Perbandingan Algoritma AES dan Algoritma XTEA Pada Pengamanan File Audio

Diajukan sebagai Syarat Untuk Menyelesaikan

Pendidikan Program Strata-1 pada

Jurusan Teknik Informatika

Oleh :

Septa Nopita Sari

NIM:09021281320027

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2019

LEMBAR PENGESAHAN TUGAS AKHIR

PERBANDINGAN ALGORITMA AES DAN ALGORITMA XTEA PADA PENGAMANAN FILE AUDIO

Oleh :

SEPTA NOPITA SARI
NIM : 09021281320027

Indralaya, Oktober 2019

Pembimbing I,	Pembimbing II,
Drs.Megah Mulya ,M.T.	Osvari Arsalan,M. T.
NIP 196602202006041001	NIP 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, M.T
NIP 197706012009121004

ii

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Jumat tanggal 04 Oktober telah dilaksanakan sidang tugas akhir oleh Jurusan Teknik Informatikan Fakultas Ilmu Komputer Universita Sriwijaya.

Nama : Septa Nopita Sari
NIM : 09021281320027
Judul : Perbandingan Algoritma AES dan Algoritma XTEA pada Pengamanan File Audio

1. Pembimbing I

   Drs. Megah Mulya, M.T
   NIP. 196602202006041001 .....

2. Pembimbing II

   Osvari Arsalan ,M. T.
   NIP. 198806282018031001 .....

3. Penguji I

   Yunita, M.Cs.
   NIP. 198306062015042002 .....

4. Penguji II

   Alvi Syahrini Utami, M.Kom.
   NIP. 197812222006042003 .....

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, M.T
NIP 197706012009121004

iii

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Septa Nopita Sari
NIM	: 09021281320027
Program Studi	: Teknik Informatika
Judul Skripsi	: Perbandingan Algoritma AES dan ALgoritma XTEA pada Pengamanan File Audio
Hasil Pengecekan Software *iThenticate/Turnitin*	: 20 %

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Indralaya, Oktober 2019

Septa Nopita Sari

NIM. 09021281320027

MOTTO

Bismillahirrohmanirrohim..

“Janganlah pernah menyerah ketika anda masih mampu berusaha lagi. Tidak ada kata berakhir sampai anda berhenti mencoba” – Brian Dyson

SEMANGAT

Kupersembahkan Hasil Karyaku Ini Kepada :

- **Orang tuaku**
- **saudarahku**
- **Sahabat dan Teman-Teman IF Reguler 2013**

COMPARISON OF AES ALGORITHM AND XTEA ALGORITHM IN AUDIO FILE SAFETY

Oleh :

SEPTA NOPITA SARI

NIM : 09021281320027

ABSTRACT

Information security is one of the absolute things that must be fulfilled in the development of the digital world and information technology, including audio files. Many developed algorithms are considered to have strong security that can be applied in securing audio file data such as the AES algorithm or the XTEA algorithm. However, to determine a good algorithm is not only seen from strong security, other factors that need to be taken into account are the speed and balance are the same before and after the encryption and decryption process. Therefore in this study a comparison of the computation time of AES and XTEA algorithms is performed in encrypting and decrypting, as well as the balance of the file before it is encrypted and after decryption. The data used are audio files of various sizes. From the research conducted obtained results for the average time of encryption of the two black algorithms for AES 136070,177 Ms and 123770.36 Ms for XTEA. For the average decryption time of the two algorithms 112201.22332 Ms for AES and 94951.5793 Ms for XTEA. As for the security of the algorithm (*avalanche effect*) the two algorithms used are safe namely the average percentage has reached half (45%). And for the balance of the file before and after the decrypted return the same result that can be played back as before.

Keywords: Encryption, Decryption, Audio Files, AES Algorithm, XTEA Algorithm.

