APLIKASI MOBILE CATATAN HARIAN MENGGUNAKAN KEAMANAN ALGORITMA AES 256 DAN SHA 2

SKRIPSI

disusun oleh

Eka Yuliyanti

12.11.6394

PROGRAM SARJANA
PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016

APLIKASI MOBILE CATATAN HARIAN MENGGUNAKAN KEAMANAN ALGORITMA AES 256 DAN SHA 2

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana
pada Program Studi Teknik Informatika

disusun oleh

Eka Yuliyanti

12.11.6394

PROGRAM SARJANA
PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016

PERSETUJUAN

SKRIPSI

APLIKASI MOBILE CATATAN HARIAN MENGGUNAKAN KEAMANAN ALGORITMA AES 256 DAN SHA 2

yang dipersiapkan dan disusun oleh

Eka Yuliyanti

12.11.6394

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 Oktober 2015

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom
NIK. 190302181

PENGESAHAN

SKRIPSI

APLIKASI MOBILE CATATAN HARIAN MENGGUNAKAN KEAMANAN ALGORITMA AES 256 DAN SHA 2

yang dipersiapkan dan disusun oleh

Eka Yuliyanti

12.11.6394

telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Mei 2016

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Nila Feby Puspitasari, S.Kom, M.Cs **NIK. 190302161**	
Robert Marco, MT **NIK. 190302228**	
Joko Dwi Santoso, M.Kom **NIK. 190302181**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 30 Juni 2016

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, 30 Juni 2016

Eka Yuliyanti

NIM. 12.11.6394

MOTTO

"If you look at what you have in life, you'll always have more. If you look at what you don't have in life, you'll never have enough"

- Oprah Winfrey-

"Happiness is when what you think, what you say, and what you do are in harmony"

-Mahatma Gandhi-

"If today were the last day of your life, would you want to do what you are about to do today?"

-Steve Jobs-

"Never give up on what you really to do. The person with big dream is more powerful the one with all fact"

-Albert Einstein-

"It matters not what someone is born, but what they grow to be"

-J.K. Rowling-

PERSEMBAHAN

Penulis mempersembahkan skripsi ini kepada semua pihak yang terlibat dalam proses pembuatan skripsi baik secara langsung maupun tidak langsung.

1. Tuhan Yang Maha Esa yang memberikan segala kelancaran, kemudahan, kekuatan dan kasih sayang-Nya.
2. Terimakasih kepada kedua orang tua saya, Bapak Agus Haryanto dan Ibu Rusmiyanti atas kasih sayang, doa dan dukungannya sampai sejauh ini.
3. Terimakasih untuk kakak tersayang Eko Hadiyanto dan adik-adikku tercinta M. Syaiful Mujab dan Syifa Nadya M, atas doa dan dukungan kalian.
4. Terimakasih untuk *my partner in crime* Padaria Mulya Paramanandi yang tak pernah bosan menemani, mengingatkan dan mendukung saya.
5. Bapak Joko Dwi Santoso, M.Kom yang telah membimbing dan membantu saya dari awal sampai akhir proses pembuatan skripsi serta telah memberikan dukungan saat ujian pendadaran. Terimakasih banyak.
6. Para dosen STMIK Amikom Yogyakarta yang telah memberikan banyak ilmu selama kuliah.
7. Sahabat-sahabat seperjuangan Meja Hijau yang tidak bisa saya sebutkan satu-persatu. Kalian sudah saya anggap seperti keluarga saya sendiri. Semua cerita dan kenangan yang pernah ada akan selalu menjadi memori indah. Terimakasih atas canda tawa kebersamaan, dukungan, nasehat dan doa kalian semua.
8. Teman-teman 12-S1TI-10 yang telah menemani dari awal kuliah sampai selesai. Terimakasih telah memberikan saya banyak pelajaran hidup. Semoga kita semua sukses dan apapun yang kita cita-citakan dapat tercapai.

