RANCANG BANGUN APLIKASI FILECRYPTOR UNTUK ENRKIPSI FILE DENGAN METODE AES-128

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik Pada
Jurusan Teknik Informatika

Oleh :

MOCH IKHSAN AFANDI
10751000209

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2014

LEMBAR PERSETUJUAN

RANCANG BANGUN APLIKASI FILECRYPTOR UNTUK ENRKIPSI FILE DENGAN METODE AES-128

TUGAS AKHIR

Oleh:

MOCH IKHSAN AFANDI
10751000209

Telah diperiksa dan disetujui sebagai laporan tugas akhir
di Pekanbaru, pada tanggal 3 Februari 2014

Pekanbaru 3 Februari 2014

Disetujui

Pembimbing

Benny Sukma Negara, ST, M.T
NIP. 198 20313 200901 1 009

LEMBAR PENGESAHAN

RANCANG BANGUN APLIKASI FILECRYPTOR UNTUK ENRKIPSI FILE DENGAN METODE AES-128

TUGAS AKHIR

Oleh :

MOCH. IKHSAN AFANDI
10751000209

Telah dipertahankan di depan sidang dewan penguji
Sebagai salah satu syarat untuk memperoleh gelar sarjana Teknik Informatika
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
Di Pekanbaru, pada tanggal, 28 Januari 2014

Pekanbaru, 3 Februari 2014
Mengesahkan,

Dekan	Ketua Jurusan
Dra. Hj. Yenita Morena, M.Si	**Elin Haerani, ST, M.Kom**
NIP. 19601125 198503 2 002	**NIP. 19810523 200710 2 003**

DEWAN PENGUJI

Ketua	: DR. Okfalisa, ST., M.Sc	_____
Sekretaris I	: Benny S. Negara, ST., M.T	_____
Anggota I	: Nazruddin Safaat, ST., M.T	_____
Anggota II	: Surya Agustian, ST., M.Kom	_____

RANCANG BANGUN APLIKASI *FILECRYPTOR* UNTUK ENKRIPSI FILE DENGAN METODE AES-128

MOCH IKHSAN AFANDI
NIM: 10751000209

Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

Keamanan dalam menyimpan file merupakan suatu hak privasi seseorang. Perkembangan teknologi *smartphone* dengan sistem operasi Android yang memungkinkan pengguna untuk menyimpan berbagai jenis file baik yang bersifat publik sampai sensitif. Enkripsi merupakan salah satu cara untuk mengamankan file tersebut. Dengan menggunakan AES-128 (*Advance Encryption Standard*) pada *mobile device* untuk mengamankan file. Perancangan aplikasi enkripsi menggunakan algoritma AES-128, dengan mengkonversi file menjadi bentuk biner dan byte lalu dilakukan proses enkripsi dengan algoritma AES-128 dalam proses ini disertai fungsi hash untuk menjaga integritas data sehingga aplikasi mengetahui pada saat dekripsi kemungkinan file yang telah dienkripsi mengalami perubahan atau tidak, aplikasi yang dirancang dilengkapi dengan fitur pengiriman password kepada email yaitu dengan memanfaatkan sistem pengiriman email SMTP digunakan sebagai *mail server* yang mampu mengirimkan email secara otomatis kepada email pengguna dengan protocol IMAP. Pengujian dilakukan meliputi komponen interface, kompatibilitas sistem operasi, integritas data dan keamanan sistem pengiriman email. Hasil pengujian memperlihatkan bahwa AES memiliki kecepatan hingga 1mb perdetik untuk enkripsi, penambahan ukuran file sesuai dengan panjang kunci, perbaikan threading proses sistem operasi, aplikasi mengetahui ketika file enkripsi mengalami perubahan dikarenakan hash file tidak sama, serta kelemahan sistem pengiriman email yaitu password dapat di ketahui oleh program *sniffing*.

Kata kunci: *Advanced Encryption Standard* (AES),Enkripsi, SMTP**,** IMAP, File, *Android, Mobile Device.*

Application Development FILECRYPTOR File Encryption Using AES-128 Algorithm

MOCH IKHSAN AFANDI
NIM: 10751000209

Informatics Engineering Departement
Faculty of Sciences and Technology
State Islamic University of Sultan Syarif Kasim Riau

ABSTRACT

Securing file are users private right. Technology advancement on Smartphone under Android Operating System allows users to save various file whether private or shared. Encryption can be used as tool to securing those files, by using AES-128 (Advanced Encryption Standard) as encryption algorithm in mobile device application. AES is cryptography algorithm that has several advantages such as speed processing and a standard since 2001. Application developed using AES-128, by converting file into stream bits and byte then processed by AES-128 algorithm, the running process of encryption is combined with hash function to keep data integrity so then application knows whether the encrypted file has been tempered, application has an additional feature, it can sent password to users email by using SMTP mail server that capable to sent email automatically with IMAP protocol. Under device testing include interface, operating system compatibility, data integrity and email sending system, AES-128 shows a significant encryption speed up to 1 mb per second and adding file size as an effect of key length range about 40kb to 50 kb, threading improvement had been made for system operation, the application detects if encrypted file had been tempered because of different hash result, and show weakness of email sending system where password can be retrieved by sniffing program.

