ANALISIS KINERJA ALGORITMA MODIFIED AES DENGAN *ADJUSTED SHIFTROWS* DAN *BIT-PERMUTATION* PADA *SMARTPHONE* ANDROID

OLEH :

NUR RACHMAT

09042681620003

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018

ANALISIS KINERJA ALGORITMA MODIFIED AES DENGAN *ADJUSTED SHIFTROWS* DAN *BIT-PERMUTATION* PADA *SMARTPHONE* ANDROID

TESIS

Diajukan untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

OLEH :

NUR RACHMAT

09042681620003

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2018

LEMBAR PENGESAHAN

ANALISIS KINERJA ALGORITMA MODIFIED AES DENGAN *ADJUSTED SHIFROWS* DAN *BIT-PERMUTATION* PADA *SMARTPHONE* ANDROID

Diajukan untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

OLEH :
NUR RACHMAT
09042681620003

Palembang, Desember 2018

Pembimbing

Samsuryadi, M.Kom., Ph.D.
NIP. 197102041997021003

Mahasiswa

Nur Rachmat
NIM. 09042681620003

Mengetahui,
Koordinator Program Studi Magister Teknik Informatika

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Pada hari Selasa tanggal 18 Desember 2018 telah dilaksanakan ujian sidang Tesis II oleh Magister Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

N a m a	:	Nur Rachmat
N I M	:	09042681620003
Judul	:	Analisis Kinerja Algoritma Modified AES dengan *Adjusted Shiftrows* dan *Bit-Permutation* pada *Smartphone* Android

1. Pembimbing

Samsuryadi, M.Kom., Ph.D.
NIP. 197102041997021003

2. Penguji I

Prof. Dr. Ir. Siti Nurmaini, M.T.
NIP. 196908021994012001

3. Penguji II

Dr. Reza Firsandaya Malik, M.T.
NIP. 197604252010121001

Mengetahui,
Koordinator Program Studi Magister Teknik Informatika

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

LEMBAR PERNYATAAN

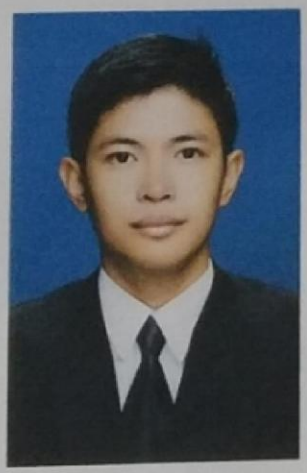
Yang bertanda tangan di bawah ini :

Nama	: Nur Rachmat
NIM	: 09042681620003
Program Studi	: Magister Teknik Informatika
Judul Tesis	: Analisis Kinerja Algoritma Modified AES dengan *Adjusted Shiftrows* dan *Bit-Permutation* pada *Smartphone* Android

Hasil Pengecekan Software iThenticate/Turnitin : **10 %**

Menyatakan bahwa laporan tesis saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tesis 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.



Palembang, Desember 2018

METERAI TEMPEL CC555AFF504087247 6000 ENAM RIBU RUPIAH

(Nur Rachmat)

NIM. 09042681620003

LEMBAR PERNYATAAN

KATA PENGANTAR

Puji dan syukur kepada Tuhan karena atas segala rahmat-Nya, penulis dapat menyelesaikan tugas akhir ini. Tugas akhir yang berjudul **"Analisis Kinerja Algoritma Modified AES dengan *Adjusted Shiftrows* dan *Bit-Permutation* pada *Smartphone* Android"** ini disusun untuk memenuhi salah satu persyaratan kelulusan tingkat S2 pada Jurusan Magister Teknik Informatika Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih yang tak terhingga kepada pihak-pihak telah memberikan dukungan, bimbingan, motivasi dan kemauan kepada penulis untuk menyelesaikan tesis ini, yaitu kepada:

