Algoritma Simetri Rijndael 128 Pada *Real-Time Chatting* Menggunakan Teknologi *Multithreading*

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh:

Mohammad Sulthan Alif Utama
09021181621138

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN TUGAS AKHIR

ALGORITMA SIMETRI RIJNDAEL 128 PADA *REAL-TIME CHATTING* MENGGUNAKAN TEKNOLOGI *MULTITHREADING*

Oleh:

MOHAMMAD SULTHAN ALIF UTAMA
NIM: 09021181621138

Palembang, 6 Januari 2021

Pembimbing I

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

Pembimbing II

Muhammad Ali Buchari, M.T.
NIP. 198803302019031006

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Kamis tanggal 6 Januari 2021 telah dilaksanakan ujian sidang Tugas Akhir (TA) oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Mohammad Sulthan Alif Utama
NIM : 09021181621138
Judul : Algoritma Rijndael 128 Pada *Real-Time Chatting* Menggunakan Teknologi Multithreading

1. Pembimbing I

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

2. Pembimbing II

Muhammad Ali Buchari, M.T.
NIP. 198803302019031007 .....

3. Penguji I

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

4. Penguji II

Mastura Diana Marieska, MT.
NIP. 198603212018032001 .....

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	:	Mohammad Sulthan Alif Utama
NIM	:	09021181621138
Program Studi	:	Teknik Informatika
Judul Skripsi	:	Algoritma Rijndael 128 Pada *Real-Time Chatting* Menggunakan Teknologi Multithreading

Hasil Pengecekan Software *iThenticate/Turnitin* : 20%

Menyatakan bahwa Laporan Skripsi saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsri penjiplakan/plagiat dalam Laporan Skripsi 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, 20 Januari 2021

Mohammad Sulthan Alif Utama

NIM. 09021181621138

MOTTO DAN PERSEMBAHAN

MOTTO:

“Kapan Lagi”

Segala sesuatu yang baik tidak boleh ditunda. *It’s okay* ketika kita gagal mengambil keputusan karena kita akan belajar dari situ. Dan ini juga hidup pertama kita, belajarlah banyak-banyak. Jadi, kapan lagi?

-- Sulthan --

“**Maka apabila kamu telah selesai dari satu urusan maka kerjakanlah dengan sungguh-sungguh urusan yang lain”.**

(Al-Insyirah: 7)

Ku persembahkan penelitian ini kepada:

- **Papa Mahmudi Hasan, Almarhumah Mama Fatma Dalena, Farah dan Jaihan.**
- **Keluargaku tercinta**
- **Teman dan Sahabatku**
- **Fakultas dan Almamater Kebanggaanku**
- **Ilmu pengetahuan, Bangsa dan Negara**

Rijndael 128 Symmetry Algorithm in Real-Time Chatting Application Using Multithreading Technology

By:
Mohammad Sulthan Alif Utama
NIM: 09021181621138

ABSTRACT

Easy access to communication media using media such as chat application will have an impact on the security of information. The encryption of the messages is needed to reduce the possibility that the text and files are known, manipulated or stolen by public. This encryption process is called cryptography which has many algorithms, one of them is the Rijndael symmetry algorithm. This research will analyze the impact of multithreading in increasing the speed of encryption and decryption. This research using 6 types of data that consist of text and file. Each of them was tested 10 times and produced a prototype software to compare the speed of encryption and decryption and the speed of sending messages using different number of threads. From the results that have been done with 2 aspects of testing, this research found that a significant effect in the encryption and decryption process using a different number of threads.

