UNIVERSITAS PERTAHANAN REPUBLIK INDONESIA

Implementasi Enkripsi untuk Database dan Dokumen Rahasia pada Sistem Aplikasi Statistik Pusat Pelaporan dan Analisis Transaksi Keuangan Sebagai Upaya Pertahanan Siber

Tesis Yang Ditulis Untuk Memenuhi Sebagian Persyaratan dalam Mendapatkan Gelar Magister Terapan Pertahanan

John Swatrahadi Permana
120220405013

FAKULTAS SAINS DAN TEKNOLOGI PERTAHANAN
REKAYASA PERTAHANAN SIBER

JAKARTA
2024

LEMBAR PERSETUJUAN TESIS

Nama	:	John Swatrahadi Permana
NIM	:	120220504013
Program Studi	:	Rekayasa Pertahanan Siber
Fakultas	:	Fakultas Sains dan Teknologi Pertahanan
Judul Proposal Tesis	:	**Implementasi Enkripsi untuk Database dan Dokumen Rahasia pada Sistem Aplikasi Statistik Pusat Pelaporan dan Analisis Transaksi Keuangan Sebagai Upaya Pertahanan Siber**

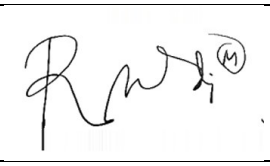
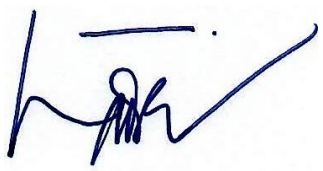
Pembimbing I	Pembimbing II
	
Dr. Hendrana Tjahjadi, ST., M. Si	Dr. Ir. Rinaldi Munir, M.T.
Pangkat/Korps/NRP/NIP	Pangkat/Korps/NRP/NIP
Tanggal : 24 Januari 2024	Tanggal : 24 Januari 2024

Mengetahui
Kepala Program Studi Rekayasa Pertahanan Siber
Fakultas Sains dan Teknologi Pertahanan,

Dr. H.A. Danang Rimbawa, S.Si., M.T.,
M.Tr.Opsla., CEH., CSBA., IPM., ASEAN Eng.
Kolonel Laut (E) NRP. 10829/P
Tanggal: 24 Januari 2024

LEMBAR PENGESAHAN TESIS

Nama	:	John Swatrahadi Permana
NIM	:	120220504013
Program Studi	:	Rekayasa Pertahanan Siber
Fakultas	:	Fakultas Science dan Teknologi Pertahanan
Judul Proposal Tesis	:	**Implementasi Enkripsi untuk Database dan Dokumen Rahasia pada Sistem Aplikasi Statistik Pusat Pelaporan dan Analisis Transaksi Keuangan Sebagai Upaya Pertahanan Siber**

No.	Nama	Tanda Tangan	Tanggal
1.	Pembimbing I: Dr. Hendrana Tjahjadi, ST., M. Si		24 Januari 2024
2.	Pembimbing II: Dr. Ir. Rinaldi Munir, M.T		24 Januari 2024
3.	*Reviewer* I : Dr. Ir. H. Achmad Farid Wadhdi, M.M 196303201989031001		24 Januari 2024
4.	*Reviewer* II : Kolonel Laut (E) Dr. H.A. Danang Rimbawa, S.Si., M.T., M.Tr. Opsla., CEH., CSBA		24 Januari 2024
5.	*Reviewer* III : Letkol Laut (S) Dr. Yudhi Biantoro, S.Kom., M.T.I		24 Januari 2024

PERNYATAAN ORISIONALITAS

Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya atau bagian karya yang pernah diajukan untuk Memperoleh gelar kesarjanaan jenjang apapun di suatu Perguruan Tinggi; dan sepanjang sepengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragraf, subbab atau bab dari karya yang pernah ditulis atau diterbitkan; kecuali yang secara tertulis diajukan dalam naskah ini dan disebutkan dalam Daftar Referensi.

Apabila di kemudian hari terbukti bahwa terdapat plagiat dalam tesis ini, saya bersedia menerima sanksi sesuai ketentuan peraturan/undang-undang yang berlaku.