1. Allah SWT
2. Kedua orang tua, Istri dan Saudara serta jagoan kecilku M. Akhsan Alkhantara dan M. Ikhsan Albhiantara, yang telah memberi motivasi dalam diri penulis untuk menyelesaikan perkuliahan di akhir semester ini.
3. Yayasan MDP dan STMIK GI MDP Palembang yang telah memberikan kesempatan kepada Penulis untuk melanjutkan pendidikan di Fasilkom Universitas Sriwijaya.
4. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. Sukemi, M.T., selaku Koordinator Program Studi Magister Teknik Informatika.
6. Bapak Samsuryadi, M.Kom., Ph.D., selaku dosen pembimbing yang telah sabar membimbing dan membantu penulis.

7. Bapak dan Ibu Dosen yang selama ini telah melimpahkan ilmunya kepada penulis selama proses belajar mengajar di Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Bapak Johannes Petrus, S.Kom., M.T.I., selaku Ketua STMIK GI MDP yang telah memberikan dukungan kepada penulis untuk menyelesaikan studi S2 di Universitas Sriwijaya.
9. Teman-teman Magister Teknik Informatika angkatan 2016, untuk persahabatan dan masa-masa perkuliahan yang menyenangkan dan tak terlupakan.
10. Teman-teman civitas akademika Fakultas Ilmu Komputer Universitas Sriwijaya dan Kampus MDP atas dukungan dan doanya.
11. Untuk semua pihak yang telah membantu penyelesaian tesis ini dan tidak dapat disebutkan satupersatu.

Akhir kata, penulis menyadari bahwa tesis ini jauh dari kata sempurna. Untuk itu penulis mengharapkan kritik dan saran yang membangun dari semua pihak untuk penyempurnaan tesis ini dan semoga tesis ini dapat bermanfaat bagi pihak yang membutuhkan.

Palembang, Desember 2018

Penulis

ANALISIS KINERJA ALGORITMA MODIFIED AES DENGAN *ADJUSTED SHIFTROWS* DAN *BIT-PERMUTATION* PADA *SMARTPHONE* ANDROID

Nur Rachmat

Abstrak

Upaya untuk melindungi kerahasiaan data khususnya pesan pada *smartphone* Android adalah dengan teknik enkripsi. Beberapa algoritma yang cukup terkenal dan banyak digunakan masih memiliki kinerja yang cukup tinggi pada penggunaan memori dan CPU. Sementara itu s*martphone* Android memiliki sumber daya yang terbatas, sehingga upaya untuk meningkatkan kinerja algoritma pada *platform* Android perlu dilakukan. Berbagai upaya untuk meningkatkan performa algoritma Modified AES telah dilakukan, salah satunya adalah menggunakan tahapan *Adjusted ShiftRows* dan *Bit-Permutation*. Penelitian ini menggabungkan tahapan *Adjusted ShiftRows* dan *Bit-Permutation* ke dalam tahapan algoritma Modified AES dan membandingkan kinerja algoritma Modified AES dengan algoritma Rijndael, Serpent dan Twofish pada panjang kunci 128 bit dan 256 bit. Serta menentukan algoritma yang paling optimal untuk diimplementasikan pada *smartphone* Android. Hasil penelitian didapatkan algoritma Modified AES dengan *Adjusted ShiftRows* dan *Bit-Permutation* menunjukkan peningkatan efisiensi dan kinerja karena waktu enkripsi yang lebih cepat serta mengurangi penggunaan memori dan CPU sehingga algoritma ini layak untuk diterapkan pada *smartphone* Android.