Keyword: Cryptography, Rijndael 128, Multithreading

Palembang, January 6th 2021

Pembimbing I	Pembimbing II
Drs. Megah Mulya, M.T.	Muhammad Ali Buchari, M.T.
NIP. 196602202006041001	NIP. 198803302019031006 7

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

Algoritma Simetri Rijndael 128 Pada *Real-Time Chatting* Menggunakan Teknologi *Multithreading*

Oleh:
Mohammad Sulthan Alif Utama
NIM: 09021181621138

ABSTRAK

Mudahnya mengakses media komunikasi dengan menggunakan media seperti aplikasi *chatting* akan memberikan dampak bagi keamanan informasi. Penyandian terhadap pesan diperlukan untuk meminimalisir kemungkinan teks dan berkas tersebut diketahui, dimanipulasi atau diambil secara luas oleh orang. Proses penyandian ini disebut kriptografi yang memiliki banyak algoritma, salah satunya adalah algoritma simetri Rijndael. Penelitian ini akan menganalisa pengaruh *multithreading* dalam meningkatkan kecepatan enkripsi dan dekripsi. Penelitian ini menggunakan data sebanyak 6 jenis data yang terdiri dari jenis data teks dan berkas. Masing-masing diuji sebanyak 10x dan telah menghasilkan prototipe untuk membandingkan kecepatan enkripsi dekripsi dan kecepatan pengiriman pesan menggunakan jumlah *thread* yang berbeda. Dari hasil yang telah dilakukan dengan 2 aspek pengujian, ditemukan pengaruh signifikan yang terjadi pada proses enkripsi dekripsi dengan menggunakan jumlah *thread* yang berbeda.

Kata Kunci: Kriptografi, Rijndael 128, *Multithreading*

Palembang, 6 Januari 2021

Pembimbing I	Pembimbing II
Drs. Megah Mulya, M.T.	Muhammad Ali Buchari, M.T.
NIP. 196602202006041001	NIP. 198803302019031006 7

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

KATA PENGANTAR

Puji syukur kepada Allah SWT atas berkat, kesempatan dan rahmat-Nya yang telah melimpahkan rahmat dan karunianya kepada Penulis sehingga mampu menyelesaikan Tugas Akhir ini dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat untuk menyelesaikan Pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Dalam kesempatan ini Penulis ingin menyampaikan kepada seluruh pihak di bawah ini yang telah memberikan banyak dukungan dan bantuan dalam proses penyelesaian penelitian ini. Saya ucapkan beribu terima kasih kepada:

1. Orang tua saya, Papa saya Mahmudi Hasan dan Almarhumah Ibu Saya Fatma Dalena serta Ibu tersayang saya Fitriani yang jasa dan doanya dalam mendukung saya selama proses penyusunan skripsi yang tak terhitung. Adik-adik saya Shafa Azka Fairuz, M. Jaihan Syah, Wais Al-Qarni, Alsya Kania, dan Naura Aninda serta seluruh keluarga besar saya yang selalu mendoakan, menghibur, serta memberikan dukungan baik secara moril maupun materil.
2. Pembimbing Tugas Akhir saya, Bapak Drs Megah Mulya, M.T. dan Muhammad Ali Buchari, M.T. yang telah membimbing penulis dengan detail dan memberi banyak masukan selama penyusunan tugas akhir ini.
3. Penguji Tugas Akhir, Ibu Alvi Syahrini Utami, M.Kom dan Ibu Mastura Diana Marieska, M.T. atas jasanya sudah membantu menyempurnakan tugas

akhir penulis dengan masukan-masukan yang bermanfaat dan menyeluruh selama proses seminar proposal hingga masa perbaikan paska seminar komprehensif.

4. Pembimbing Akademik saya Ibu Yunita, S.Si, M.Cs sebagai pengarah seluruh proses akademik penulis dan memberikan masukan-masukan berarti bagi penulis hingga penyusunan tugas akhir.

5. Kepada orang-orang paling berpengaruh di hidup saya Sacharum Noor Zhafiroh, Hanum Sabrina AJ, A. Rafik, Jhoni Iskandar, dan M. Irfan Triananto Putra yang selalu menyertai penulis dan bersedia untuk meluangkan waktunya berbagi cerita dan berbagi momen di selama penyusunan tugas akhir ini.

6. Kepada teman-teman se-kosan perjuangan yang selalu memberikan dukungan, mengajak bermain ketika penulis lelah,dan memberikan nasehat-nasehat berarti selama proses penyusunan skripsi ini.