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat, hidayah dan karunia-Nya. Shalawat serta salam senantiasa tercurahkan kepada baginda Nabi Besar Muhammad SAW, sehingga tugas akhir dalam bentuk skripsi yang berjudul "Aplikasi Catatan Harian Menggunakan Keamanan Algoritma AES 256 dan SHA 2" ini dapat diselesaikan sesuai dengan waktu yang telah direncanakan.

Tugas akhir ini merupakan syarat terakhir yang harus ditempuh untuk menyelesaikan pendidikan pada jenjang Strata Satu (S1) dan memperoleh gelar Sarjana Komputer, sekaligus sebagai tanda bahwa mahasiswa telah menyelesaikan kuliah pada Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.

Pada kesempatan ini penulis menyampaikan rasa hormat dan terimaksih kepada:

1. Bapak Prof. Dr. M.Suyanto, M.M selaku ketua STMIK Amikom Yogyakarta.
2. Bapak Sudarmawan, M.T selaku ketua Jurusan S1 Teknik Informatika.
3. Bapak Joko Dwi Santoso, M.Kom selaku dosen pembimbing. Terimakasih atas segala bimbingan dan ilmu pengetahuan yang telah diberikan.
4. Bapak/Ibu Dosen dan seluruh staff serta pegawai STMIK Amikom Yogyakarta yang telah memberikan ilmu dan kemudahan selama menuntut ilmu.

Dan semua pihak yang telah membantu penulis dalam menyelesaikan skripsi ini, yang tidak bisa disebutkan satu-persatu. Terimakasih. Dan tentunya

sebagai manusia yang tidak pernah luput dari kesalahan, penulis menyadari bahwa Skripsi ini jauh dari sempurna, untuk itu penulis mengharapkan kritik dan saran yang konstruktif dari semua pihak demi penyempurnaan dimasa yang akan datang.

Akhir kata, semoga Skripsi ini dapat memberikan manfaat bagi pihak- pihak terkait dan pembaca pada umumnya.

Yogyakarta, 30 Juni 2016

Eka Yuliyanti

12.11.6394

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu dengan tujuan agar informasi yang tersimpan tidak dapat terbaca oleh siapapun kecuali orang-orang yang berhak.

Oleh karena itu, sangat diperlukan sebuah sistem keamanan data untuk menjaga kerahasiaan informasi agar tetap terjaga. Salah satunya adalah metode algoritma simetri, karena algoritma ini menggunakan kunci yang sama pada saat melakukan proses enkripsi dan dekripsi data yang sangat besar akan sangat cepat.

Tujuan dari tugas akhir ini adalah membuat sebuah catatan harian atau *diary* berbasis *Mobile* Android dengan tingkat keamanan ganda yang mana terdapat kode-kode khusus untuk membukanya sehingga kerahasiaan yang terdapat di dalamnya baik berupa teks maupun gambar tetap terjaga dengan aman. Algoritma kriptografi (cipher) yang digunakan adalah AES 256 dan SHA 2.

Kata Kunci : Kriptografi, *AES 256*, *SHA 2*, *Diary*, Android.

ABSTRACT

Cryptography is a field of knowledge which uses a mathematical equation to perform the encryption and decryption process. This technique is used to convert the data into the form of a specific code in order for the stored information cannot be read by anyone except those who are eligible.

Therefore, it is necessary a data security system to protect the confidential information in order to stay awake. One of them is the method of symmetric algorithms, as these algorithms use the same key at the time of encryption and decryption process extremely large data sets will be very fast.

The purpose of this thesis is to create a journal or diary-based Mobile Android with multiple security levels that where there are special codes to unlock it so that the confidentiality of the included either text or image is maintained safely. Cryptographic algorithm (cipher) that is used is AES 256 and SHA 2.

Keywords *: Cryptography, AES 256, SHA 2, Diary, Android.*