Kata kunci : Modified AES, *Adjusted ShiftRows, Bit-Permutation,* Rijndael, Serpent, Twofish

PERFORMANCE ANALYSIS OF MODIFIED AES ALGORITHM WITH ADJUSTED SHIFTROWS AND BIT-PERMUTATION ON ANDROID SMARTPHONE

Nur Rachmat

Abstract

Efforts to protect the confidentiality of data, especially messages on Android smartphones, are by encryption techniques. Some fairly well-known and widely used algorithms still have quite high performance on memory and CPU usage. Meanwhile, Android smartphones have limited resources, so efforts to improve the performance of algorithms on the Android platform need to be done. Various efforts to improve the performance of the Modified AES algorithm have been carried out, such as using Adjusted ShiftRows and Bit-Permutation stages. This study combines the Adjusted ShiftRows and Bit-Permutation stages into the Modified AES algorithm stage and compares the performance of the Modified AES algorithm with the Rijndael, Serpent and Twofish algorithms on 128 bits and 256 bits key lengths. Furthermore determine the most optimal algorithm to be implemented on an Android smartphone. The results showed that the Modified AES algorithm with Adjusted ShiftRows and Bit-Permutation showed increased efficiency and performance due to faster encryption time, reduced memory and CPU usage, therefore this algorithm is feasible to be applied on Android smartphones.

Keyword : Modified AES, *Adjusted ShiftRows, Bit-Permutation,* Rijndael, Serpent, Twofish

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Penggunaan internet saat ini meningkat pesat. Hal ini menyebabkan peningkatan kebutuhan akan keamanan data dan informasi yang penyebarannya dibutuhkan setiap saat. Teknik enkripsi adalah salah satu hal yang sangat penting dan sangat bermanfaat untuk mengamankan pesan. Salah satu teknik enkripsi yang paling banyak digunakan adalah Rijndael (AES), (Kumar dan Rana, 2016).

Algoritma Rijndael memiliki empat tahapan utama yakni *AddRoundKey, SubBytes, ShiftRows* dan *MixColumns.* Diantara empat tahapan dalam algoritma AES, *MixColumns* membutuhkan banyak sumber daya dan komputasi yang tinggi dalam implementasinya dibandingkan dengan tahap lainnya, (Wenceslao dkk., 2015). Hal ini disebabkan *MixColumns* memiliki keamanan yang kuat pada *chipher* untuk menghindari serangan linear atau diferensial. Namun, mengganti *MixColumns* dengan proses atau tahapan alternatif dapat meningkatkan kecepatan dari algoritma AES, (Tyagi dan Priyanka, 2014).

Beberapa penelitian telah berhasil memodifikasi algoritma AES antara lain adalah (Kawle dkk., 2014) dan (Gamido dkk., 2018). Kedua penelitian tersebut mengusulkan pergantian tahapan *MixColumn* dengan *Permutation* atau *Bit-Permutation.* Tahapan ini mampu mengurangi masalah komputasi yang tinggi dari algoritma AES. Penelitian tersebut menunjukkan efisiensi waktu yang lebih baik dari algoritma AES.

Penelitian serupa yang memodifikasi algoritma AES adalah (Shtewi dkk., 2010) mengusulkan penyesuaian tahapan *ShiftRows* atau *Adjusted ShiftRows*. Performa *Adjusted ShiftRows* diklaim mampu mengurangi waktu enkripsi sehingga kinerja algoritma menjadi lebih cepat, (Dewangan dan Agrawal, 2012). Sayangnya pada penelitian (Gamido dkk., 2018) dan (Shtewi dkk., 2010) baru dilakukan untuk mengukur waktu enkripsi dan objek enkripsi berupa *file* teks dan

gambar pada perangkat *desktop* dengan panjang kunci 128 bit. Serta belum ditemukan penelitian yang menggabungkan tahapan *Adjusted ShiftRows* dan *Bit-Permutation* pada *smartphone* Android.

Penelitian perbandingan kinerja dari algoritma Rijndael, Serpent, dan Twofish pada *smartphone* (Montoya B. dkk., 2013) dan (Farisi, 2018). (Montoya B. dkk., 2013) membandingkan *benchmark* (MB/s), waktu (ms), penggunaan *memory* (KB), dan persentase penggunaan *processor* (%) pada perangkat bergerak. Hasil pengujian ini menunjukkan kinerja algoritma Twofish lebih unggul dari algoritma Rijndael dan Serpent berdasarkan pengujian *benchmark*. Sementara hasil pengujian waktu menunjukkan Serpent lebih cepat daripada algoritma Rijndael dan Twofish. Algoritma Rijndael unggul pada pengujian penggunaan CPU yang lebih rendah. Sedangkan hasil pengujian penggunaan memori menunjukkan kinerja algoritma Twofish lebih unggul. Sementara penelitian (Farisi, 2018) hanya membandingkan waktu (ms), penggunaan *memory* (KB), dan persentase penggunaan *processor* (%). Namun penelitian ini menyimpulkan bahwa algoritma Serpent memiliki kinerja terbaik dalam proses enkripsi dan dekripsi pada *smartphone* dibandingkan algoritma Twofish dan Rijndael. Sayangnya kedua penelitian ini sama-sama melakukan pengujian pada panjang kunci 128 bit.

Berdasarkan studi literatur yang telah dilakukan, penelitian ini akan mengganti tahapan *MixColumn* dengan *Bit-Permutation* dan menyesuaikan tahapan *ShiftRows* dengan *Adjusted ShiftRows* serta melanjutkan penelitian (Farisi, 2018) yang melakukan perbandingan terhadap kinerja yang diterapkan pada *smartphone* Android. Penelitian ini akan membandingkan algoritma Modified AES dengan tiga besar algoritma kandidat AES lainnya yaitu Rijndael, Serpant dan Twofish pada panjang kunci 128 bit dan 256 bit. Penelitian ini penting dilakukan untuk menemukan algoritma mana yang memiliki kinerja terbaik dalam penerapannya pada *smartphone*, sehingga dapat membantu para pengembang aplikasi dalam merancang aplikasi dengan keamanan yang tinggi dan sumber daya yang efisien.

1.2. Perumusan Masalah

Pengamanan pesan pada perangkat bergerak *(smartphone)* dapat dilakukan dengan menyematkan algoritma enkripsi. Algoritma enkripsi yang paling banyak digunakan dengan tingkat keamanan yang tinggi saat ini adalah AES. Namun masih ditemukannya masalah komputasi yang tinggi pada AES menjadikan algoritma ini harus dimodifikasi dengan berbagai pendekatan diantaranya menghilangkan tahapan *MixColumn* dan menyesuaikan tahapan *ShiftRows*.

Selain itu beberapa algoritma masih harus diuji kinerjanya pada *smartphone* antara lain adalah Rijndael, Serpent dan Twofish. Beberapa penelitian sebelumnya telah membandingkan algoritma Rijndael, Serpent dan Twofish. Namun belum dilakukan penelitian yang membandingkan beberapa algoritma tersebut pada s*martphone* Android dengan panjang kunci 256 bit.

Berdasarkan kenyataan tersebut penelitian ini akan memodifikasi algoritma AES dengan *Adjusted ShiftRows* dan *Bit-Permutation* lalu membadingkan kinerja algoritma Modified AES dengan algoritma Rijndael, Serpent dan Twofish pada *smartphone* Android pada panjang kunci 128 bit dan 256 bit. Adapun *research question* yang harus dijawab pada penelitian ini nantinya antara lain adalah :

1. Bagaimana memodifikasi algoritma Modified AES dengan *Adjusted ShiftRows* dan *Bit-Permutation?*
2. Algoritma mana yang memiliki kinerja terbaik dari 4 algoritma yang dianalisis?
3. Algoritma manakah yang paling efisien dalam hal penggunaan sumber daya pada *smartphone* Android?
4. Apakah kinerja algoritma Modified AES dengan *Adjusted ShiftRows* dan *Bit-Permutation* mampu mengungguli algoritma Rijndael, Serpent dan Twofish pada *smartphone* Android?

