UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

MODEL PENGAMANAN BERKAS MENGGUNAKAN KRIPTOGRAFI ASIMETRIS RSA DAN ALGORITMA KOMPRESI PPM PADA FILE CURRICULUM VITAE (CV)

SKRIPSI

SITI ANNISA

1810511106

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

2022

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

MODEL PENGAMANAN BERKAS MENGGUNAKAN KRIPTOGRAFI ASIMETRIS RSA DAN ALGORITMA KOMPRESI PPM PADA FILE CURRICULUM VITAE (CV)

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer

SITI ANNISA

1810511106

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

2022

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Siti Annisa

NIM : 1810511106

Tanggal : 22 Juni 2022

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 22 Juni 2022

Yang menyatakan,

(Siti Annisa)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini

Nama : Siti Annisa

NIM 1810511106

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan Ilmu pengetahuan, menyetujui untuk memberikan kepada Universtias Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non Ekslusif *(Non-exclusive Royalty Free Right*) atas karya Ilmiah saya yang berjudul:

Model Pengamanan Berkas Menggunakan Kriptografi Asimetris RSA dan Algoritma Kompresi PPM Pada File Curriculum Vitae (CV)

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pemyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 14 Juni 2022

Yang menyatakan,

(Siti Annisa)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama	: Siti Annisa
NIM	: 1810511106
Program Studi	: Informatika
Judul	: Model Pengamanan Berkas Menggunakan Kompresi PPM dan Kriptografi Asimetris RSA Pada File Curriculum Vitae (CV)

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S-1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Bayu Hananto, S.Kom., M.Kom.
Penguji 1

I Wayan Widi P. S.Kom., MTI.
Penguji 2

Henki Bayu Seta, S.Kom., M.TI.
Pembimbing 1

Noor Falih, S.Kom., M.T.
Pembimbing 2

Dr. Ermatita, M.Kom.
Dekan Fakultas Ilmu Komputer

Desta Sandya Prasvita, S.Kom., M.Kom.
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Persetujuan : 20 Juli 2022

ABSTRAK

Model pengamanan berkas adalah suatu model yang mengimplementasikan satu atau lebih algoritma keamanan, dalam hal ini kriptografi, untuk melindungi keabsahan, integritas, dan keamanan berkas. Sudah banyak penelitian yang mengusung model pengamanan berkas guna memenuhi kebutuhan akan perlindungan keamanan. Namun, berdasarkan penelitian sebelumnya, model pengamanan berkas masih dapat dikembangkan. Peneliti mengusung model pengamanan berkas baru menggunakan kriptografi asimetris RSA dan algoritma kompresi PPM. Kriptografi asimetri RSA dipilih dengan alasan kuatnya algoritma dalam mengamankan berkas. Algoritma kompresi PPM dipilih sebagai penyokong kelemahan RSA dengan mengurangi besarnya ukuran *file ciphertext* dikarenakan besarnya bilangan yang digunakan pada saat enkripsi. Penelitian ini bertujuan untuk mengukur performa dari model pengamanan berkas menggunakan kriptografi asimetris RSA dan algoritma kompresi PPM dari segi keamanan, waktu, dan ukuran berkas yang dihasilkan.

Kata kunci: Model pengamanan berkas, Kriptografi, Asimetri, RSA, Algoritma, Kompresi, PPM

ABSTRACT

File security model is a model used to implement one or more security algorithm, in this case cryptography, to ensure file's validity, integrity, dan safeness. There are a lot of study about file security model to secure a file. But, based on previous studies, a file secutiy model is still can be developed. Researcher is proposing a new file secutiy model using asymmetric cryptography RS dan PPM compression algorithm. Asymmetric cryptography RSA is choosen because of its safeness. PPM compression algorithm is used to help decreasing ciphertext file's size due to big numbers usage on encryption process. This study aims to measure the performance of the new file security model using asymmetric cryptography RSA dan PPM compression algorithm in terms of security, time, and file's size.

***Keywords**: File security model, Cryptography, Asymmetric, RSA, Algorithm, Compression, PPM*

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah SWT karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan penelitian yang berjudul "Model Pengamanan Berkas Menggunakan Kriptografi Asimetris RSA dan Algoritma Kompresi PPM Pada File Curriculum Vitae (CV)". Dalam penelitian ini penulis mendapatkan bantuan moril berupa saran, bimbingan, dan doa dari berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

a. Ibu Dr. Ermatita, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
b. Bapak Desta Sandya Prasvitas, S.Kom., M.Kom., selaku Ketua Program Studi S1 Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
c. Bapak Henki Bayu Seta, S.Kom., M.TI., selaku dosen Pembimbing I.
d. Bapak Noor Falih, S.Kom., M.T., selaku dosen Pembimbing II.
e. Seluruh dosen Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah memberikan ilmunya serta membimbing penulis selama delapan semester.
f. Orang tua serta sahabat penulis yang selalu memberikan dukungan sehingga penulis dapat menyelesaikan penelitian dengan baik.

Jakarta, 20 Juni 2022

Penulis,

Siti Annisa

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN