IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES, DAN ELGAMAL) PADA APLIKASI DESKTOP BERBASIS PHYTON

SKRIPSI

disusun oleh

M. Urfa Nurfathan

11.11.5341

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA

2015

IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES, DAN ELGAMAL) PADA APLIKASI DESKTOP BERBASIS PHYTON

SKRIPSI

Untuk memenuhi sebagian persyaratan
mencapai derajad Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

M. Urfa Nurfathan

11.11.5341

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA

2015

PERSETUJUAN

SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES, DAN ELGAMAL) PADA APLIKASI DESKTOP BERBASIS PYTHON

yang dipersiapkan dan disusun oleh

M. Urfa Nurfathan

11.11.5341

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 10 Maret 2015

Dosen Pembimbing

Ema Utami, Dr., S.Si, M.Kom
NIK. 190302037

PENGESAHAN

SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES, DAN ELGAMAL) PADA APLIKASI DESKTOP BERBASIS PYTHON

yang disusun oleh

M. Urfa Nurfathan

11.11.5341

yang telah dipertahankan di depan Dewan Penguji
pada tanggal 17 April 2015

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Windha Mega Pradnya D, M.Kom **NIK. 190302185**	
Hartatik, ST, M.Cs **NIK. 190302232**	
Ema Utami, Dr., S.Si, M.Kom **NIK. 190302037**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
tanggal 25 April 2015

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 25 April 2015

M. Urfa Nurfathan

NIM. 11.11.5341

MOTTO

Ibnu Abbas ra berkata : "Sulaiman bin Dawud as disuruh memilih antara ilmu, harta dan kerajaan maka beliau memilih ilmu, lalu beliau diberi harta dan kerajaan".

Abul Aswad berkata : "Tidak ada sesuatu yang lebih utama dari pada ilmu. Para raja itu memerintah manusia (orang kebanyakan), sedangkan para ahli ilmu itu memerintah para raja".

"sebaik-baiknya manusia adalah yang paling bermanfaat bagi manusia lainnya." [HR. Thabrani & Daruquthni]

Berusahalah untuk tidak menjadi manusia yang berhasil, tapi berusahalah untuk menjadi manusia yang berguna. [Albert Einstein]

"Rahasia didalam kehidupan ini, meskipun anda terjatuh hingga tujuh kali, anda harus bangkit hingga delapan kali." (Paulo Cuelho)

Kecerdasan bukan penentu kesuksesan, tetapi kerja keras merupakan penentu kesuksesan yang sebenarnya. (Anonymous)

"Tidak ada kata terlambat untuk belajar, belajar bersyukur dalam hidup kepada yang memberi hidup"

[Penulis]

”Ku olah kata, ku baca makna, ku ikat dalam alinea, ku bingkai dalam bab sejumlah lima, jadilah makarya, gelar sarjana ku terima, orang tua, calon istri, calon mertua pun bahagia”

[Penulis]

”Jadilah seperti karang di lautan yang kuat dihantam ombak dan kerjakanlah hal yang bermanfaat untuk diri sendiri dan orang lain, karena hidup di dunia hanyalah sekali. Ingat hanya pada Allah apapun dan dimanapun kita berada kepada Dia-lah tempat meminta dan memohon”

[Penulis]

”Tidak ada kekayaan yang melebihi akal, dan tidak ada kemelaratan yang melebihi kebodohan”

[Penulis]

”Kekasih yang setia adalah kekasih yang selalu menutup pintu buat cintanya orang lain”

[Penulis]

PERSEMBAHAN

Sembah sujud serta syukur kepada Allah SWT. Taburan cinta dan kasih sayang-Mu telah memberikanku kekuatan, membekaliku dengan ilmu serta memperkenalkanku dengan cinta. Atas karunia serta kemudahan yang Engkau berikan akhirnya skripsi yang sederhana ini dapat terselesaikan. Sholawat dan salam selalu terlimpahkan keharibaan Rasulullah SAW. Kupersembahkan karya sederhana ini kepada orang yang sangat kukasihi dan kusayangi.

- ✓ Kedua orang tua Paino dan Nur Aisiyati yang tak lelah salalu mendo'akan, mencintai dan mengasih sayangi tak terhingga. Takkan pernah mampu aku membalas keikhlasan kalian, walaupun dengan gunung emas sekalipun.
- ✓ Adik-adikku Zulfa Fikriana Rahma dan Faiz Salman Ar-Rosiid. Semoga kita selalu membuat Abah dan Umi bahagia dan bangga, dan kita adalah penerus keluarga kita harus jadi orang yang berguna. ☺
- ✓ Calon istri (Amin) Afriyanti Irawati Utami yang sudah setia memberikan semangat dan mempercayaiku. Sudah lama kita tak bertemu, semoga kita dipertemukan dalam janji dihadapan Allah SWT dalam sebuah pernikahan.
- ✓ Dosen Pembimbing Ema Utami, Dr., S.Si, M.Kom yang sudah sangat membantu dalam proses pengerjaan laporan skripsi saya.
- ✓ Dosen Penguji 1 dan 2 Bu Windha dan Bu Hartatik yang sudah bersedia meluangkan waktu dalam proses ujian skripsi saya. (**A**)lhamdulillah.
- ✓ Rekan seperjuangan, Kelas 11-S1TI-10 yang tidak bisa saya sebutkan namanya satu persatu, sukses selalu buat kita semua, jaga silaturahmi.

