727 198603 1 003

LEMBAR PERSEMBAHAN

Motto:

Maka apabila engkau telah selesai (dari sesuatu urusan),

Tetaplah bekerja keras (untuk urusan yang lain)

(Q.S. Al-Insyiroh: 6-7)

Sometimes it is the people no one imagines anything

of who do the things no one can imagine

(Alan Turing)

Skripsi ini kupersembahkan kepada:

- Allah SWT
- Kedua Orang Tuaku Tercinta
- Seluruh Keluarga Besarku
- Semua Dosen dan Guruku
- Almamaterku

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji syukur penulis panjatkan kepada Allah SWT karena atas berkat rahmat, karunia, kasih sayang dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **"PENERAPAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) UNTUK ENKRIPSI DAN DEKRIPSI CITRA BERFORMAT .BMP DAN .PNG"** dengan baik. Shalawat dan salam penulis haturkan kepada Nabi Muhammad SAW, beserta keluarga, sahabat, dan para pengikutnya hingga akhir zaman.

Skripsi ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Sains Bidang Studi Matematika di Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya. Penulisan skripsi ini tidak lepas dari bantuan berbagai pihak baik secara langsung maupun tidak langsung, untuk itu penulis menyampaikan terima kasih sebesar-besarnya kepada:

1. Ayahanda **Hirmanto** dan Ibunda **Umayu**, beserta keluarga besar yang selalu memberikan dukungan, doa, dan nasihat tanpa henti.
2. Bapak **Drs. Sugandi Yahdin, M.M.** dan Ibu **Des Alwine Zayanti, M.Si.** selaku Ketua Jurusan dan Sekretaris Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya, serta **Ibu Sri Indra Maiyanti, M.Si.** selaku Pembimbing Akademik. Terima kasih telah memberikan waktu dan masukan untuk penulis.

3. Ibu **Anita Desiani, S.Si., M.Kom.** selaku Pembimbing Utama dan Bapak **Drs. Ali Amran, M.T.** selaku Pembimbing Kedua. Terima kasih telah bersedia menyediakan waktu, pikiran, motivasi dan saran serta kesabaran memberikan arahan dan bimbingan terbaik kepada penulis dalam masa penyusunan skripsi ini.
4. Bapak **Drs. Sugandi Yahdin, M.M.**, Bapak **Drs. Endro Setyo Cahyono, M.Si.**, dan Ibu **Dr. Ning Eliyati, M.Pd.** selaku Penguji Utama yang telah bersedia meluangkan waktu dalam memberikan tanggapan, kritik, saran yang bermanfaat dalam perbaikan dan penyelesaian skripsi ini.
5. **Seluruh Dosen** Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya yang telah memberikan ilmu kepada penulis selama masa perkuliahan.
6. Bapak **Irwansyah** selaku admin dan Ibu **Hamidah** selaku pegawai tata usaha Jurusan Matematika dan Ilmu Pengetahuan Alam yang telah membantu selama penulis menjalani perkuliahan.
7. Sahabatku **Kerenila**, **Wili**, **Annisa**, **Indah**, **Novika**, **Marnita**, **Eka**, **Elsa**, **Vidya**, **Feren**, **Ria**, **Shaly**, **Nirwan**, **Febrizal**, **Anna**, **Fitri**, **Mba Vinda**, **Mba Lita**, dan seluruh teman-teman angkatan 2015.
8. Adik-adik **Ega P**, **Ega M**, **Siti**, **Rieren**, **Bella**, **Kaima** atas semua motivasi dan doanya.
9. Teman-teman organisasi **LDF KOSMIC**, **HIMASTIK**, **IKAHIMATIKA Wilayah II**, **FLP Ogan Ilir** untuk semangat, pengalaman, dan dukungannya.

10. Semua pihak yang tidak bisa disebutkan satu persatu yang telah memberikan bantuan, doa, dan dukungan selama penulisan skripsi ini.

Semoga skripsi ini dapat bermanfaat dalam menambah wawasan dan pengetahuan bagi seluruh mahasiswa Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sriwijaya.

Wassalamu'alaikum Wr. Wb.

Indralaya, Januari 2020

Penulis

APPLICATION OF ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM FOR IMAGE ENCRYPTION AND DECRYPTION ON .BMP AND .PNG FILE

By:

YUSTI QOMAH
08011281520093

ABSTRACT

An image is a representasion of an object that produced from data recording system. In transferring and receiving image, the information contained in the image can be known by unwanted people. Cryptography is used to secure data. .bmp and .png are files that have large sizes because of their good quality. This study uses AES cryptography algorithm is used to encrypt and decrypt .bmp and .png file. Histogram analysis results of the .bmp image encryption show a significant difference between the plain image and the encrypted image for each of the red, green, and blue channels. Histogram analysis on .png image also show significant difference beetwen the plain image and the encrypted image, so the information in the image is difficult to know. Encrypted image have a larger size than the plain image, both in .bmp and .png image. From the histogram analysis and encryption results, can be concluded that the AES algorithm is good for .bmp and .png image encryption and decryption.