1.3. Batasan Masalah

Batasan masalah penelitian ini adalah :

1. Algoritma yang dibandingkan adalah Rijndael, Serpent, Twofish dan Modified AES dengan *Adjusted ShiftRows* dan *Bit-Permutation*.
2. Data yang dienkripsi dan didekripsi berupa pesan teks.
3. Panjang kunci yang digunakan pada penelitian ini adalah 128 bit dan 256 bit.
4. Pengujian dilakukan pada *smartphone* berbasis Android.
5. Parameter yang diuji adalah waktu, penggunaan *memory*, penggunaan *processor* dan panjang karakter.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Menggabungkan tahapan *Adjusted ShiftRows* dan *Bit-Permutation* pada algoritma Modified AES.
2. Membandingkan kinerja proses enkripsi dan dekripsi dari algoritma Rijndael (AES), Serpent, Twofish dan Modified AES pada *smartphone* Android pada panjang kunci 128 bit dan 256 bit.
3. Membandingkan parameter waktu, penggunaan memori, penggunaan processor (CPU) dan panjang karakter yang diuji dari algoritma Rijndael, Serpent, Twofish dan Modified AES.
4. Menganalisa hasil pengujian algoritma Modified AES dengan *Adjusted ShiftRows* dan *Bit-Permutation.*

1.5. Manfaat Penelitian

Manfaat hasil penelitian ini adalah sebagai berikut :

1. Mengetahui kinerja dari masing-masing Algoritma kriptografi pada *smartphone* Android pada panjang kunci 128 bit dan 256 bit.
2. Mengetahui kinerja dari algoritma Modified AES dengan *Adjusted ShiftRows* dan *Bit-Permutaton.*

3. Memberikan pilihan algoritma yang tepat untuk dapat digunakan para pengembang aplikasi pada *smartphone* Android dalam mengamankan isi pesan.

1.6. Sistematika Penulisan

Sistematika penulisan tesis ini terdiri dari 5 (lima) bab sebagai berikut:

BAB 1 : PENDAHULUAN

Terdiri atas latar belakang masalah, perumusan masalah, tujuan penelitian, ruang lingkup penelitian, dan sistematika penulisan.

BAB 2 : TINJAUAN PUSTAKA

Bab ini berisikan tentang teori-teori yang berkaitan dengan permasalahan yang dibahas pada penulisan tesis ini.

BAB 3 : METODOLOGI PENELITIAN

Metodologi penelitian terdiri atas metodologi yang diusulkan meliputi tahapan penelitian, pengumpulan data dan metode analisis data.

BAB 4 : HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil dan pembahasan dari data-data hasil pengujian yang telah dilakukan

BAB 5 : KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan tentang hasil yang tela diperoleh serta merupakan jawaban dari tujuan yang ingin dicapai.

DAFTAR PUSTAKA

Ammari, F.T. dan Lu, J. (2013) : Enhanced XML Encryption Using Classification Mining Technique for e-Banking Transactions, *Int. J. Inf. Retr. Res.* 3, 81–103

Ammari, F.T., Lu, J. dan Abur-rous, M. (2014a) : Securing Financial XML Transactions Using Intelligent Fuzzy Classification Techniques, *Emerg. Trends ICT Secur.* 214–326

----- (2014b) : Intelligent Banking XML Encryption Using Effective Fuzzy Logic, in *Emerging Trends in ICT Security* 591–617

Bernstein, D.J. (2015) : Crypto competitions: AES: the Advanced Encryption Standard, https://competitions.cr.yp.to/aes.html, diakses 23 Agustus 2018

Chandrasekaran, J., Subramanyan, B. dan Selvanayagam, R. (2011) : A chaos based approach for improving non linearity in S box design of symmetric key cryptosystems, in *Communications in Computer and Information Science* 132 CCIS 516–22