- ✓ Organisasi mahasiswa STMIK Amikom Yogyakarta. HMJTI mengajarkan manajemen dan tanggung jawab, FOSSIL memberikan banyak ilmu dan relasi, LPM Journal arti seni dalam segala hal serta kejujuran.
- ✓ Teman HMJTI: Ira, Nafi, Ita, Yayan, Laela, Vidia, Tesa, Rose, Bobby, Totok, Singgih, Riyan, Vicky, Rizal, Irfan, Jati, Ibnu, Santosa, angkatan 2010, 2012, dan 2013. #almamaterhitam.
- ✓ Teman FOSSIL: Singgih, Yusan, Andreyas, Kokon, Herman, Rangga, Yudi, Masinul, Danang, Pailus, dan yang lainnya.
- ✓ Teman LPM Journal: Ilham, Ndaru, Laras, Tyas, Ayu, Alif, Igo, Mas Oben, Mas Ngaliman, Morita, Sintya, Geslin, Asih, dan yang lain.
- ✓ Teman kontrakan galau yang memperbolehkan saya nginap selama berhari-hari.
- ✓ Teman-teman Kedai Digital yang sudah memperbolehkan bekerja dan memberi internet. Hhehe ☺

KATA PENGANTAR

Alhamdulillahirabbil'alamiin, segala puji bagi Allah SWT Tuhan semesta alam. Atas berkat, rahmat, taufik serta hidayah-Nya yang tiada terkira besarnya, sehingga penulis dapat menyelesaikan skripsi dengan judul "**IMPLEMENTASI ALGORITMA KRIPTOGRAFI HYBRID (DES, AES, DAN ELGAMAL) PADA APLIKASI DESKTOP BERBASIS PHYTON**".

Dalam penyusunannya, penulis memperoleh banyak bantuan dari berbagai pihak, oleh karena itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, MM selaku ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, MT selaku ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ibu Ema Utami, Dr., S.Si, M.Kom selaku dosen pembimbing yang telah memberikan arahan, bimbingan, motivasi, waktu dan masukan yang sangat membantu dalam pembuatan laporan skripsi ini.
4. Bapak Ibu dosen, staff dan karyawan STMIK AMIKOM Yogyakarta yang telah memberikan ilmu dan bantuan yang bermanfaat.
5. Kedua orang tua beserta keluarga tercinta yang senantiasa mendoakan dan memberi dukungan penuh kepada penulis.

6. Semua teman-teman kelas 11-S1-TI 10, teman-teman organisasi, sahabat-sahabat, dan kekasih tercinta yang membantu secara tidak langsung hingga skripsi ini dapat diselesaikan dengan sebaik-baiknya.
7. Semua pihak yang telah membantu dalam penyusunan tugas skripsi ini yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih jauh dari sempurna karena keterbatasan dan minimnya pengalaman penulis. Meskipun demikian penulis berharap segala laporan skripsi ini bermanfaat bagi yang membacanya dan penulis dengan senang hari menerima kritik dan saran yang membangun dari para pembaca.

Akhirnya, semoga laporan skripsi ini dapat bermanfaat bagi penulis dan para pembaca.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 25 April 2015

M. Urfa Nurfathan

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Informasi di era globalisasi ini merupakan peran penting dalam kehidupan sehari-hari, khususnya dalam dunia bisnis. Hal penting yang menjadi bahan analisis yang dilakukan oleh peneliti adalah tentang informasi rahasia. Selama ini informasi-informasi yang seharusnya rahasia masih dapat diketahui orang lain. Adapun langkah yang diupayakan untuk merahasiakan informasi tersebut sudah dilakukan. Beberapa pertanyaan yang muncul: Upaya apa lagi yang dilakukan untuk merahasiakan informasi? Bagaimana cara merahasiakannya?

Pada skripsi ini, peneliti mencoba untuk menganalisis dan mengusulkan solusi guna menyelesaikan pokok-pokok masalah yang ada. Menggunakan metode analisis sistem SWOT. Melakukan perancangan model proses menggunakan ERD dan Flowchart.

Aplikasi yang dihasilkan berbentuk prototype base-on desktop “PyCryptoTools”, yang ditujukan untuk memberikan solusi dalam pengiriman maupun penerimaan informasi rahasia. Di samping itu, peneliti juga menambahkan agar informasi yang sudah dirahasiakan selalu berubah-ubah dengan tujuan keamanan yang terjamin tanpa mengubah informasi aslinya.

Kata-kunci: Kriptografi, informasi, rahasia, analisis, pengembangan, implementasi, *testing*.

ABSTRACT

Information in this era of globalization is an important role in everyday life, especially in the business world. It is important that the subject of the analysis conducted by researchers is about confidential information. So far, the information confidential should still be known to others. The steps that attempted to conceal the information was done. Several questions arise: What other efforts are being made to conceal information? How do I keep it a secret?

In this thesis, the researcher tried to analyze and propose solutions to resolve the issues of the present. SWOT system analysis method. Do the designing process models using the ERD and Flowchart.

Generated application form on the desktop prototype base "PyCryptoTools", which is intended to provide a solution in the delivery and receipt of confidential information. In addition, the researchers also added that the information that has been withheld always changing with guaranteed security purposes without change original information.

Keywords: *Cryptography, information, confidential, analysis, development, implementation, testing.*