PENGEMBANGAN *PROTOTYPE* SISTEM *HYBRID CRYPTOSYSTEM* UNTUK ENKRIPSI DAN DEKRIPSI FILE PDF MENGGUNAKAN ALGORITMA RSA, AES, MD5

TESIS

Oleh:

Farham Harvianto
1211601685

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2015

PENGEMBANGAN *PROTOTYPE* SISTEM *HYBRID CRYPTOSYSTEM* UNTUK ENKRIPSI DAN DEKRIPSI FILE PDF MENGGUNAKAN ALGORITMA RSA, AES, MD5

TESIS

Diajukan untuk memenuhi salah satu persyaratan

memperoleh gelar Magister Ilmu Komputer (MKOM)

Oleh:

Farham Harvianto

1211601685

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2015

PROGRAM STUDI MAGISTER ILMU KOMPUTER

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini,

Nama	: Farham Harvianto
Nim	: 1211601685
Program Studi	: Magister Ilmu Komputer
Konsentrasi	: Rekayasa Komputasi Terapan
Fakultas/Program	: Pascasarjana

Menyatakan bahwa TESIS yang berjudul :

PENGEMBANGA *PROTOTYPE* SISTEM *HYBRID CRYPTOSYSTEM* UNTUK ENKRIPSI DAN DEKRIPSI FILE PDF MENGGUNAKAN AlGORITMA RSA, AES DAN MD5

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan hasil karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. Saya izinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan apabila di kemudian pernyataan ini tidak benar.

Jakarta, 20 Februari 2015

(Farham Harvianto)

PROGRAM STUDI:MAGISTER ILMU KOMPUTER

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama	:	Farham Harvianto
NIM	:	1211601685
Konsentrasi	:	Rekayasa Komputasi Terapan
Jenjang Studi	:	Strata 2
Judul	:	Pengembangan Prototype System Hybrid Cryptosystem untuk Enkripsi dan Dekripsi File PDF Menggunakan Algoritma RSA, AES, dan MD5

Jakarta, 7 Maret 2015

Tim Penguji : Tanda tangan :

Ketua,
Prof. Dr. Moedjiono, M.Sc .....

Anggota / Pembimbing Utama,
Dr. Ir. Nazori Az, M.T .....

Pembimbing Pendamping,
Mardi Hardjianto, M.Kom .....

Ketua Program Studi

Dr. Ir. Nazori Az, M.T

ABSTRAK

Data anggaran Negara merupakan salah satu dokumen rahasia pada suatu kementerian lembaga pemerintahan di indonesia. Didalamnya terdapat berbagai informasi penting tentang suatu anggaran masing-masing kementrian lembaga tersebut. data anggaran yang selesai diolah disimpan dalam bentuk *Portable Document Format*. Penyimpanan dokumen anggaran ini disimpan didalam *hardisk* staf anggaran dan *Compact Disk*, tetapi bukan tidak mungkin suatu saat akan terjadi kehilangan data atau data dibaca oleh orang yang tidak berhak. Untuk mengatasinya perlu dibuatkan sistem untuk mengamankan dan menjaga keaslian file tersebut, yaitu dengan menggunakan teknik enkripsi. Pada penelitian ini, digunakan metode enkripsi simetris dan asimetris dalam pengamanan *file* PDF. Untuk enkripsi simetris menggunakan *Advanced Encryption Standart* dan untuk enkripsi asimetris meggunakan *Rivest Samir Adlemann*. Untuk menjaga keaslian *file* PDF, perlu menggunakan teknik *hash* atau enkripsi satu arah yaitu dengan menggunakan *Message Digest* 5, sehingga menghasilkan *Prototype* sistem *Hybrid Cryptosystem* untuk enkripsi dan dekripsi file PDF. Hasil dari penelitan yang telah dilakukan terhadap aplikasi ini, dokumen anggaran disetiap kementrian dan lembaga menjadi aman, tidak terbaca dan terjaga keasliannya oleh orang-orang yang tidak bertanggung jawab.

Kata Kunci : Enkripsi, RSA, AES, MD5, Asimetris, Simetris.

ABSTRACT

State budget data is one of the secret documents on a ministry of government agencies in Indonesia. In which there are a variety of important information about the budget of each ministry institutions. Complete budget data processed are stored in Portable Document Format. This budget document storage is stored in the hard drive and Compact Disk budget staff, but it is not impossible that one day there will be loss of data or data read by unauthorized people. To fix the system needs to be made to secure and maintain the authenticity of the file, ie using encryption techniques. In this study, use symmetric and asymmetric encryption methods in securing PDF files. For symmetric encryption using the Advanced Encryption Standard and receipts for asymmetric encryption Samir Adlemann Rivest. To maintain the authenticity of a PDF file, it is necessary to use a hash or encryption technique one way is by using the Message Digest 5, resulting in a Prototype Hybrid Cryptosystem system to encrypt and decrypt PDF files. The results of the research that has been conducted on this application, the budget documents in each ministry and agency to be safe, and secure authenticated unreadable by people who are not responsible.

Keyword : Encryption, RSA, AES, MD5, Asymmetric, Symmetric

KATA PENGANTAR

Puji dan Syukur yang sedalam-dalamnya kepada Allah SWT, karena hanya dengan rahmat dan karunia-Nya-lah naskah proposal tesis yang berjudul "Pengembangan *Prototype* system *Hybrid Cryptosystem* untuk enkripsi dan dekripsi *file* PDF menggunakan algoritma RSA, AES dan MD5" dapat diselesaikan. Shalawat serta salam senantiasa tercurahkan kepada Rasulullah yang telah membawa risalah dan Qalam-Nya sehingga penulis dapat memahami dan melaksanakan kewajiban menuntut ilmu.