Dewangan, C.P. dan Agrawal, S. (2012) : A Novel Approach to Improve Avalanche Effect of AES Algorithm, *Int. J. Adv. Res. Comput. Eng. Technol.* 1, 248–52

Farisi, A. (2018) : Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone, *J. Tek. Inform. DAN Sist. Inf.* 4, 199–208

Firebase (2018) : Firebase Realtime Database | Firebase, https://firebase.google.com/docs/database/, diakses 11 September 2018

Gamido, H. V., Sison, A.M. dan Medina, R.P. (2018) : Modified AES for Text and Image Encryption, *Indones. J. Electr. Eng. Comput. Sci.* 11, 942–48

Gangadari, B.R. dan Rafi Ahamed, S. (2016) : Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications, *Healthc. Technol. Lett.* 3, 177–83

Gupta, K.C., Pandey, S.K. dan Ray, I.G. (2017) : Applications of design theory for the constructions of MDS matrices for lightweight cryptography, *J. Math. Cryptol.* 11, 85–116

Jakob Nielsen (2006) : Quantitative Studies: How Many Users to Test?, https://www.nngroup.com/articles/quantitative-studies-how-many-users/, diakses 4 September 2018

Kanitkar, V. dan Delis, A. (1997) : A Case for Real-Time Client-Server Databases, in *Real-Time Database and Information Systems: Research Advances* (Boston, MA) 395–408

Kawle, P., Hiwase, A., Bagde, G., Tekam, E. dan Kalbande, R. (2014) : Modified Advanced Encryption Standard, *Int. J. Soft Comput. Eng.* 4, 21–23

Kumar, P. dan Rana, S.B. (2016) : Development of modified AES algorithm for data security, *Opt. - Int. J. Light Electron Opt.* 127, 2341–45

Liang, S., Liu, J., Zhang, R. dan Wang, C. (2010) : A modified AES algorithm for the platform of Smartphone, *Proc. - Int. Conf. Comput. Asp. Soc. Networks, CASoN'10* 749–52

Montoya B., A.O., Munoz G., M.A. dan Kofuji, S.T. (2013) : Performance analysis of encryption algorithms on mobile devices, *2013 47th Int. Carnahan Conf. Secur. Technol.* 1–6

Puranik, D.G., Feiock, D.C. dan Hill, J.H. (2013) : Real-time monitoring using AJAX and WebSockets, in *Proceedings of the International Symposium and Workshop on Engineering of Computer Based Systems* 110–18

Rahman, M.T., Pinandito, A. dan Pramukantoro, E.S. (2017) : Perbandingan Performansi Algoritme Kriptografi Advanced Encryption Standard (AES) dan Blowfish pada Text di Platform Android, *J. Pengemb. Teknol. Inf. dan Ilmu Komput.* 1, 1551–59

Rosa, A.S. dan Shalahuddin, M. (2013) : *Rekayasa Perangkat Lunak*

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. dan Ferguson, N. (1998) : Twofish: A 128-bit block cipher, *NIST AES Propos.* 15,

Shtewi, A.A., Hasan, B.E.M., El, A. dan Hegazy, F.A. (2010) : An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems, *Int. J. Comput. Sci. Netw. Secur.* 10, 226–32

Sularsono, E., Raharjo, W.S. dan Lukito, Y. (2014) : Implementasi Algoritma Rijndael 128 Pada Aplikasi Chatting Berbasis Html5 Websocket, *J. Teknol. Komput. dan Inform.* 10, 66–79

Tyagi, N. dan Priyanka (2014) : A Survey on Ensemble of Modifications on AES Algorithm, *J. Basic Appl. Eng. Res.* 1, 19–24

Wenceslao, F. V, Gerardo, B.D. dan Tanguilig, B.I.T. (2015) : Modified AES Algorithm Using Multiple S-Boxes, in *Second International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA2015)* 5 1–9