PERBANDINGAN ALGORITMA AES DAN ALGORITMA XTEA DALAM PENGAMANAN FILE AUDIO

Oleh :

SEPTA NOPITA SARI

NIM : 09021281320027

ABSTRAK

Keamanan informasi merupakan salah satu hal yang mutlak yang harus dipenuhi dalam perkembangan dunia digital dan teknologi informasi, tidak terkecuali pada file audio. Banyak algoritma yang dikembangkan dianggap memiliki keamanan yang kuat yang dapat diterapkan dalam pengamanan data file audio seperti algoritma AES atau algoritma XTEA. Namun, untuk menentukan algoritma yang baik tidaklah hanya dilihat dari keamanan yang kuat, factor lain yang perlu diperhitungkan yaitu kecepatan dan keseimbangan apakah sama sebelum dan sesudah dilakukannya proses enkripsi dan dekripsi. Oleh karena itu pada penelitian ini dilakukan perbandingan kecepatan algoritma AES dan XTEA dalam melakukan enkripsi dan dekripsi , serta keseimbangan file sebelum di enkripsi dan sesudah didekripsi. Data yang digunakan adalah file audio dengan berbagai ukuran. Dari penelitian yang dilakukan diperoleh hasil untuk waktu rata-rata enkripsi kedua algoritam untuk AES 136070,177 Ms dan 123770,36 Ms untuk XTEA. Untuk waktu rata-rata dekripsi kedua algoritma 112201,2332 Ms untuk AES dan 94951,5793 Ms untuk XTEA. Sedangkan untuk keamanan algoritma (*avalanche effect*) kedua algoritma yang digunakan ini aman yaitu persentase rata-rata sudah mencapai separuhnya (45%). Dan untuk keseimbangan file sebelum dan sesudah di dekripsikan kembali hasilnya sama yaitu bisa di putar kembali seperti semula.

Kata kunci : Enkripsi, Dekripsi, *File Audio*, Algoritma AES, Algoritma XTEA.

KATA PENGANTAR

Bismillahirrohmaanirrohim, Alhamdulillaahirobbil 'aalamiin...

Penulis ucapkan atas kehadirat Allah Subhanahu wa Ta'ala yang penuh rahmat dan sholawat teriring salam penulis lantunkan *Allahumma sholli 'ala muhammad.* Semoga senantiasa senantiasa tercurah kepada Rasulullah Muhammad Shollahu 'alaihi wa sallam, beserta keluarga dan para sahabat yang berperan penting dalam peradaban manusia hingga saat ini. Tugas akhir dengan judul ***"Perbandingan Algoritma AES dan Algoritma XTEA pada Pengamanan File Audio"*** ini dapat diselesaikan penulis untuk memenuhi salah satu syarat pendidikan program Strata-I pada Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada pihak-pihak yang telah berperan dalam menyelesaikan tugas akhir ini. Pihak-pihak tersebut antara lain :

1. Bapak Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya beserta jajarannya.
2. Bapak Rifkie Primartha, M.T. selaku Ketua Jurusan Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya sekaligus sebagai penguji tugas akhir.
3. Bapak Drs. Megah Mulya, M.T. dan Osvari Arsalan, M. T., selaku pembimbing tugas akhir di Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberikan bimbingan dan arahan dalam proses pengerjaan tugas akhir.
4. Ibu Yunita, M.Cs. dan Ibu Alvi Syahrini Utami, M.Kom selaku dosen penguji tugas akhir yang telah memberikan masukan agar tugas akhir ini lebih baik lagi.
5. Ibu Novi Yusliani, M.T selaku pembimbing Akademik di Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Seluruh Dosen Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberikan ilmu pengetahuan kepada penulis selama kegiatan akademik berlangsung.
7. Seluruh Karyawan dan Karyawati Fasilkom UNSRI yang telah membantu dalam urusan administrasi selama kegiatan akademik.
8. Keluarga besar penulis khususnya orangtua, Ayahku Sudi Hartono dan Ibuku Kurnili Wati, saudaraku Derli Antoni dan Anggi Pirioska yang telah banyak memberikan doa,

dukungan moril dan materil kepada penulis selama penyelesaian tugas akhir hingga selesai.

9. Sahabat Penulis Heny Maryani, mutiara sefa, Buk yeye, mbak ade, dian lukita sari, monica putra, Dewi Putri Siagian, lidya panjaitan, winta sari, meila, bela, kak adit, kak rici, zhita, nadia, Husnita Mala, Suyatmi, Yeye, Lisa, Ayu dan Kiki yang menemani dan membantu proses tugas akhir.