Dalam penyusunan proposal tesis ini, penulis menyampaikan terima kasih yang tulus kepada:

1. Allah SWT yang telah memberikan kesehatan, kekuatan, kelimpahan rahmat kepada penulis sehingga dapat mengerjakan tesis ini sampai selesai.
2. Papah M.Hasan Santoso dan Mamah Satiti yang senantiasa memberikan kasih sayang, nasihat, dukungan semangat, pengorbanan yang tiada tara serta doa yang tak pernah berhenti mengalir dan juga Kakaku Yusparani dan Adikku Lissa Tania tersayang yang selalu memberikan semangat.
3. Bapak Prof. Dr. Moedjiono, M.Sc selaku Direktur Program Pascasarjana Universitas Budi Luhur.
4. Bapak Dr. Ir. Nazori AZ, M.T. selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur dan selaku pembimbing yang banyak membimbing dan memberi masukan dalam penyusunan tesis ini..
5. Bapak Mardi Hardjianto, M.Kom, selaku pembimbing tesis yang banyak memberikan bimbingan, bantuan dan tak henti-hentinya memberikan dukungan.
6. Seluruh Dosen Program Magister Ilmu Komputer Universitas Budi Luhur yang banyak memberikan ilmu selama perkuliahan.
7. Sahabatku Akbar Muchbarak dan Ahmad Pudolli beserta Istri Dewi Kusumaningsih dan sikecil Defandra yang telah sangat membantu penulis selama perkuliahan Pascasarjana ini berlangsung.
8. Team Bimbingan Tesis, Chyquita Danuputri dan Dolly Shaka yang selalu bimbingan dan berdiskusi bersama.

9. Kekasih Evi Lutfiati yang telah memberikan semangat sehingga penulis dapat menyelesaikan tesis ini.
10. Group diskusi tesis, Dedy Alamsyah, Ryan Zulham, Agi Chandra, Helmi Veris, Wiko Setyo, Dudi Parulian yang selalu berdiskusi dan memberikan saran.
11. Kelas Komputer Terapan yang selalu kompak dalam segala hal dalam perkuliahan semester terakhir.
12. Seluruh Angkatan XIII Magister Ilmu Komputer Universitas Budi Luhur yang telah membantu penulis.
13. Bagian Penyusunan Anggaran Biro Perencanaan dan Keuangan Lembaga Ilmu Pengetahuan Indonesia, Bpk.Opan Supandi, Bpk. Ismed Dharmawan, Bpk. Djwardi, Bpk. M. Machdi, Bpk. Adi, Bpk. Janter, Bpk. Suryono, Ibu Rini, Wakhid, Irfan, Finik, Agustine, Mellisa, Iwan, yang telah membantu dalam penyelesaian tesis ini.
14. CPNS Biro Perencanaan dan Keuangan LIPI, Desy, Adimas, Finik dan Ismi yang selalu mensupport didalam kantor
15. Serta semua pihak yang tidak dapat dituliskan.

Penulis menyadari bahwa penulisan tesis ini jauh dari sempurna. Untuk itu penulis berharap mendapatkan kritik dan saran yang dapat berguna untuk membangun demi kesempurnaan tulisan tesis ini.

Jakarta, Februari 2015

Farham Harvianto

DAFTAR ISI

DAFTAR GAMBAR

Gambar **Hal**

DAFTAR TABEL

Tabel **Hal**

DAFTAR LAMPIRAN

Lampiran **Hal**

DAFTAR PUSTAKA

[Abutaha 2011] Abutaha, Mohammed, et.al. "Survey Paper : Cryptography is The Science of Information Security", *Communication Theory of Secrecy Systems*, Vol.5, No.3, Juli 2011.

[Alexandre 2008] Alexandra Blonce, Eric Filio, Laurent Frayssignes, "Portable Document Format (PDF) Security Analysis and Malware Threats", *Jurnal Informatika*, Vol.5 No.1, April 2008.

[Aniello 2010] Aniello Castiglione, Alfredo De santis, Cludio Soriente, "Security and Privacy issues in the Portable Document Format", *The Journal of System and Software* 83, 2010.

[Anjali 2013] Anjali Pati, Rajeshwari Goudar, "A Comparative Survey Of Symametric Encryption Tehnique For Wireless Device", *International Journal .Of Sciencetific & Technology Research*, Vol.2, Issue 8, August 2013.

[Anjana 2014] Anjana S Chandran, "Repeated Encryption on RSA", *International Journal of Advanced Research in Computer Science and Software Engineering*, April 2014.

[Arinta 2012] Arinta Nugrahani, Mike Yuliana, M Zen Samsono, "Implementasi Metode Kriptografi RSA pada Priority Dealer untuk Layanan Penjualan dan Pemesanan Handphone berbasis J2ME", Kampus ITS, Surabaya 2012.

[Aris 2008] Aris Munandar, Sigit Purnama, "Analisis *Hybrid Cryptosystem* pada *Hypertext Transfer Protocol Secure* (HTTPS)", Sekolah Tinggi Sandi Negara, Bogor 2008.

[Didi 2006] Didi Surian, "Algoritma Kriptografi AES Rijndael", *Jurnal Teknik Elektro, TESLA* Vol.8, No.2, 97-101, Oktober 2006.

[Ebrahim 2013] Mansoor Ebrahim, Shujaat Khan, Umer bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis", *International Journal of Computer Application*, Vol.61 No.20, January 2013.

[Georgiana 2013] Georgiana Mateescu, Marius Vladescu, "A Hybrid Approach of System Security for Small and Medium Enterprises: Combining Different