Keywordsi: *Advanced Encryption Standard (AES), Encryption, SMTP, IMAP, File, Android, Mobile Device.*

KATA PENGANTAR

Alhamdulillaahi Robbil'alamin, syukurkepada Allah SWT atas segala limpahan rahmat dan karunia-Nya yang diberikan sehingga penulis sehingga dapat menyelesaikan penelitian sekaligus penulisan laporan tugas akhir ini. Sholawat kepada Nabi Muhammad SAW sebagai teladan bagi umat manusia.

Laporan tugas akhir ini merupakan salah satu prasyarat untuk memenuhi persyaratan akademis dalam rangka meraih gelar kesarjanaan di Jurusan Teknik Informatika, Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau (UIN SUSKA Riau). Selama menyelesaikan tugas akhir ini, penulis telah banyak mendapatkan bantuan, bimbinganserta petunjuk dari banyak pihak baik secara langsung maupun tidak langsung. Untuk itu dalam kesempatan ini penulis ingin mengucapkan terimakasih yang sebesar-besarnya kepada:

1. Prof. Dr. H. M. Nazir, selaku Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Dra. Yenita Morena, M.Si. selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
3. Elin Haerani, M.Kom, selaku Ketua Jurusan Teknik Informatika, Fakultas Sains dan Teknologi.
4. Dr. Okfalisa, ST., M.Sc, selaku dosen ketua sidang yang banyak membantu dan memberi masukan penulis dalam penyempurnaan Laporan Tugas Akhir ini.
5. Benny Sukma Negara, MT, selaku dosen pembimbing penelitian yang banyak membarikan saran dan memberikan waktu untuk memperbaiki demi kesempurnaan laporan penelitian ini..
6. Nazruddin Syafaat , M.T, selaku dosen penguji I yang banyak membantu dan memberi masukan penulis dalam penyempurnaan Laporan Tugas Akhir ini.
7. Surya Agustian , M.Kom, selaku dosen penguji I yang banyak membantu dan memberi masukan penulis dalam penyempurnaan Laporan Tugas Akhir ini.
8. M. Affandes**,** M.T**,** sebagai koordinator tugas akhir yang telah memberi semangat selama penelitian ini.

9. Ayah, Ibu, dan keluarga besar penulis yang selalu memberikan doa, dorongan, serta semangat untuk penulis..

10. Sahabat Penulis, Batri Anugrah yang sudah memberikan dorongan semangat dan bantuan kepada Penulis untuk menyelesaikan tugas akhir ini.

11. Sahabat Penulis, Freddy yang telah memberikan bantuan dalam pengembangan tugas akhir ini.

12. Sahabat Penulis, Dimas yang telah menjadi penyemangat dan memberikan tempat berkumpul untuk bersama-sama mengerjakan tugas akhir.

13. Sahabat Penulis, Rahman, Hendra, Febri, Lina, Imam, Eriyanto, Saidil, Didi, Heri, Zaenal, Nuryadi, atas semua dukungan dan motivasinya selama ini, dan semua teman-teman TIF 2007 yang tidak dapat disebutkan satu persatu, saya ucapkan terimakasih.

14. Teman-teman sesama Mahasiswa Teknik Informatika, khusunya TIF 07 D yang juga turut memberi semangat luar biasa, terimakasih.

15. Dan terimakasih juga penulis ucapkan untuk Almamater Teknik Informatika,Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau serta pihak-pihak lain yang tidak dapat penulis sebutkan satu persatu. Terimakasih banyak atas bantuan dan dukungannya yang berharga.

Penulis juga menyadari dalam penulisan laporan ini masih terdapat banyak kekurangan. Oleh karena itu, saran dan kritik sangat penulis harapkan untuk kemajuan bagi penulis secara pribadiserta kesempurnaan dimasa yang akan datang.

Pekanbaru, 29 Januari 2014

Penulis

DAFTAR ISI