SKRIPSI

IMPLEMENTASI HYBRID CRYPTOSYSTEM MENGGUNAKAN CAMELLIA DAN DUAL MODULUS RSA SERTA METODE E2EE UNTUK PENGIRIMAN FILE

MITZAQON GHOLIZHAN AR ROMANDHON
NPM 20081010116

DOSEN PEMBIMBING
Achmad Junaidi, S.Kom., M.Kom.
Andreas Nugroho Sihananto, S.Kom., M.Kom.

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA
SURABAYA

2024

Halaman ini sengaja dikosongkan

LEMBAR PENGESAHAN

IMPLEMENTASI HYBRID CRYPTOSYSTEM MENGGUNAKAN CAMELLIA DAN DUAL MODULUS RSA SERTA METODE E2EE UNTUK PENGIRIMAN FILE

Oleh :
MITZAQON GHOLIZHAN AR ROMANDHON
NPM. 20081010116

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi Prodi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jawa Timur Pada Tanggal 30 Agustus 2024

Menyetujui

Achmad Junaidi, S.Kom., M.Kom. NPT. 3 7811 04 0199 1	.....	**(Pembimbing I)**
Andreas Nugroho Sihananto, S.Kom., M.Kom. NIP. 19900412 2024061 003	.....	**(Pembimbing II)**
Eva Yulia Puspaningrum, S.Kom., M.Kom. NIP. 19890705 2021212 002	.....	**(Ketua Penguji)**
Firza Prima Aditiawan, S.Kom., MTI. NIP. 19860523 2021211 003	.....	**(Anggota Penguji)**

Mengetahui

Dekan Fakultas Ilmu Komputer

Prof. Dr. Ir. Novirina Hendrasarie, MT.
NIP. 19681126 199403 2 001

LEMBAR PERSETUJUAN

IMPLEMENTASI HYBRID CRYPTOSYSTEM MENGGUNAKAN CAMELLIA DAN DUAL MODULUS RSA SERTA METODE E2EE UNTUK PENGIRIMAN FILE

Oleh:

MITZAQON GHOLIZHAN AR ROMANDHON

NPM. 20081010116

Menyetujui,

Koordinator Program Studi Informatika

Fakultas Ilmu Komputer

Fetty Tri Anggraeny, S.Kom., M.Kom.

NIP. 19820211 2021212 005

Halaman ini sengaja dikosongkan

SURAT PERNYATAAN ORISINALITAS

Yang bertandatangan di bawah ini:

Nama Mahasiswa	:	MITZAQON GHOLIZHAN AR ROMANDHON
Program Studi	:	Informatika
Dosen Pembimbing	:	1. Achmad Junaidi, S.Kom., M.Kom.
		2. Andreas Nugroho Sihananto, S.Kom., M.Kom.

dengan ini menyatakan bahwa isi sebagian maupun keseluruhan disertasi dengan judul:

IMPLEMENTASI HYBRID CRYPTOSYSTEM MENGGUNAKAN CAMELLIA DAN DUAL MODULUS RSA SERTA METODE E2EE UNTUK PENGIRIMAN FILE

adalah benar-benar hasil karya intelektual mandiri, diselesaikan tanpa menggunakan bahan-bahan yang tidak diizinkan dan bukan merupakan karya pihak lain yang saya akui sebagai karya sendiri. Semua referensi yang dikutip maupun dirujuk telah ditulis secara lengkap pada daftar pustaka. Apabila ternyata pernyataan ini tidak benar, saya bersedia menerima sanksi sesuai peraturan yang berlaku.

Surabaya, 10 September 2024
Yang Membuat Pernyataan,

MITZAQON GHOLIZHAN AR ROMANDHON
NPM. 20081010116

Halaman ini sengaja dikosongkan

ABSTRAK

Nama Mahasiswa / NPM	:	Mitzaqon Gholizhan Ar Romandhon / 20081010116
Judul Skripsi	:	Implementasi Hybrid Cryptosystem Menggunakan Camellia Dan Dual Modulus RSA Serta Metode E2EE Untuk Pengiriman File
Dosen Pembimbing	:	1. Achmad Junaidi, S.Kom., M.Kom. 2. Andreas Nugroho Sihananto, S.Kom., M.Kom.

Kebutuhan akan keamanan atas data merupakan hal yang sangat penting dalam era digital saat ini, terutama pada proses pertukaran data yang bersifat sensitif terhadap serangan siber. Selain keamanan data, ukuran data yang semakin besar juga menjadi permasalahan dalam proses pertukaran file karena waktu yang dibutuhkan dalam pemrosesan juga semakin lama. Pertukaran file sendiri merupakan hal yang umum untuk dilakukan pada saat ini, baik yang dilakukan oleh perorangan maupun dalam skala perusahaan. Penelitian ini melakukan implementasi skema hybrid cryptosystem menggunakan algoritma Camellia dan Dual Modulus RSA serta metode E2EE yang bertujuan untuk mengatasi permasalahan-permasalah tersebut. Pemilihan skema hybrid cryptosystem adalah untuk mendapatkan kekuatan dari masing-masing algoritma, sehingga keamanan dan kecepatan dari tiap algoritma dapat didapatkan. Metode enkripsi end-to-end sendiri digunakan sebagai lapisan keamanan tambahan. Tahapan yang dilakukan dalam penelitian ini adalah studi literatur, perancangan, implementasi dan pengujian. Hasil dari pengujian yang telah dilakukan, diperoleh bahwa untuk proses pembangkitan kunci skema hybrid memiliki waktu tempuh yang mirip dengan algoritma DM-RSA dengan perbedaan 9.3% lebih cepat dan pada proses enkripsi dan dekripsi memiliki waktu tempuh yang mirip dengan algoritma Camellia dengan perbedaan 2.3% lebih cepat. Untuk keseluruhan proses algoritma hybrid memiliki waktu tempuh yang mirip dengan algoritma Camellia untuk skenario ukuran data 600MB dan 1200MB dengan perbedaan 25.2% lebih lambat.

Kata kunci : Kriptografi, Hybrid Cryptosystem, Hybrid Cryptography, Algoritma Camellia, Algoritma Dual Modulus RSA (DM-RSA), Pengiriman File, End-to-End Encryption (E2EE)

Halaman ini sengaja dikosongkan

ABSTRACT

Student Name / NPM	:	Mitzaqon Gholizhan Ar Romandhon / 20081010116
Thesis Title	:	Implementation Of Hybrid Cryptosystem Using Camellia, Dual Modulus RSA, And E2EE For File Transmission
Advisors	:	1. Achmad Junaidi, S.Kom., M.Kom. 2. Andreas Nugroho Sihananto, S.Kom., M.Kom.

The need for data security is crucial in today's digital era, particularly in the exchange of data that is sensitive to cyber-attacks. Besides data security, the increasing size of data has also become a challenge in the file exchange process, as larger files require more time to process. File exchanges have become commonplace today, whether conducted by individuals or at the corporate level. This study implements a hybrid cryptosystem scheme using the Camellia and Dual Modulus RSA algorithms, along with the E2EE method, to address these issues. The selection of the hybrid cryptosystem scheme is aimed at leveraging the strengths of each algorithm, ensuring both security and speed. The end-to-end encryption method serves as an additional security layer. The stages carried out in this research include literature review, design, implementation, and testing. Based on the testing results, the key generation process in the hybrid scheme has a similar execution time to the DM-RSA algorithm, with a difference of 9.3% faster, and the encryption and decryption processes exhibit similar times to the Camellia algorithm, with a difference of 2.3% faster. Overall, the hybrid algorithm's execution time is comparable to that of Camellia for data sizes of 600MB and 1200MB, with 25.2% differences.

Keywords: Cryptography, Hybrid Cryptosystem, Hybrid Cryptography, Camellia Algorithm, Dual Modulus RSA (DM-RSA) Algorithm, File Transfer, End-to-End Encryption (E2EE)

Halaman ini sengaja dikosongkan

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala rahmat, hidayah dan karunia-Nya kepada penulis sehingga skripsi dengan judul **"Implementasi Hybrid Cryptosystem Menggunakan Camellia Dan Dual Modulus RSA Serta Metode E2EE Untuk Pengiriman File"** dapat terselesaikan dengan baik.

Penulis mengucapkan terima kasih kepada Bapak Achmad Junaidi, S.Kom., M.Kom., selaku Dosen Pembimbing utama dan Bapak Andreas Nugroho Sihananto, S.Kom., M.Kom., yang telah meluangkan waktunya untuk memberikan bimbingan, nasehat serta motivasi kepada penulis. Dan penulis juga banyak menerima bantuan dari berbagai pihak, baik itu berupa moril, spiritual maupun materiil. Untuk itu penulis mengucapkan terima kasih kepada:

1. Allah SWT, yang telah memberikan rahmat, hidayah, serta karunia-Nya sehingga penelitian dan laporan skripsi ini dapat diselesaikan.
2. Orang tua dan keluarga penulis, yang selalu mendoakan dan memberikan dukungan selama proses penulisan skripsi ini.
3. Saya sebagai penulis, yang tidak pernah menyerah, yang selalu percaya bahwa setiap usaha selalu membuahkan hasil.
4. Ibu Prof. Dr. Ir. Novirina Hendrasarie, MT., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jawa Timur.
5. Ibu Fetty Tri Anggraeny, S.Kom., M.Kom., selaku Ketua Program Studi Informatika Fakultas Ilmu Sosial Dan Ilmu Komputer Universitas Pembangunan Nasional "Veteran " Jawa Timur.
6. Bapak Fawwaz Ali Akbar, S.Kom., M.Kom., selaku dosen wali yang sering kali memberikan penulis saran-saran serta nasihat perkuliahan selama masa studi.
7. Seluruh Dosen Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur yang telah memberikan ilmunya kepada penulis selama perkuliahan.
8. Teman-teman "Setunggal", yang senantiasa memberikan arahan, bimbingan serta dukungan pada proses penelitian dan penulisan skripsi.

Penulis menyadari bahwa di dalam penyusunan skripsi ini banyak terdapat kekurangan. Untuk itu kritik dan saran yang membangun dari semua pihak sangat diharapkan demi kesempurnaan penulisan skripsi ini. Akhirnya, dengan segala keterbatasan yang penulis miliki semoga laporan ini dapat bermanfaat bagi semua pihak umumnya dan penulis pada khususnya.

Surabaya, 10 September 2024

Penulis

DAFTAR ISI

Halaman ini sengaja dikosongkan

DAFTAR GAMBAR

DAFTAR TABEL

Halaman ini sengaja dikosongkan