Jakarta, 23 Januari 2024

John Swatrahadi Permana

KATA PENGANTAR

Puji syukur peneliti panjatkan kehadirat Allah Subhanahu Wa Ta'ala karena berkat rahmat dan karunia-Nya penyusunan tesis dengan judul: "Implementasi Enkripsi untuk Database dan Dokumen Rahasia pada Sistem Aplikasi Statistik Pusat Pelaporan dan Analisis Transaksi Keuangan Sebagai Upaya Pertahanan Siber" dapat diselesaikan. Penyusunan tesis ini ditujukan sebagai salah satu syarat dalam memperoleh gelar Magister pada Program Studi Rekayasa Pertahanan Siber Fakustas Science dan Teknologi Pertahanan Universitas Pertahanan. Penyusunan tesis ini dapat diselesaikan berkat Kehendak Allah Subhanahu Wa Ta'ala kemudian bantuan dan dukungan dari berbagai pihak baik secara langsung maupun tidak langsung. Untuk itu, pada kesempatan ini peneliti mengucapkan terima kasih kepada:

1. Papaku Bambang Taufiq SW dan Mamaku Tutik Sumarti (Rahimahullah) yang telah berjasa terhadapku hingga aku bisa sampai dengan saat ini.
2. Istri dan anak- anakku, yang kusayangi penyemangat hidupku.
3. Bapak Letnan Jenderal TNI Jonni Mahroza S.IP., M.A., M.Sc., CIQnR., CIQaR., Ph.D selaku Rektor Universitas Pertahanan Republik Indonesia.
4. Bapak Prof. Dr. Ir. Muhamad Asvial, M.Eng selaku Dekan Fakustas Science dan Teknologi PertahananUniversitas Pertahanan Republik Indonesia
5. Bapak Kolonel Laut (E) Dr. H.A. Danang Rimbawa, S.Si., M.T., M.Tr. Opsla., CEH., CSBA selaku kaprodi Rekayasa Pertahanan Siber sekaligus sebagai reviewer seminar proposal.
6. Bapak Kolonel Laut (E) Suginta Ginting, S.Kom., MMSI., M.Tr. Hanla sebagai kaprodi Rekayasa Pertahanan Siber sekaligus sebagai reviewer seminar proposal.
7. Bapak Kolonel Laut (P) Ruby Alamsyah, M.Tr.Opsla., M.Han., CIPA., CIT., CIIQA selaku Kepala Program Studi Rekayasa Pertahanan Siber yang juga telah memberikan arahan dalam penyusunan proposal tesis.
8. Bapak Dr. Hendrana Tjahjadi, ST., M. Si sebagai Pembimbing I yang telah memberikan bimbingan dan arahan baik mulai pada saat Kuliah AI, Kriptografi hingga penyusunan Tesis. Semoga apa yang Bapak lakukan menjadi nilai Ibadah.
9. Bapak Dr. Ir. Rinaldi Munir, M.T. sebagai Pembimbing II dan juga dosen mata kuliah Kriptografi sudah banyak memberikan ilmu semoga menjadi amal jariyah.
10. Bapak Dr. Ir. H. Achmad Farid Wadjdi, M.M. sebagai reviewer seminar proposal, seminar hasil
11. Bapak Letkol Laut (S) Dr. Yudhi Biantoro, S.Kom., M.T.I yang telah memberikan reviewnya pada seminar hasil

12. Mbak Bunbunan Hesty sebagai Staf Prodi RPS yang sudah banyak membantu Kami mulai dari masuk sampai lulus
13. Bapak Maimirza yang saat ini sudah menjadi Deputi, Terima kasih sudah memberikan ijin untuk mengikuti seleksi beasiswa Unhan
14. Bapak Albert H. Wounde yang telah mengajukan penugasan belajar di Unhan
15. Bapak Achmad Sukroni selaku Kapus TI PPATK saat ini yang telah memberikan semangat
16. Mas Arief Kurniawan sebagai Atasan Langung yang membidangi Pengembangan Aplikasi sekaligus tempat Konsultasi penyelesaian tesis
17. Teman-teman di BPAS Khususnya dan Logis pada Umumnya yang telah memberi dukungan
18. Teman-teman di Bermakna yang telah membantu kelancaran tugas belajar
19. Mas Bams di PEKA yang telah banyak memberi masukan
20. Bos Yohan yang juga lagi Kuliah di UI yang banyak memberi ejekan ejekan seloroh yang sangat bermakna
21. Teman- teman di Kelas RPS yang selalu berseloroh semangat Huh Hah dan juga seringkali berseloroh Jangan semangat tetap kasih kendor membuatku jadi galau, tapi okelah dan kompak sekali.
22. Mr. Husin Anak A S T A C A L A Mapala Telkom Universiti bocah petualang.
23. Para dosen penguji yang telah memberikan kritik dan saran yang membangun dalam penyelesaian tesis ini.

