APLIKASI ENKRIPSI MENGGUNAKAN SISTEM KRIPTOGRAFI HIBRID AES, BLOWFISH, RSA, SHA2, DAN STEGANOGRAFI LSB

SKRIPSI

disusun oleh

Faisal Fani Wijaya

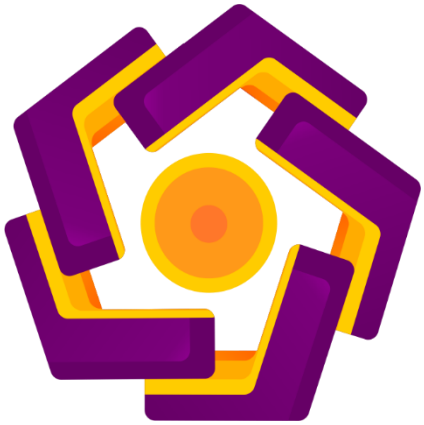
13.11.7330

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018

APLIKASI ENKRIPSI MENGGUNAKAN SISTEM KRIPTOGRAFI HIBRID AES, BLOWFISH, RSA, SHA2, DAN STEGANOGRAFI LSB

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Faisal Fani Wijaya

13.11.7330

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018

PERSETUJUAN

SKRIPSI

APLIKASI ENKRIPSI MENGGUNAKAN SISTEM KRIPTOGRAFI HIBRID AES, BLOWFISH, RSA, SHA2, DAN STEGANOGRAFI LSB

yang dipersiapkan dan disusun oleh

Faisal Fani Wijaya

13.11.7330

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 22 September 2016

Dosen Pembimbing,

Emha Taufiq Luthfi, S.T., M.Kom.

NIK. 190302125

PENGESAHAN

SKRIPSI

APLIKASI ENKRIPSI MENGGUNAKAN SISTEM KRIPTOGRAFI HIBRID AES, BLOWFISH, RSA, SHA2, DAN STEGANOGRAFI LSB

yang dipersiapkan dan disusun oleh

Faisal Fani Wijaya

13.11.7330

telah dipertahankan di depan Dewan Penguji
pada tanggal 23 April 2018

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ahlihi Masruro, M.Kom. **NIK. 190302148**	
Yuli Astuti, M.Kom. **NIK. 190302146**	
Emha Taufiq Luthfi, S.T., M.Kom. **NIK. 190302125**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 2 Mei 2018

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

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, 29 April 2018

Faisal Fani Wijaya

NIM. 13.11.7330

MOTTO

1. "Barangsiapa beriman kepada Allah dan hari akhir hendaklah berbicara yang baik-baik atau diam." (HR. Bukhari).
2. “Ilmu tanpa agama buta, agama tanpa ilmu lumpuh.”(Albert Einstein)
3. “Tidak ada yang mudah, tapi tidak ada yang tidak mungkin.”(Napoleon Bonaparte).

PERSEMBAHAN

Skripsi ini saya persembahkan untuk:

1. Bapak dan Ibuku tercinta yang telah memberikan kasih sayang dan dukungan yang tak terhingga.
2. Dosen pembimbing dan dosen penguji yang telah banyak membantu penyelesaian skripsi ini.
3. Rekan – rekan dari kelas TI-09 yang tak bisa saya sebutkan satu per satu serta teman – teman dari jurusan S1 informatika khususnya angkatan 2013.
4. Semua pihak yang telah membantu dalam penyelesaian skripsi ini.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi tentang "aplikasi enkripsi menggunakan sistem kriptografi hibrid AES, Blowfish, RSA, SHA2, dan steganografi LSB".

Dalam penulisan skripsi ini tidak lepas dari hambatan dan kesulitan, namun berkat bantuan dari berbagai pihak segala hambatan tersebut dapat diatasi dengan baik. Oleh karena itu penulis dengan setulus hati mengucapkan terima kasih kepada:

1. Bapak Emha Taufiq Luthfi, S.T, M.Kom. selaku dosen pembimbing yang telah banyak membantu dalam penyelesaian skripsi ini.
2. Bapak Ahlihi Masruro, M.Kom, dan Ibu Yuli Astuti, M.Kom selaku dosen penguji.
3. Teman - teman dari kelas TI-09 dan teman – teman dari jurusan S1 informatika khususnya angkatan 2013.
4. Bapak dan Ibuku yang tanpa kenal lelah selalu memberikan dukungan.
5. Semua pihak yang telah membantu penyelesaian skripsi ini.

Terakhir penulis menyadari bahwa skripsi ini masih jauh dari sempurna oleh karena itu penulis membutuhkan kritik dan saran yang membangun untuk memperbaiki kekurangan - kekurangan dalam skripsi ini.

Yogyakarta,29 April 2018

Faisal Fani Wijaya
13.11.7330

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Salah satu upaya yang bisa dilakukan untuk mengamankan data dan informasi adalah dengan melakukan enkripsi data. Akan tetapi data yang telah terenkripsi sekalipun tetap memiliki kelemahan. Kelemahan tersebut dapat berasal dari kelemahan algoritma yang dipakai, selain itu suatu data yang terenkripsi akan mudah dibedakan dengan data biasa hal tersebut dikarenakan data yang terenkripsi pasti sangat acak dan tidak beraturan.Hal tersebut akan membuat penyerang dengan mudah membedakan mana data terenkripsi dan mana yang bukan. Selain menggunakan enkripsi teknik steganografi juga dapat digunakan untuk mengamankan data. Tetapi data yang disembunyikan biasanya berupa data asli tanpa enkripsi terlebih dahulu. Dari situ muncul pertanyaan: Bagaimana jika menggabungkan kedua teknik tersebut untuk mengamankan data? Bagaimana cara membangun suatu system kriptografi yang menggabungkan beberapa algoritma sekaligus?

Pada Skripsi ini, peneliti mencoba untuk menganalisis permasalahan yang ada dan mencoba untuk mencari cara untuk membangun suatu system krptografi hibrida. Peneliti melakukukan analisis kebutuhan fungsional dan non fungsional, melakukan perancangan system menggunakan UML serta melakukan perancangan interface.

Aplikasi yang dihasilkan berbasis desktop dan dapat digunakan untuk mengenkripsi dan menyembunyikan data dengan menggunakan kriptografi hibrida yang merupakan gabungan dari beberapa algoritma kriptografi, hash, dan teknik steganografi.

Kata Kunci: Algoritma, Kriptografi, Steganografi, Hash, Enkripsi, Data.

ABSTRACT

One effort that can be done to secure data and information is by using data encryption. However, data that has been encrypted still has weaknesses. Weaknesses can be derived from the weakness of the algorithm used, besides that an encrypted data will be easily distinguished from the usual data it is because the encrypted data must be very random and irregular.That will make the attacker easily distinguish which data is encrypted and which is not. In addition to using encryption steganographic technique can also be used to secure data. But the hidden data is usually the original data without encryption first. From there the question arises: What if combine the two techniques to secure data? How to build a cryptographic system that combines several algorithms at once?

In this thesis, researchers try to analyze the existing problems and try to find a way to build a hybrid cryptography system. The researcher performs functional and non functional requirement analysis, designing system using UML and doing interface design.

The application is desktop-based and can be used to encrypt and hide data by using hybrid cryptography that is a composite of some cryptographic algorithms, hashes, and steganography techniques.

***Keyword**: Algorithm, Cryptography, Steganography, Hash, Encryption, Data.*