7. Yang terakhir kepada seluruh keluarga BO Intel, LDF WIFI dan anak kelas INFORGEN ‘16. Kalian hebat!

Semoga pihak-pihak diatas dan seluruh orang baik yang pernah saya temui dapat dimudahkan urusannya oleh Allah SWT sampai kapanpun. Saya ucapkan terima kasih banyak-banyak.

Palembang, 6 Januari 2021
Penulis,

Mohammad Sulthan Alif Utama

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab pendahuluan ini akan dibahas latar belakang permasalahan, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan. Bab ini juga berisikan penjelasan mengenai gambaran umum dari keseluruhan kegiatan yang dilakukan dalam penelitian tugas akhir.

1.2 Latar Belakang

Teknologi informasi dan komunikasi telah mengalami perubahan yang cepat, sehingga proses komunikasi pun ikut mengalami perubahan signifikan. Salah satu media komunikasi yang sedang diminati adalah media komunikasi menggunakan jaringan internet seperti aplikasi *chatting* atau lebih dikenal juga dengan istilah *instant messaging*. (Saleh & Tahir, 2018). Aplikasi *chatting* merupakan suatu bentuk komunikasi yang memungkinkan pengguna untuk mengirimkan pesan singkat ke pengguna lain secara langsung atau *real time*. Perkembangkan aplikasi *chatting* begitu pesat berdasarkan riset yang dilakukan oleh perusahaan riset pasar Nielsen menunjukkan bahwa saat ini orang Indonesia menyukai metode berkomunikasi menggunakan aplikasi *chatting* yang mencapai angka 79%. Hal ini menunjukkan jika penetrasi penggunaan aplikasi *chatting* di Indonesia tergolong masif dan cepat.

Namun dari fenomena meningkatnya perkembangan aplikasi *chatting* tersebut ada konsekuensi yang timbul yaitu perihal keamanan informasi Setidaknya dibutuhkan suatu mekanisme pengamanan yang memungkinkan pesan yang dikirim tidak diterima dan diketahui oleh pihak yang tidak berhak. Salah satu mekanisme yang dapat dilakukan adalah memanfaatkan teknik pengamanan kriptografi untuk menyamarkan pesan yang dikirim ke dalam suatu bentuk pesan yang sulit untuk dipahami maknanya. Selain itu, diperlukan pengamanan secara *end-to-end* (E2E) yang memungkinkan pesan yang dikirim hanya dapat dibaca oleh orang-orang yang sedang berkomunikasi saja, tidak ada *eavesdropper* (pihak ketiga atau *secret listener*) yang dapat mengakses kunci kriptografi yang dibutuhkan untuk enkripsi-dekripsi percakapan, termasuk penyedia telekomunikasi, penyedia internet bahkan *developer* dari aplikasi *chatting.*

Pada tahun 2014, salah satu media chatting WhatsApp memperkenalkan teknologi *End-to-End Encryption.* Teknologi ini menawarkan pertukaran dan proses komunikasi antar kedua belah pihak aman dan sulit untuk dilacak. Teknologi ini menawarkan pesan sampai ke tempat tujuan pengguna dengan aman. (Endeley, 2018)

Eko Sularsono, dkk. (2014) melakukan penelitian kriptografi dengan metode algoritma simetri Rijndael 128 untuk mengamankan pesan pada aplikasi *real-time chatting* dengan cara melakukan penyadapan menggunakan *Man-In-The-Middle Attach* secara sekuensial. Hasil dari penelitian ini menujukkan bahwa data *nickname* dan nama *room* yang disimpan pada server sebelumnya telah mengalami proses enkripsi dengan algoritma Rijndael. Data

password *room* yang tersimpan pada server sebelumnya telah mengalami proses *hashing* menggunakan algoritma SHA-3. Hal ini membuat keamanan data yang tersimpan di dalam server lebih terjaga keamanannya (Sularsono & Raharjo, 2014)

Berdasarkan hasil penelitian tentang kriptografi yang telah dijelaskan diatas, maka pada tugas akhir ini akan mengimplementasikan proses enkripsi dan dekripsi menggunakan kriptografi simetri Rijndael 128 dengan menggunakan teknologi *multithreading* untuk membandingkan kecepatan proses enkripsi dan dekripsi yang terjadi serta menentukan berapa *n thread* yang optimal dalam proses enkripsi dan dekripsi.

Pemilihan algoritma Rijndael 128 didasarkan pada kejadian *Institute of Standards and Technology* (NIST) yang menyeleksi standar kriptografi terbaru yang dinamakan Advanced Encryption Standard (AES) dan menetapkan Rijndael sebagai pemenang AES. Pada bulan Mei 2002, Rijndael dijadikan sebagai standar algoritma kriptografi oleh pemerintah federal Amerika Serikat. Untuk alasan ini, algoritma Rijndael 128 dapat digunakan sebagai standar keamanan yang kuat untuk mengenkripsi pesan.

1.3 Rumusan Masalah

Permasalahan dalam penelitian ini adalah bagaimana mengimplementasikan algoritma simetri Rijndael 128 pada aplikasi *real-time chatting* menggunakan teknologi *multithreading* dan pengaruh *multithreading* dalam kecepatan proses enkripsi-dekripsi program. Selanjutnya dirumuskan pertanyaan penelitian sebagai berikut:

1. Bagaimana membuktikan pengaruh *multithreading* dalam meningkatkan kecepatan proses enkripsi-dekripsi dan membandingkan secara langsung dengan proses sekuensial*?*
2. Bagaimana membagi proses enkripsi-dekripsi teks dan file dengan algoritma kriptografi Rijndael 128 ke dalam *n* buah *thread* sehingga kecepatan proses enkripsi-dekripsi teks dan berkas dapat ditingkatkan?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini sebagai berikut:

1. Membuktikan pengaruh *multithreading* dalam meningkatkan kecepatan pengiriman serta kecepatan proses enkripsi-dekripsi dan membandingkan secara langsung dengan proses sekuensial.
2. Menentukan jumlah n *thread* yang tepat dalam proses enkripsi-dekripsi teks dan berkas yang dikirimkan dari sisi klien untuk diproses secara *multithreading* sehingga kecepatan waktu proses enkripsi-dekripsi teks dan berkas dapat ditingkatkan.
3. Melakukan perbandingan kecepatan pengiriman serta kecepatan kedua proses enkripsi-dekripsi dengan dan tanpa menggunakan teknologi *multithreading* dengan melakukan perbandingan waktu eksekusi program.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

1. Menghasilkan perangkat lunak perpesanan instan yang cepat dan aman yang dapat mengimplementasikan kriptografi simetri algoritma Rijndael 128 dan menggunakan teknologi *multithreading*.
2. Menambah referensi baru untuk penelitian lainnya yang membahas tentang pemograman *multithreading* yang mengimplementasikan keamanan kriptografi algoritma Rijndael 128.

1.6 Batasan Masalah

Batasan masalah yang ditentukan pada penelitian ini adalah:

1. Algoritma enkripsi yang digunakan adalah algoritma Rijndael 128.
2. Besar memori komputer pada saat pengujian adalah 12.00 GB.
3. Sistem operasi pada komputer pengujian adalah Microsoft Windows 10 Home.
4. Aplikasi yang dibangun merupakan aplikasi berbasis *desktop.*
5. Pengamanan yang digunakan dapat berupa *plainteks* dan berkas yang berekstensi .zip.

1.7 Sistematika Penulisan

Sistematika penulisan tugas akhir ini mengikuti standar penulisan skripsi Sarjana Fakultas Ilmu Komputer Universitas Sriwijaya, yaitu:

BAB I. PENDAHULUAN

Dalam bab ini dijelaskan tentang latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah/ruang lingkup, metodologi penelitian, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan membahas segala hal tentang dasar-dasar teori yang digunakan dalam penelitian, seperti definisi kriptografi, algoritma Rijndael 128, *multithreading*, WebSocket, arsitektur jaringan *client-server* dan penelitian lain yang relevan.

