



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 Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non Ekklusif (*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 pernyataan 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:

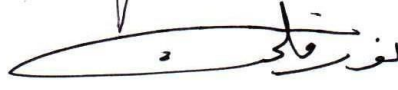
Nama : Siti Annisa
NIM : 1810511106
Program Studi : Informatika
Judul : Model Pengamanan Berkas Menggunakan Kompresi PPM dan Kriptografi Asimetris RSA Pada File Curriculum Vitae (CV)

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 security model is still can be developed. Researcher is proposing a new file security model using asymmetric cryptography RSA dan PPM compression algorithm. Asymmetric cryptography RSA is chosen 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

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA.....	i
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA.....	ii
PERNYATAAN ORISINALITAS.....	iii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	iv
ABSTRAK.....	vi
<i>ABSTRACT</i>	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
DAFTAR LAMPIRAN.....	xiv
BAB I.....	1
I.1 Latar Belakang.....	1
I.2 Rumusan Masalah.....	2
I.3 Tujuan Penelitian.....	2
I.4 Manfaat Penelitian.....	3
I.5 Ruang Lingkup Penelitian.....	3
I.6 Luaran yang Diharapkan.....	4
I.7 Sistematika Penulisan.....	4
BAB II.....	6
II.1 Aspek-Aspek Keamanan.....	6
II.2 Ancaman Keamanan.....	6
II.3 Kompresi Data.....	7
II.4 Algoritma PPM.....	8
II.5 Tujuan Kriptografi.....	9
II.6 Jenis-Jenis Kriptografi.....	10
II.7 Istilah-Istilah Dalam Kriptografi.....	13
II.8 Algoritma RSA.....	14
II.9 Proses Pembangkitan Kunci.....	16
II.10 Proses Enkripsi RSA.....	19
II.11 Proses Dekripsi RSA.....	20
II.12 Kekuatan dan Kelemahan RSA.....	21

II.13 Referensi Penelitian Sejenis	22
BAB III.....	30
III.1 Tahapan Berpikir	30
III.2 Tahapan Penelitian	32
III.3 Alat dan Bahan Penelitian.....	34
III.4 Jadwal Penelitian	35
BAB IV	37
HASIL DAN PEMBAHASAN	37
IV.1 Identifikasi Masalah	37
IV.2 Analisis Proses Kompresi dan Enkripsi.....	37
IV.3 Analisis Proses Dekripsi dan Dekompresi.....	45
IV.4 Analisis Kebutuhan <i>Website</i>	72
IV.5 Penjelasan Singkat <i>Website</i>	73
IV.6 Perancangan Aplikasi	73
IV.7 Perancangan Antarmuka Pengguna <i>Website</i>	80
IV.8 Implementasi.....	86
IV.9 Pengujian	93
IV.9.1 Pengujian Rasio Kompresi & Waktu Komputasi	93
IV.9.2 Pengujian Keterkaitan Spesifikasi Perangkat	98
IV.9.3 Pengujian Frequency Test	101
IV.9.4 Pengujian Pengaruh Kompresi PPM.....	105
IV.9.5 Pengujian Pengaruh <i>Server</i>	106
IV.9.6 Pengujian Pengaruh Koneksi Internet	108
BAB V.....	111
PENUTUP	111
V.1 Kesimpulan	111
V.2 Saran	113
DAFTAR PUSTAKA	114
DAFTAR RIWAYAT HIDUP.....	117
LAMPIRAN	118

DAFTAR TABEL

Tabel 2. 1 Referensi Penelitian	25
Tabel 3. 1 Jadwal Penelitian	35
Tabel 4. 1 <i>Range</i> dan Probabilitas Tiap Karakter	39
Tabel 4. 2 Hasil Proses Kompresi	41
Tabel 4. 3 Hasil Proses Dekompresi	70
Tabel 4. 4 Tabel Hasil Proses <i>Encode</i>	94
Tabel 4. 5 Tabel Hasil Proses <i>Decode</i>	95
Tabel 4. 6 Tabel Hasil Proses <i>Encode</i> di Perangkat 1	98
Tabel 4. 7 Tabel Hasil Proses <i>Encode</i> di Perangkat 2	99
Tabel 4. 8 Tabel Hasil Proses <i>Encode</i> di Perangkat 3	100
Tabel 4. 9 Tabel Hasil <i>Frequency Test</i>	102
Tabel 4. 10 Hasil Proses <i>Encode</i> dan <i>Decode</i> Menggunakan Kompresi PPM dan Kriptografi RSA	105
Tabel 4. 11 Hasil Proses <i>Encode</i> Menggunakan Kriptografi RSA	105
Tabel 4. 12 Hasil Proses <i>Encode</i> Menggunakan <i>Server</i> Pertama	107
Tabel 4. 13 Hasil Proses <i>Encode</i> Menggunakan <i>Server</i> Kedua	107
Tabel 4. 14 Hasil Proses <i>Encode</i> Pada Percobaan Pertama	108
Tabel 4. 15 Hasil Proses <i>Encode</i> Pada Percobaan Kedua	109
Tabel 4. 16 Hasil Proses <i>Encode</i> Pada Percobaan Ketiga	109