10. Untuk semua teman Diskusi yang memberikan ilmu, semangat, dan bantuan untuk penyelesaian dokumentasi tugas akhir.

12. Kakak-kakak dan adik-adik yang penulis kenal dan sayangi di Universitas Sriwijaya.

14. Seluruh pihak yang telah membantu dalam penyusunan dan penyempurnaan tugas akhir ini yang tidak dapat disebutkan satu-persatu.

Penulis menyadari banyak kekurangan dari proposal ini, penulis mengharapkan saran dan tanggapan yang membangun dari semua pihak dan semoga tugas akhir ini dapat bermanfaat bagi pembaca dan perkembangan ilmu bidang steganografi dengan gabungan kriptografi serta dapat memberikan masukan sebagai sumbangan pikiran dalam rangka peningkatan mutu dalam pembelajaran. Aamiin.

Indralaya, Oktober 2019

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini membahas tentang latar belakang masalah, rumusan masalah, tujuan penelitian, dan batasan masalah. Bab ini juga menjelaskan secara umum tentang keseluruhan penelitian. Pendahuluan dimulai dengan penjelasan mengenai latar belakang masalah dimana algoritma yang digunakan dapat menyelesaikan kasus keamanan data file audio berdasarkan penelitian yang telah dilakukan sebelumnya. Setelah mengetahui permasalahan, maka dari permasalahn tersebut perlu dilakukan perbandingan antara algoritma AES (*Advanced Encryption Standard)* dan algoritma XTEA (*Extended Tiny Encryption Algorithm*).

1.2 Latar Belakang Masalah

Teknologi informasi merupakan suatu media yang dapat membantu manusia dalam membuat, mengubah, menyimpan, mengelola data, mengomunikasikan data/atau menyebarkan informasi. Tujuan dari adanya teknologi informasi ini sendiri adalah agar bisa membantu dalam memecahkan suatu masalah, membuka kreatifitas, meningkatkan efektifitas dan efisiensi dalam aktivitas manusia. Salah satu pekerjaan manusia yang sangat terbantu dengan adanya teknologi informasi yaitu pekerjaan manusia dalam mengamankan data.

Masalah keamanan data merupakan salah satu aspek penting dalam teknologi informasi. Salah satu solusi yang ditawarkan untuk menjaga keamanan data yaitu kriptografi. Kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti, kerahasian data, keabsahan data, integritas data, serta autentikasi data (A Menezes, Oorschot and Vanstone, 1996). Untuk menjaga keamanan data digunakan enkripsi dan dekripsi yang gunanya untuk membuat data ataupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak atau memiliki kunci.

Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi saat ini. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin keamanan data dan kerahasian informasi. kriptografi menjadi ilmu yang sangat berkembang pesat, dalam waktu yang singkat banyak bermunculan algoritma-algoritma yang dianggap lebih unggul dari pendahulunya, salah satunya adalah algoritma simetri seperti algoritma *DES (Data Encryption Standard), Blowfish, IDEA, AES, XTEA, MARS.* Dari sekian banyak algoritma yang ada, dipilihlah dua algoritma yang akan dibandingkan dalam penelitian ini yaitu, algoritma AES *(Advanced Encryption Standard)* dan algoritma XTEA *(Extended Tiny Encryption Algorithm).*

Algoritma AES (*Advanced Encryption Standard*) merupakan algoritma kunci simetris, yaitu algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses dekripsi. Penggunaan algoritma AES ini karena memiliki tingkat keamanan yang cukup tinggi. Hal ini berdasarkan penelitian yang

dilakukan oleh A Raji Reddy dan Mohan H.S (2011) yaitu *Performance Analysis Of AES and MARS Encryption Algorithms* yang menyatakan bahwa AES memiliki keamanan yang lebih tinggi dari MARS. Dan juga berdasarkan penelitian M Anand Kumar (2012) yaitu *Performance the Efficiency of Blowfish and Rejindael (AES) Algorithms* yang menyatakan bahwa pada saat sistem membutuhkan keamanan yang tinggi AES dapat digunakan dibandingkan Blowfish yang memiliki performa yang lebih bagus namun tingkat keamanannya masih dibawah AES.

Algoritma XTEA (*Extended Tiny Encryption Algorithm*) merupakan algoritma *block cipher* yang dirancang oleh Wheeler dan Roger Needhan dari *Cmbridge Computer Laboratory* pada tahun 1977. XTEA beroperasi dalam ukuran blok 64 *bit* dan panjang kunci 128 *bit*. Bentuk *feistel*nya pun masih sama, yang membedakan adalah fungsi *feistel* dan penjadwalan kunci yang digunakan. Pada XTEA, pada ronde ganjil digunakan K[sum & 3], sedangkan pada ronde genap digunakan K[sum >>11&3]. XTEA menggunakan angka delta yang sama dengan TEA. Pada dekripsi, variabel sum diinisialisasi dengan nilai 0xc6ef3720=delta*32=delta<<5.

Pada penelitian sebelumnya yang diteliti oleh Niladree De dan Jaydeb Bhaumik (2012) yaitu *A Modified XTEA* menyatakan bahwa arsitektur XTEA yang sudah dimodifiikasi sesuai untuk perangkat dimana biaya rendah dan konsumsi daya rendah. Berdasarkan penelitian dari Arsalan dan Achmad Imam Kistijantoro (2015) yaitu *Modification Of Key Scheduling For Security Improvement In XTEA* menyatakan bahwa strategi perbaikan algoritma XTEA

dapat dilakukan dengan memodifikasi penjadwalan kunci menjadi penjadwalan dinamis dengan perbedaan distribusi utama rata-rata 73,33% atau rata 46 putaran berbeda dari total 64 ronde untuk masing-masing penggunaan tombol master yang berbeda. Dan juga berdasarkan penelitian Vignesh Ballal, Kiran Kumar V.G , Meghan dan Shanta Rama Rai (2017) yaitu *A Study Comparation of Lightweight Cryptographic Algorithm* menyatakan bahwa algoritma XTEA memiliki konsumsi daya yang lebih sedikit dibandingkan blowfish, area blowfish lebih besar dari XTEA, *delay gate* blowfish lebih besar dari XTEA. Oleh karena itu algoritma XTEA adalah algoritma terbaik dan sesuai di antara kedua algoritma.

Untuk membuktikan keamanan dari kedua algoritma tersebut maka diperlukan media sebagai data yang akan diamankan. Pengamanan data dapat dilakukan pada semua format yang ada dalam komputer seperti *format teks, format image, format audio dan format video.* Dalam penelitian ini yang digunakan adalah *format audio MP3*. *Format audio mp3* adalah salah satu *format audio* yang paling sering digunakan dalam penyimpanan data karena data yang disimpan menyerupai data asli, dan ukurannya tidak terlalu besar dibandingkan dengan *format* lain.

Berdasarkan latar belakang diatas maka diperlukan sebuah aplikasi sistem kriptografi yang menerapkan algoritama AES dan algoritma XTEA untuk proses enkripsi dan dekripsi *file audio MP3*. *File audio mp3* yang terenkripsi nantinya tidak dapat diputar lagi sehingga diperlukan aplikasi untuk mendekripsikan *file audio mp3* tersebut agar dapat diputar seperti semula.

1.3 Rumusan Masalah

Rumusan masalah dalam penelitain ini adalah :

1. Bagaimana membangun aplikasi yang mengimplementasikan algoritma AES dan algoritma XTEA
2. Apakah algoritma yang digunakan aman, bagaimanan perbandingan waktu enkripsi dan dekripsinya, serta apakah file sebelum di enkripsi sama dengan sesudah dekripsi?.

1.4 Tujuan Penelitian

Adapun Tujuan dari penelitian ini adalah :

1. Membangun sebuah aplikasi yang menerapkan algoritma algoritma AES dan algoritma XTEA dalam proses enkripsi dan dekripsi.
2. Untuk mengetahui tingkat keamanan algoritma (*avalanche effect*), waktu enkripsi dan dekripsi, dan kesamaan file sebelum enkripsi dengan file sesudah dekripsi.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Dapat membantu pengguna dalam memahami algoritma AES dan algoritma XTEA dalam mengamankan *file audio mp3*.