Keywords: *Cryptography, Encryption, Decryption, Advanced Encryption Standard*

Pembimbing Kedua

Drs. Ali Amran, M.T
NIP. 19661213199402 2 001

Pembimbing Utama

Anita Desiani, M.Kom
NIP. 19771211200312 2 002

Mengetahui
Ketua Jurusan Matematika

Drs. Sugandi Yahdin, M.M
NIP. 19580727 198603 1 003

PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK ENKRIPSI DAN DEKRIPSI CITRA BERFORMAT .BMP DAN .PNG

Oleh:

YUSTI QOMAH
08011281520093

ABSTRAK

Citra merupakan suatu representasi dari suatu objek yang dihasilkan dari sistem perekaman data. Dalam penyampaian dan penerimaan citra, informasi yang terkandung di dalam citra bisa diketahui oleh pihak yang tidak diinginkan. Kriptografi digunakan untuk mengamankan data. Format .bmp dan .png adalah format yang memiliki ukuran file besar karena kualitasnya yang baik. Penelitian ini menggunakan algoritma kriptografi AES digunakan untuk mengenkripsi dan dekripsi citra .bmp dan .png. Hasil analisis histogram pada enkripsi citra .bmp menunjukkan perbedaan yang signifikan antara citra asli dengan citra terenkripsi untuk setiap kanal red, green, dan blue. Analisis histogram pada citra berformat .png juga menunjukkan perbedaan yang signifikan antara citra asli dengan citra terenkripsi, sehingga informasi di dalam citra sulit untuk diketahui. Citra terenkripsi memiliki ukuran file lebih besar dari citra asli, baik dalam format .bmp maupun .png. Dari analisis histogram dan hasil enkripsi, dapat disimpulkan bahwa algoritma AES cukup baik untuk enkripsi dan dekripsi citra berformat .bmp dan .png.

Kata Kunci: *Kriptografi, Enkripsi, Dekripsi, Advanced Encryption Standard*

Pembimbing Kedua

Drs. Ali Amran, M.T
NIP. 19661213199402 2 001

Pembimbing Utama

Anita Desiani, M.Kom
NIP. 19771211200312 2 002

Mengetahui
Ketua Jurusan Matematika

Drs. Sugandi Yahdin, M.M
NIP. 19580727 198603 1 003

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Informasi tidak hanya berbentuk teks. Gambar, audio, video juga adalah bentuk dari informasi yang menjadi objek dari sebuah komunikasi. Dalam penyampaian dan penerimaan informasi berbentuk gambar, informasi yang ingin disampaikan bisa diketahui terlebih dahulu oleh pihak yang tidak dikenal sebelum sampai kepada penerima informasi yang seharusnya. Andini dan Magdalena (2017) menyatakan bahwa teknik kriptografi mampu mengatasi tingkat kemanan yang rendah dalam proses komunikasi.

Beberapa pihak seperti kepolisian memanfaatkan teknik kriptografi untuk mengamankan data rahasia. Kriptografi awalnya hanya digunakan untuk merahasiakan pesan teks. Seiring perkembangan zaman, kriptografi mulai banyak diaplikasikan pada berbagai jenis dokumen digital yang bersifat rahasia, salah satunya citra (gambar). Citra merupakan suatu representasi, kemiripan, atau imitasi dari suatu objek yang dihasilkan dari sistem perekaman data. Sebuah citra bisa bersifat optik, analog ataupun digital (Murni, 1992). Berdasarkan warnanya, format file citra dibagi menjadi lima, yaitu Bitmap (.bmp), Tagged Image Format (.tif, .tiff), Protable Network Graphics (.png), Joint Photographic Experts Group (.jpg, .jpeg), dan Graphics Interchange Format (.gif) (Putra, 2010).

Murni (1992) menjelaskan bahwa gambar dengan format .bmp memiliki ukuran yang sangat besar, karena tidak terkompresi. Format .png juga mempunyai ukuran yang besar dan kualitas gambar yang baik. Walaupun format .png adalah

format untuk menyimpan citra terkompresi, data yang terkandung di dalam gambar tidak hilang. Format .bmp dan .png memiliki ukuran lebih besar dari format lain seperti .jpg dan .gif.

Advanced Encryption Standard (AES) adalah algoritma yang sering digunakan dalam kriptografi, dimana AES menerapkan kunci simetrik (Stallings, 2004). Beberapa penelitian mengenai algoritma AES di antaranya Arif dan Mandarini (2016) yang mengaplikasikan algoritma AES pada *Short Message Service* (SMS), Medina *et al*. (2018) menggunakan AES untuk ekripsi teks dan gambar, Goyal *et al*. (2018) dan Harahap, dkk (2016) melakukan enkripsi dan dekripsi teks menggunakan algoritma AES, sedangkan Siledar *and* Tayde (2015) menggunakan file .jpg untuk enkripsi dan dekripsi menggunakan AES. Beberapa penelitian yang menggunakan algoritma AES banyak diaplikasikan pada teks.