DAFTAR GAMBAR

Gambar 2. 1 Mekanisme Kriptografi Simetri	11
Gambar 2. 2 Mekanisme Kriptografi Asimetris.....	13
Gambar 2. 3 Diagram Kriptografi.....	14
Gambar 3. 1 Tahapan Berpikir	31
Gambar 4. 1 Tahapan Proses Kompresi	39
Gambar 4. 2 Isi Hasil Kompresi Website	41
Gambar 4. 3 Hasil Kompresi Website.....	41
Gambar 4. 4 Tahapan Pembangkitan Kunci Publik	42
Gambar 4. 5 Tahapan Enkripsi	44
Gambar 4. 6 Hasil Kompresi+Enkripsi dengan Website.....	45
Gambar 4. 7 Isi Hasil Kompresi+Enkripsi dengan Website	45
Gambar 4. 8 Tahapan Pembangkitan Kunci Privat	46
Gambar 4. 9 Tahapan Dekripsi	68
Gambar 4. 10 Tahapan Dekompresi.....	70
Gambar 4. 11 <i>Flowchart</i> Pembangkitan Kunci	74
Gambar 4. 12 <i>Flowchart</i> Proses <i>Encode</i>	75
Gambar 4. 13 <i>Flowchart</i> Proses <i>Decode</i>	76
Gambar 4. 14 <i>Activity diagram</i> Pembangkitan Kunci.....	77
Gambar 4. 15 <i>Activity diagram</i> <i>Encode</i>	78
Gambar 4. 16 <i>Activity diagram</i> <i>Decode</i>	79
Gambar 4. 17 <i>Use case</i> Diagram Sistem	80
Gambar 4. 18 Rancangan Halaman Utama.....	81
Gambar 4. 19 Rancangan Otentikasi HR	81
Gambar 4. 20 Rancangan Halaman HR	82
Gambar 4. 21 Rancangan Halaman Pembangkitan Kunci.....	82
Gambar 4. 22 Rancangan Halaman Pengunduhan Berkas	83
Gambar 4. 23 Rancangan Halaman Pelamar Kerja.....	83
Gambar 4. 24 Rancangan Halaman Memasukkan Kunci	84
Gambar 4. 25 Rancangan Halaman Mengunggah Berkas	85
Gambar 4. 26 Rancangan Halaman Hasil <i>Encode</i>	85
Gambar 4. 27 Rancangan Halaman Mengunduh Berkas.....	86
Gambar 4. 28 Tampilan Halaman Utama	87
Gambar 4. 29 Tampilan Halaman Otentikasi	87
Gambar 4. 30 Tampilan Kesalahan Otentikasi	88
Gambar 4. 31 Tampilan Halaman HR.....	88
Gambar 4. 32 Tampilan Halaman Kunci Privat.....	89
Gambar 4. 33 Tampilan Halaman Kunci Publik.....	89
Gambar 4. 34 Tampilan Halaman Sebelum Adanya Kunci Publik.....	90
Gambar 4. 35 Tampilan Halaman Memasukkan Kunci Publik	90
Gambar 4. 36 Tampilan Halaman untuk Mengunggah CV	91

Gambar 4. 37 Tampilan Halaman untuk Memilih CV yang Akan Diunggah.....	91
Gambar 4. 38 Tampilan Halaman Setelah Mengunggah CV.....	92
Gambar 4. 39 Tampilan Halaman Sukses Mengunggah CV	92
Gambar 4. 40 Tampilan Halaman Sukses Mengunduh CV	93
Gambar 4. 41 Tampilan Halaman Tidak Berhasil Mengunduh CV	93
Gambar 4. 42 Spesifikasi Perangkat 1	98
Gambar 4. 43 Spesifikasi Perangkat 2	99
Gambar 4. 44 Spesifikasi Perangkat 3	100
Gambar 5. 1 Perbandingan Waktu Komputasi.....	97
Gambar 5. 2 Perbandingan Rasio Kompresi.....	97
Gambar 5. 3 Perbandingan Waktu <i>Encode</i> dan <i>Decode</i>	97
Gambar 5. 4 Perbandingan Spesifikasi Perangkat	101
Gambar 5. 5 Perbandingan Pengaruh Penggunaan PPM.....	106
Gambar 5. 6 Perbandingan Koneksi Internet Terhadap Waktu Komputasi.....	110

DAFTAR LAMPIRAN

Lampiran 1 Tabel ASCII.....	118
Lampiran 2 Tabel Nilai ERFC.....	120
Lampiran 3 Hasil Plagiarisme	121