BAB III. METODOLOGI PENELITIAN

Bab ini akan membahas mengenai tahapan yang akan dilaksanakan pada penelitian ini. Masing-masing rencana tahapan penelitian dideskripsikan dengan rinci dengan mengacu pada suatu kerangka kerja. Diakhir bab ini berisi perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab ini akan membahas proses pengembangan perangkat lunak. Perangkat lunak dikembangkan menggunakan metode Scrum. Pada Scrum terdapat 3 fase yaitu fase inisiasi (*Kick-off*), fase pengembangan perangkat lunak (*Sprint*) dan fase pengujian (*Hand Over*) yang akan dijelaskan pada subbab masing-masing.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab ini akan menjelaskan hasil percobaan penelitian. Percobaan dilakukan menggunakan data uji yang telah ditentukan berikut dengan alat penelitian yang telah disebut sebelumnya.

BAB VI. KESIMPULAN DAN SARAN

Bab ini akan memberikan poin-poin kesimpulan dan saran atas hasil pengujian dan penelitian yang didapatkan dalam penelitian ini.

1.8 Kesimpulan

Pada bab ini dapat disimpukan bahwa masalah yang harus diselesaikan pada penelitian ini adalah membuktikan pengaruh *multithreading* dalam meningkatkan dan membandingkan secara langsung dengan proses sekuensial dan bagaimana membagi proses enkripsi teks dan berkas dengan algoritma kriptografi Rijndael 128 ke dalam *n* buah *thread* sehingga kecepatan proses enkripsi-dekripsi teks dan berkas dapat ditingkatkan.

DAFTAR PUSTAKA

Abood, O.G. & Guirguis, S.K. 2018. A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications (IJSRP), 8(7).

Amrullah, M.A., Lhaksmana, K.M. & Adytia, D. 2018. Pembangunan dan pengujian protokol MQTT & WebSocket untuk Aplikasi IoT Rumah Cerdas berbasis Android. 5(2): 3760–3769.

Daemen, J. & Rijmen, V. 2014. LNCS 1820 - The Block Cipher Rijndael.

Endeley, R.E. 2018. End-to-End Encryption in Messaging Services and National Security — Case of WhatsApp Messenger. 95–99.

Hamidi, B. & Hamidi, L. 2017. Synchronization Possibilities and Features in Java. European Journal of Interdisciplinary Studies, 1(1): 75.

Nani, P.A., Katolik, U. & Mandira, W. 2016. Implementasi Multithreading Programming Concept Untuk Meningkatkan Efisiensi Proses Steganografi Metode LSB.

Pada, S. & Android, K. n.d. Pola Komunikasi Pengguna Aplikasi Chatting (Studi Pada Komunitas Android Rahmita, Suwardi Makassar. 4: 91–105.

Murdowo, S. 2014. Mengenal Proses Perhitungan Enkripsi Menggunakan Algoritma Kriptografi Advance Encryption Standard (Aes) Rijdnael. (http://jurnal.amikjtc.com/index.php/jurnal/article/view/55, diakses 10 Februari 2020).

Sularsono, E. & Raharjo, W.S. 2014. Implementasi Algoritma Rijndael 128 Pada Aplikasi Chatting Berbaris HTML5 Websocket. 10(2): 66–79. Surian, D. 2006. Algoritma kriptografi aes rijndael. 8(2): 97–101.

Schwaber, K., & Sutherland, J. (2017). Panduan Definitif untuk Scrum: Aturan Main. *Imperial Journal of Interdisciplinary Research (IJIR)*, *2*(12), 293–298. Diterima dari https://www.scrumguides.org/docs/scrumguide/v2017/2017-Scrum-Guide-Indonesian.pdf

Nani, P. A. (2013) 'Implementasi multithreading programming concept untuk efisiensi proses steganografi metode lsb', (April).

Warno (2012) 'Pembelajaran Pemrograman Bahasa Java Dan Arti Keyword', 8, pp. 40–51.