Semoga Allah Subhanahu Wa Ta'ala membalas kebaikan-kebaikan berbagai pihak atas bantuannya. Peneliti menyadari bahwa tesis ini masih kurang sempurna, oleh karena itu dengan kerendahan hati mengharap kritik dan saran yang konstruktif demi kesempurnaan tesis ini.

Akhirnya, semoga tesis ini dapat memberikan manfaat terhadap pengembangan ilmu pertahanan dan bermanfaat bagi *stakeholder* terkait dalam upaya memperkuat pertahanan siber dalam melindungi infrastruktur informasi vital.

Jakarta, 23 Januari 2024

John Swatrahadi Permana

ABSTRAK

IMPLEMENTASI ENKRIPSI UNTUK DATABASE DAN DOKUMEN RAHASIA PADA SISTEM APLIKASI STATI0053TIK PUSAT PELAPORAN DAN ANALISIS TRANSAKSI KEUANGAN SEBAGAI UPAYA PERTAHANAN SIBER

JOHN SWATRAHADI PERMANA

PPATK memiliki asset yang berharga berupa informasi intelijen keuangan, informasi tersebut adalah file hasil analisis, file keterangan ahli, database asset dan database tersangka yang harus dilindungi kerahasiaannya dari ancaman kebocoran data. Permasalahan untuk melindungi informasi rahasia berupa file dan database pada suatu sistem aplikasi adalah kinerja sistem dapat menurun sehingga mengurangi kenyamanan pengguna sistem. Tujuan dari penelitian ini adalah mengimplementasikan teknik hybrid kriptografi AES 256 dan RSA sebagai upaya pertahanan siber pada sistem aplikasi statistik penanganan perkara TPPU dan TPPT dengan tanpa mengurangi kenyamanan pengguna sistem aplikasi. Metode penelitian yang digunakan adalah kuantitatif ekperimen untuk mengetahui pengaruh variabel independen terhadap variabel dependen (hasil) dalam kondisi yang terkendalikan. Kondisi dikendalikan agar tidak ada variabel lain yang mempengaruhi variabel dependen. Hasil penelitian proses untuk mengenkripsi file kecepatannya rata-rata 521088,2201 kB/s, kemudian proses untuk mendekripsi file rata-rata 96040,34 kB/s. Hybrid Kriptografi dapat berjalan lebih cepat memproses file data dokumen daripada Algoritma AES 128 saja. Pada penelitian terdahlu dengan metode AES 128 mengenkripsi file berukuran 5 MB membutuhkan waktu rata-rata enkripsi dan dekripsi masing-masing 60 detik dan 0,02 detik. sedangkan dengan hybrid kriptografi untuk memproses file 2,55 MB hanya memerlukan waktu 0.000669 untuk proses enkripsinya dan 0.003945 untuk proses dekripsinya. Metode Hybrid Kriptografi yaitu perpaduan antara kriptografi kunci simetrik dan kriptografi kunci asimetrik dapat memperkuat upaya pertahanan siber dari ancaman keboran data pada infrastruktur informasi vital sektor administrasi Pemerintah yang bertugas untuk mencegah dan memberantas tindak pidana pencucian uang dan pendanaan terorisme salah satunya pada aplikasi statistik penanganan TPPU dan TPPT.