Ahmed *et al.* (2017) menyimpulkan bahwa hasil enkripsi menggunakan algoritma AES memiliki tingkat keacakannya yang tinggi. Hameed *et al*. (2018) juga menyatakan bahwa AES memerlukan waktu yang singkat untuk melakukan enkripsi dan dekripsi dengan tingkat kemanan yang tinggi. Dengan beberapa kelebihan AES, penelitian ini menerapkankan algoritma AES untuk enkripsi dan dekripsi file citra berformat .bmp dan .png.

1.2 Perumusan Masalah

Bagaimana menerapkan algoritma AES untuk mengenkripsi data atau file citra berformat .bmp dan .png.

1.3 Pembatasan Masalah

1. Citra bujur sangkar dan berwarna yang berformat .bmp dan .png dengan maksimal 512 x 512 piksel.
2. Menggunakan analisis histogram untuk mengukur tingkat kemanan.

1.4 Tujuan

Menerapkan algoritma AES untuk mengenkripsi data atau file citra berformat .bmp dan .png.

1.5 Manfaat

1. Dapat melakukan enkripsi dan dekripsi pada file yang dianggap rahasia.
2. Sebagai referensi dan wawasan tambahan mengenai penggunaan bahasa pemrograman java untuk penerapan kriptografi terutama dalam enkripsi file citra.

DAFTAR PUSTAKA

Ahmed, Falah Y.H., Omar Farook Mohammad., Subhi R.M. Zeebaree. 2017. A Survey and Analysis of the Image Encryption Methods. *International Journal of Applied Engineering Research* Vol. 12 (No. 23): 13265–13280.

Andini, Nur dan Rita Magdalena. 2017. Analisa dan Implementasi Teknik Kriptografi pada Citra Digital Menggunakan Kriptografi Visual. *E-Proceeding of Engineering* Vol. 4 (No.1): 420–427.

Arif, Ahmad dan Putri Mandarini. 2016. Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) 128 Bit pada Sistem Keamanan Short Message Service (SMS) Berbasis Android. *Jurnal TEKNOIF* Vol. 4 (No. 1): 84-93.

Astuti, I F., Awang H K., Fresly N P. 2015. Implementasi Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarman* Vol. 10 (No.1): 20–31.

Blanchet, Gerard and Maurice Charbit. 2006. *Digital Signal and Image Processing using MATLAB*. ISTE Ltd: London.

FIPS 197. 2001. *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Information 197.

Gonzales, Rafael C and Richard E Woods. 1992. *Digital Image Processing*. Prentice Hall: New Jersey.

Goyal, Nandini., et al. 2018. Text Encryption and Decryption using AES Algorithm. *International Journal of Electronics, Electrical and Computational System* Vol. 7 (No.3): 638-643.

Harahap, Erwin., Aditia Rahmat Tulloh., Yurika Permanasari. 2016. Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. *Jurnal Matematika UNISBA* Vol. 15 (No.1): 7-13.

Hameed, Mustafa Emad., Masrullizam Mat Ibrahim., Nurulfajar Abd Manap. 2018. Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution, Differential Cryptanalysis and Level of
Security. *Journal of Telecommunication, Electronic and Computer Engineering* Vol. 10 (No.1): 139-145.

Jantan, Aman and Mohammad Ali Bani Younes. 2008. An Image Encryption Approach Using a Combination of Permutation Technique Followed by

Encryption. *International Journal of Computer Science and Network Security*. Vol. 8 (No. 4): 191–197.

Levkine, Guennadi. *Test Image Collections*. https://www.hlevkin.com/06testimages.htm. (Mei 2019).

Medina, Ruji P, Ariel M Sison, Heidilyn V Gamido. 2018. Modified AES for Text and Image Encryption. *Indonesian Journal of Electrical Engineering and Computer Science* Vol. 11 (No.3): 942–948.

Murni, Aniati. 1992. *Pengantar Pengolahan Citra*. Elex Media Komputindo: Jakarta.

Putra, D. 2010. *Pengolahan Citra Digital*. Andi Offset: Yogyakarta.

Schneier, Bruce. 1996. *Applied Cryptography*. John Wiley & Son: New York.

Setyaningsih, Emi. 2015. *Kriptografi dan Implementasinya Menggunakan MATLAB*. Andi Offset: Yogyakarta

Siledar, Seema and Suchita Tayde. 2015. File Encryption, Decryption Using AES Algorithm in Android Phone. *International Journal of Advanced Research in Computer Science and Software Engineering* Vol. 5 (No. 5): 550-554.

Stallings, William. 2004. *Cryptography and Network Security Principles and Practices*. Pearson Education: New Delhi.

USC. *The USC-SIPI Image Database*. http://sipi.usc.edu/database/database.php. (Mei 2019).

Zunaidi, Muhammad dan Suharsil. 2018. Pengamanan Citra Digital Menggunakan Kombinasi antara Algoritma AES dan Metode LSB. *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD* Vo. 1 (No.2): 36-45.