2. Membantu pengguna dalam menambah informasi tentang algoritma mana yang lebih efisien dan tingkat keamanannya yang lebih baik diantara kedua algoritma tersebut.

1.6 Batasan Masalah

Batasan masalah penelitian ini adalah :

1. File masukan berupa file audio format Mp3.
2. Ukuran file maksimal 10 Mb.
3. Menggunakan data sekunder yaitu file audio yang diakses dari internet sebanyak 25 file audio .

Indikator yang digunakan untuk membandingkan keunggulan algoritma yang dapat dilihat dari efisien waktu dan *avalanche effect* pada

DAFTAR PUSTAKA

Ami, Aisiah Ibrahim, 2017. *Perancangan Pengamanan Data Mengggunkan Algoritma AES*. Tanggerang : Jurnal Teknik Informatika STMIK Antar Bangsa. Vol 3 No 1, Februari 2017.

Ballal, Vignesh.dkk, 2017. *A Study and Comparison Of Lightweight Cryptographic Algorithm.*India : *IOSR Jurnal Of Electronic and Comunication Engineering (IOSR-JECE).* Vol.12, issue 4, juli-agustus 2017.

Barong, J., Unmul, K., Kelua, G., Samarinda, S., & Internet, J. (2009). Sebagai Algoritma Kriptografi yang Aman, *4*(3), 7–14.

De, Niladree, dkk, 2012. *A Modified XTEA*.india: *International Jurnal of soft Computing and Enginerring (IJSCE).* Vol.2. issue .2, may 2012.

Engineering, C. (2017). Website : www.ijircce.com A Study on Data Encryption Using AES and, 8807–8811. https://doi.org/10.15680/IJIRCCE.2017.

Ibrahim, A. A. (2017). Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard), *III*(1), 53–60.

Mahajan, P., & Sachdeva, A. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security, *13*(15).

Mulawarman, J. I., Pabokory, F. N., Astuti, I. F., Kridalaksana, A. H., Studi, P., Komputer, I., … Dokumen, I. F. (2015). Implementasi Kriptografi Pengaman Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma *Advanced Standard* (AES), *10*(1).

Murdowo, S. (n.d.). Mengenal Proses Perhitungan Enkripsi Menggunakan Algoritma Kriptografi *Advanced Encryption Standard* (AES), 32–40.

Menezes, A.J, Paul C.Van Oorscgot dan Scott A.Vanstone.1996.*Handbook of Applied Cryptography. Cryptography, CRC Press, Boca Raton, New York.*

Nwe, Tin Z.dkk, 2014. *Performance Analysis of RSA and Elgamal for Audio Security.* Myanmar: *International Jurnal of Scientific and Technology Research.* Vol.03 Issue 11, june 2014.

O . Arsalan, A.I. Kistijantoro, 2015. *Modification of Key Scheduling For Security Improvement in XTEA.* Surabaya : 2015 *International Conference on Information & Communication Technology and System* (ICTS). Pp. 231-236, September 2015.

Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms : DES ,. *Procedia - Procedia Computer Science*, *78*(December 2015), 617–624. https://doi.org/10.1016/j.procs.2016.02.108

S, Mohan H. dkk, 2011. *Performance Analysis of AES and MARS Encryption Algorithms.* India : *International Jurnal Of Computer Science Issues.* Vol.8 Issue 4 No 1, july 2011.

Science, C. (2013). *A Crypt Analysis of the Tiny Encryption Algorithm in Key Generation*. Mohammad Shoeb , Vishal Kumar Gupta, *1*(38), 123–128.

Shoeb, Muhammad dkk, 2013. A crypt analysis of the tiny encryption algorithm in key generation. *International Journal of Communication and Computer Technologies*.Volume 01 – No.38, Issue: 05 May 2013

Singh, G. (2013). A Study of Encryption Algorithms (RSA , DES , 3DES and AES) for Information Security, *67*(19), 33–38.

Sudharto, J. P. (n.d.). Aplikasi enkripsi dan dekripsi meggunakan algoritma rijndael, 1–21.

Wheeler, D. J. (1994). Studi Mengenal Tiny Encryption Algorithm (TEA) dan Turun-turunannya (XTEA dan XXTEA),1-6.