REKAYASA ENKRIPSI/DEKRIPSI FILE MENGGUNAKAN KOMBINASI *ADVANCED ENCRYPTION STANDARD ALGORITHMS* (AES 256), DAN *RIVEST CODE* (RC4) UNTUK KEAMANAN DOKUMEN BERKLASIFIKASI PADA INFRASTRUKTUR INFORMASI VITAL NASIONAL

Boy Sampetua Sipahutar

NIM: 120220405007

FAKULTAS SAINS DAN TEKNOLOGI PERTAHANAN

PROGRAM STUDI REAKAYASA PETAHANAN SIBER

UNIVERSITAS PERTAHANAN RI

BOGOR

2024

REKAYASA ENKRIPSI/DEKRIPSI FILE MENGGUNAKAN KOMBINASI *ADVANCED ENCRYPTION STANDARD ALGORITHMS* (AES 256), DAN *RIVEST CODE* (RC4) UNTUK KEAMANAN DOKUMEN BERKLASIFIKASI PADA INFRASTRUKTUR INFORMASI VITAL NASIONAL

TESIS

Boy Sampetua Sipahutar

NIM: 120220405007

Ditulis untuk memenuhi sebagian persyaratan

dalam mendapatkan Gelar Magister Pertahanan

FAKULTAS SAINS DAN TEKNOLOGI PERTAHANAN

PROGRAM STUDI REAKAYASA PETAHANAN SIBER

UNIVERSITAS PERTAHANAN RI

BOGOR

2024

LEMBAR PERSETUJUAN TESIS

Nama Siswa	:	Boy Sampetua Sipahutar
Nomor Induk Mahasiswa	:	120220405007
Program Studi	:	Rekayasa Pertahanan Siber
Fakultas	:	Sains Dan Teknologi Pertahanan
Judul Proposal Tesis	:	Rekayasa Enkripsi/Dekripsi File Menggunakan Kombinasi Advanced Encryption Standard Algoritma (AES 256), Dan Rivest Code (RC4) Untuk Keamanan Dokumen Berklasifikasi Pada Infrastruktur Informasi Vital Nasional

Pembimbing I,	Pembimbing II,
	
Dr. Ir. Aulia Khamas Heikmakhtiar, S.Kom, M.Eng.	Dr. Ir. Rinaldi Munir, M.T.

Mengetahui,
Dekan Fakultas Sains dan Teknologi Pertahanan RI,

Prof. Dr. Ir. Muhamad Asvial, M.Eng.

NIP. 196804061994031014

Tanggal: 30 Januari 2024

LEMBAR PENGESAHAN TESIS

Nama Siswa	:	Boy Sampetua Sipahutar
Nomor Induk Mahasiswa	:	120220405007
Program Studi	:	Rekayasa Pertahanan Siber
Fakultas	:	Sains Dan Teknologi Pertahanan
Judul Proposal Tesis	:	Rekayasa Enkripsi/Dekripsi File Menggunakan Kombinasi Advanced Encryption Standard Algoritma (AES 256), Dan Rivest Code (RC4) Untuk Keamanan Dokumen Berklasifikasi Pada Infrastruktur Informasi Vital Nasional

No	Nama	Tandatangan	Tanggal
1	Pembimbing I: Dr. Ir. Aulia Khamas Heikmakhtiar, S.Kom, M.Eng.		30 Januari 2024
2	Pembimbing II: Dr. Ir. Rinaldi Munir, M.T.		30 Januari 2024
3	Penguji I: Dr. Yosef Prihanto, S.Si., M.Si.		30 Januari 2024
4	Penguji II: Dr. Ir. H. Achmad Farid Wadjdi, M.M.		27 Januari 2024
5	Penguji III: Letkol Laut (KH) Dr. Hondor Saragih, S.T., M.Si(Han). NRP 14633/P		30 Januari 2024

PERNYATAAN ORISIONALITAS

Yang bertanda tangan di bawah ini, saya:

Nama	: Boy Sampetua Sipahutar
NIM	: 120220405007
Program Studi	: Rekayasa Pertahanan Siber
Fakultas	: Fakultas Sains dan Teknologi Pertahanan
Judul Penelitian	: Rekayasa Enkripsi/Dekripsi File Menggunakan Kombinasi Advanced Encryption Standard Algorithms (AES 256), Dan Rivest Code (RC4) Untuk Keamanan Dokumen Berklasifikasi Pada Infrastruktur Informasi Vital Nasional

Menyatakan dengan sebenarnya bahwa dalam hasil penelitian saya ini tidak terdapat unsur-unsur penjiplakan karya penelitian atau karya ilmiah yang pernah dilakukan atau dibuat orang lain kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar rujukan.

Apabila dikemudian hari ternyata hasil penelitian ini terbukti terdapat unsur-unsur penjiplakan dan klaim dari pihak lain, maka saya bersedia untuk diproses sesuai peraturan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sebenarnya dan tanpa paksaan dari siapa pun.

KATA PENGANTAR

Dengan memanjatkan puji dan syukur kehadirat Tuhan Yang Maha Esa atas karunia dan rahmatNya sehingga penyusunan tesis dengan judul "Rekayasa Enkripsi/Dekripsi File Menggunakan Kombinasi Advanced Encryption Standard Algoritma (AES 256), Dan Rivest Code (RC4) Untuk Keamanan Dokumen Berklasifikasi Pada Infrastruktur Informasi Vital Nasional" dapat diselesaikan.

Saya menyadari bahwa tesis ini dapat terselesaikan berkat motivasi, bantuan, bimbingan, arahan dan kerjasama dari berbagai pihak. Oleh karena itu pada kesempatan ini, izinkan saya mengucapkan terima kasih yang setulusnya kepada:

- Bapak Letjen Jonni Mahroza, S.I.P., M.A., M.Sc., CIQnR., CIQaR., Ph.D. selaku Rektor Universitas Pertahanan Republik Indonesia.
- Bapak Prof. Dr. Ir. Muhamad Asvial, M.Eng. selaku Dekan Fakultas Sains dan Teknologi Pertahanan UNHAN Republik Indonesia.
- Bapak Kolonel Laut Dr. H.A. Danang Rimbawa, S.SI., M.T., M.Tr.Opsla. selaku Kepala Program Studi Rekayasa Pertahanan Siber UNHAN RI.
- Bapak Dr. Ir. Aulia Khamas Heikmakhtiar, S.Kom, M.Eng. selaku Pembimbing I.
- Bapak Dr. Ir. Rinaldi Munir, M.T. selaku Pembimbing II.
- Bapak Dr. Yosef Prihanto, S.Si., M.Si. selaku Penguji I.
- Bapak Dr. Ir. H. Achmad Farid Wadjdi, M.M. selaku penguji II.
- Bapak Letkol Laut (KH) Dr. Hondor Saragih, S.T., M.Si(Han) selaku Penguji III.
- Seluruh staf dan mahasiswa Program Studi Rekayasa Pertahanan Siber Universitas Pertahanan Republik Indonesia.
- Istri tercinta Imelda Yunika Rajagukguk dan Ananda Benedict Matthias Sipahutar.
- Semua pihak yang telah memberikan bantuan baik ide, saran maupun bantuan lainnya.

Dalam penyusunan tesis ini masih banyak terdapat kekurangan, untuk itu saya terbuka untuk kritik dan masukan yang bersifat membangun demi kesempurnaan tesis ini. Akhir kata semoga tesis ini memberikan manfaat bagi yang berkepentingan.

Bogor, 24 Januari 2024

Penulis

Boy Sampetua Sipahutar

ABSTRAK

REKAYASA ENKRIPSI/DEKRIPSI FILE MENGGUNAKAN KOMBINASI ADVANCED ENCRYPTION STANDARD ALGORITHMS (AES 256), DAN RIVEST CODE (RC4) UNTUK KEAMANAN DOKUMEN BERKLASIFIKASI PADA INFRASTRUKTUR INFORMASI VITAL NASIONAL

Penelitian ini fokus pada peningkatan keamanan dokumen digital berklasifikasi di instansi pemerintahan, menyoroti pentingnya perlindungan terhadap penyalahgunaan oleh pihak yang tidak berwenang. Dibandingkan dengan dokumen fisik yang diamankan secara fisik, dokumen digital membutuhkan metode pengamanan yang berbeda. Untuk meningkatkan keamanan distribusi dan penyimpanan dokumen digital, penelitian ini menyarankan penggunaan kombinasi algoritma enkripsi Advanced Encryption Standard (AES 256) dan Rivest Code (RC4). Penelitian dilakukan melakukan perancangan dan simulasi sistim di lokasi penelitian yang ditentukan, dengan tujuan untuk diterapkan di organisasi pemerintah seperti Kementerian Pertahanan. Pada simulasi yang dilakukan menunjukkan efektivitas metode ini dalam mengamankan dokumen berklasifikasi, hal ini diperoleh dari pengujian yang dilakukan di mana dokumen yang sudah enkripsi sudah tidak berhasil untuk dibaca dan digunakan. Selain itu keamanan kunci yang digunakan juga jauh lebih aman, dikarenakan kunci tersebut melekat pada dokumen itu sendiri sehingga tidak perlu adanya penyimpanan dan pengelolaan kunci. Selain kedua hal tersebut, integritas dokumen juga bisa dipastikan karena adanya proses validasi checksum pada proses dekripsi. Berdasarkan hasil pengujian yang dilakukan, desain pengamanan dokumen dengan kombinasi enkripsi Advanced Encryption Standard (AES 256) dan Rivest Code (RC4), menawarkan solusi bagi keamanan dokumen berklasifikasi pada infrastruktur informasi vital nasional.

Kata Kunci: *Keamanan Dokumen, Kriptografi AES 256, Kriptografi RC4*

ABSTRACT

FILE ENCRYPTION/DECRYPTION ENGINEERING USING A COMBINATION OF ADVANCED ENCRYPTION STANDARD ALGORITHMS (AES 256), AND RIVEST CODE (RC4) FOR CLASSIFIED DOCUMENT SECURITY IN THE NATIONAL VITAL INFORMATION INFRASTRUCTURE

This research focuses on improving the security of classified digital documents in government agencies, highlighting the importance of protecting against misuse by unauthorized parties. Compared to physically secured documents, digital documents require different security methods. To increase the security of distribution and storage of digital documents, this research suggests using a combination of Advanced Encryption Standard (AES 256) and Rivest Code (RC4) encryption algorithms. Research is carried out by designing and simulating systems at specified research locations, with the aim of being implemented in government organizations such as the Ministry of Defense. The simulation carried out shows the effectiveness of this method in securing classified documents. This was obtained from tests carried out where documents that had been encrypted were no longer able to be read and used. Apart from that, the security of the key used is also much safer, because the key is attached to the document itself so there is no need for key storage and management. Apart from these two things, document integrity can also be ensured because of the checksum validation process in the decryption process. Based on the results of the tests carried out, the document security design with a combination of Advanced Encryption Standard (AES 256) and Rivest Code (RC4) encryption offers a solution for the security of classified documents in vital national information infrastructure.

Keywords: *Document Security, AES 256 Cryptography, RC4 Cryptography*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

AES-256	:	The Advanced Encryption Standard
RC4	:	Rivest Cipher 4
IIVN	:	Infrastruktur Informasi Vital Nasional
Generate(d)	:	Dibangkitkan/ menghasilkan oleh sistem
Cipher text	:	Teks terenkripsi yang diubah menggunakan algoritma enkripsi
Hash (file)	:	Kode alfanumerik panjang tetap yang mewakili kata, pesan, atau data.
Encapsulation	:	Merupakan cara untuk membungkus data sehingga dapat menyembunyikan data yang seharusnya disembunyikan.
Input	:	Data atau informasi yang akan diproses oleh sistem sesuai dengan ketentuan proses yang telah ditentukan.
Output	:	Hasil dari input yang mengalami suatu proses tertentu sehingga menghasilkan sesuatu.
Class	:	Merupakan model untuk membuat sesuatu secara instan.

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Yang bertanda tangan di bawah ini, saya :

Nama	:	Boy Sampetua Sipahutar
NIM	:	120220405007
Program Studi / Fakultas	:	Rekayasa Pertahanan Siber / Sains dan Teknologi Pertahanan
HP/E-mail	:	082241473407 / boy.s.sipahutar@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada UPA Perpustakaan Universitas Pertahanan Republik Indonesia, Hak Bebas Royalti *Non-Eksklusif* (*Non-exclusive Royalty-Free Right)* atas karya ilmiah yang berjudul:

"Rekayasa Enkripsi/Dekripsi File Menggunakan Kombinasi Advanced Encryption Standard Algorithms (AES 256), Dan Rivest Code (RC4) Untuk Keamanan Dokumen Berklasifikasi Pada Infrastruktur Informasi Vital Nasional"

Beserta perangkat yang diperlukan (apabila ada). Dengan Hak Bebas Royalti *Non-Eksklusif* (*Non-exclusive Royalty-Free Right)* ini UPA Perpustakaan Universitas Pertahanan Republik Indonesia berhak menyimpan, mengalih media/formatkan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya, dan menampilkan/mempublikasikannya di internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencatumkan nama saya sebagai penulis/pencipta.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak UPA Perpustakaan Universitas Pertahanan Republik Indonesia, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Bogor, January 19, 2024

ours faithfully

Boy Sampetua Sipahutar