Kata Kunci : AES 256, Database, File Dokumen, Hybrid Kriptografi, Pertahanan Siber, PPATK, RSA

ABSTRACT

IMPLEMENTATION OF ENCRYPTION FOR DATABASE AND CONFIDENTIAL DOCUMENTS ON THE STATI0053TIK APPLICATION SYSTEM FINANCIAL TRANSACTION REPORTING AND ANALYSIS CENTER AS A CYBER DEFENSE MEASURE

JOHN SWATRAHADI PERMANA

PPATK has valuable assets in the form of financial intelligence information, this information is analysis results files, expert information files, asset databases and suspect databases whose confidentiality must be protected from the threat of data leaks. The problem with protecting confidential information in the form of files and databases in an application system is that system performance can decrease, thereby reducing the comfort of system users. The aim of this research is to implement the hybrid cryptography technique AES 256 and RSA as a cyber defense effort in the statistical application system for handling TPPU and TPPT cases without reducing the comfort of application system users. The research method used is quantitative experimentation to determine the effect of independent variables on dependent variables (outcomes) under controlled conditions. Conditions are controlled so that no other variables influence the dependent variable. The research results show that the process for encrypting files has an average speed of 521088.2201 kB/s, then the process for decrypting files has an average speed of 96040.34 kB/s. Hybrid Cryptography can process document data files faster than the AES 128 Algorithm alone. In previous research, using the AES 128 method, encrypting a 5 MB file required an average encryption and decryption time of 60 seconds and 0.02 seconds respectively. whereas with hybrid cryptography to process a 2.55 MB file it only takes 0.000669 for the encryption process and 0.003945 for the decryption process. The Hybrid Cryptography method, namely a combination of symmetric key cryptography and asymmetric key cryptography, can strengthen cyber defense efforts from the threat of data breaches in the vital information infrastructure of the Government administration sektor which is tasked with preventing and eradicating criminal acts of money laundering and terrorist financing, one of which is the application of statistics on handling TPPU and TPPT.

Keywords: AES 256, Database, Document Files, Hybrid Cryptography, Cyber Defense, PPATK, RSA

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR GRAFIK

DAFTAR BAGAN

DAFTAR SINGKATAN

AES	:	*Advanced Encryption Standard*
BIN	:	Badan Intelijen Negara
BNN	:	Badan Narkotika Nasional
DJP	:	Direktorat Jenderal Pajak
DJBC	:	Direktorat Jenderal Bea dan Cukai
DPRK	:	*Democratic People's Republic of Korea*
FATF	:	*Financial Action Task Force*
KPK	:	Komisi Pemberantasan Korupsi
PPATK	:	Pusat Pelaporan dan Analisis Transaksi Keuangan
Kemenkopolhukam	:	Kementrian Koordinator Bidang Politik Hukum dan Keamanan
TPPU	:	Tindak Pidana Pencucian Uang
TPPT	:	Tindak Pidana Pendanaan Terorisme
RSA	:	Rivest Shamir Adleman
NIST	:	*National Institute of Standards and Technology*

DAFTAR PENGERTIAN

Kriptografi	:	ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dipahami lagi maknanya (Meyer, 1982)
Hybrid Kriptografi	:	kombinasi kriptografi kunci asimetris dengan kriptografi kunci simetris
Enkripsi	:	proses mengubah teks terang menjadi teks tersandi
Deskripsi	:	Proses mengubah teks (data) yang tidak dapat dibaca menjadi informasi yang dapat dibaca
Chipper Text	:	teks terenkripsi yang diubah dari plaintext menggunakan algoritma enkripsi untuk mengamankan data pengguna
Plain Text	:	nama lain untuk teks yang belum diformat

DAFTAR NOMENKELATUR

Pertahanan Siber	:	suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan pertahanan negara.
Rezim APUPPT	:	Rezim Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme merupakan serangkaian pengaturan dan proses pelaksanaan upaya pencegahan dan pemberantasan tindak pidana pencucian uang dan pendanaan terorisme yang dikenal dengan TPPU dan TPPT, melibatkan seluruh pemangku kepentingan terkait termasuk masyarakat.
Focal Point	:	PPATK menjadi elemen yang tampak lebih mencolok sekaligus lebih menarik perhatian dibandingkan elemen yang lainnya karena PPATK bertugas sebagai Sekretaris Komite TPPU.
Pencucian Uang	:	Segala perbuatan yang memenuhi unsur-unsur tindak pidana sesuai dengan ketentuan dalam Undang-Undang pencegahan dan pemberantasan tindak pidana pencucian uang