PENERAPAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES-256) DENGAN MODE CBC DAN *SECURE HASH ALGORITHM* (SHA-256) UNTUK PENGAMANAN DATA FILE

SKRIPSI

Oleh :

SELVIYANI

201710225097

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS BHAYANGKARA JAKARTA RAYA

2021

LEMBAR PERSETUJUAN PEMBIMBING

Judul Skripsi	: Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) Untuk Pengamanan Data File
Nama Mahasiswa	: Selviyani
Nomor Pokok Mahasiswa	: 201710225097
Program Studi / Fakultas	: Informatika / Ilmu Komputer
Tanggal Lulus Ujian Skripsi	: 14 Juli 2021

Bekasi, 19 Juli 2021

MENYETUJUI,

Pembimbing I	Pembimbing II
Ahmad Fathurrozi, S.E., M.M.S.I.	**Rakhmat Purnomo, S.Pd., S.Kom., M.Kom.**
NIDN. 0327117402	**NIDN. 0322108201**

LEMBAR PENGESAHAN

Judul Skripsi	:	Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) Untuk Pengamanan Data File
Nama Mahasiswa	:	Selviyani
Nomor Pokok Mahasiswa	:	201710225097
Program Studi / Fakultas	:	Informatika / Ilmu Komputer
Tanggal Lulus Ujian Skripsi	:	14 Juli 2021

Bekasi, 19 Juli 2021

Mengesahkan,

Ketua Tim Penguji : **R. Wisnu Prio Pamungkas, S.Kom., M.Kom.** .....
NIDN. 0321127201

Penguji (I) : **Sugiyatno, S.Kom., M.Kom.** .....
NIDN. 0313077206

Penguji (II) : **Ahmad Fathurrozi, S.E., M.M.S.I.** .....
NIDN. 0327117402

Mengetahui,

Ketua Program Studi Informatika	Dekan Fakultas Ilmu Komputer
Rakhmat Purnomo, S.Pd., S.Kom., M.Kom.	**Herlawati, S.Si., M.M., M.Kom.**
NIDN. 0322108201	**NIDN. 0311097302**

LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini :

Nama	: Selviyani
NPM	: 201710225097
Program Studi	: Informatika
Fakultas	: Ilmu Komputer
Judul Tugas Akhir	: Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) Untuk Pengamanan Data File

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan **hasil karya saya sendiri dan benar keasliannya**. Apabila dikemudian hari penulisan skripsi ini merupakan plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan tata tertib di Universitas Bhayangkara Jakarta Raya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan dari pihak manapun.

Bekasi, 19 Juli 2021

Selviyani
NPM 201710225097

ABSTRACT

Selviyani. 201710225097. *The implementation of Advanced Encryption Standard (AES-256) Algorithm with CBC Mode and Secure Hash Algorithm (SHA-256) for Data File Security.*

Data Security is one of the important things to protect important messages and information from corruption, compromise or loss so that messages and information remain safe. Encryption and description techniques are considered to be able to secure data properly by protecting files from being easily read or seen by unauthorized parties. In this case, the authors used data from University of Bhayangkara Jakarta Raya to be able to secure their university data using a cryptography symmetrical algorithm called Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) as a solution to existing problems. The AES algorithm process is divided into four steps, the first step is SubBytes, the second step is ShiftRows, the third step is MixColums and the last step is AddRoundKey. And using the SHA algorithm as the hashing function. The algorithm is applied to a desktop-based file description and encryption application with the C sharp programming language.

Keywords: Data File Security, Encryption, Description, Algorithm AES-256, SHA-256

ABSTRAK

Selviyani. 201710225097. Penerapan Algoritma *Advanced Encryption Standard* (AES-256) Dengan Mode CBC dan *Secure Hash Algorithm* (SHA-256) Untuk Pengamanan Data File.

Pengamanan data atau *data protection* merupakan salah satu hal penting untuk melindungi pesan dan informasi penting dari korupsi, kompromi atau kerugian supaya pesan dan informasi tersebut tetap aman. Teknik enkripsi dan deskripsi dinilai dapat mengamankan data dengan tepat dengan melindungi file agar tidak mudah untuk dibaca atau dilihat oleh pihak yang tidak berwenang. Pada penelitian ini penulis menggunakan data dari Universitas Bhayangkara Jakarta Raya untuk dapat mengamankan data universitas mereka menggunakan algoritma kriptografi simetris *Advanced Encryption Standard* (AES) dan *Secure Hash Algorithm* (SHA) sebagai solusi untuk masalah yang ada. Proses algoritma AES sendiri terbagi menjadi empat langkah, langkah pertama yaitu *SubBytes*, langkah kedua *ShiftRows*, langkah ketiga *MixColums* dan langkah terakhir yaitu *AddRoundKey*. Serta menggunakan algoritma SHA sebagai fungsi hashing-nya. Penerapan algoritma tersebut diterapkan ke dalam aplikasi enkripsi dan deskripsi file berbasis desktop dengan bahasa pemograman C sharp.

Kata Kunci : Pengamanan Data, Enkripsi, Deskripsi, Algoritma AES-256, SHA-256

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

Sebagai sivitas akademik Universitas Bhayangkara Jakarta Raya, saya yang bertanda tangan di bawah ini :

Nama	: Selviyani
NPM	: 201710225097
Program Studi	: Informatika
Fakultas	: Ilmu Komputer
Jenis Karya	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bhayangkara Jakarta Raya **Hak Bebas Royalti Non-Esklusif (*Non-Exclusive Royalty-Free Right*)**, atas karya ilmiah saya yang berjudul :

"PENERAPAN ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES-256) DENGAN MODE CBC DAN *SECURE HASH ALGORITHM* (SHA-256) UNTUK PENGAMANAN DATA FILE"

beserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-ekslusif ini, Universitas Bhayangkara Jakarta Raya berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya dan mempublikasikannya di Internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik hak cipta.

Segala bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah ini menjadi tanggung jawab saya pribadi

Demikian pernyataan ini saya buat dengan sebenarnya.

Bekasi, 19 Juli 2021

Selviyani

NPM 201710225097

KATA PENGANTAR

Dengan mengucap puji syukur atas nikmat yang diberikan oleh Allah SWT, dan tak lupa sholawat serta salam semoga tercurah kepada Uswah Khasanah Rasulullah SAW. Penulis dapat menyelesaikan tugas akhir ini. Penulisan tugas akhir ini dilakukan dalam rangka memenuhi salah satu syarat akademik untuk mencapai gelar Sarjana Komputer Program Studi Informatika pada Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya. Penulis menyadari bahwa tanpa bantuan dan bimbingan dari beberapa pihak, tugas akhir skripsi ini tidak dapat diselesaikan dengan segera.

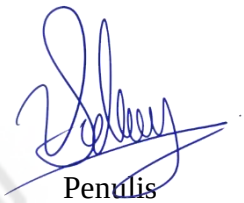
Oleh karena itu, penulis ingin menyampaikan ucapan terimakasih kepada semua pihak yang telah membantu dalam penyusunan Skripsi, dan penulis mengucapkan terimakasih kepada yang terhormat :

1. Bapak Irjen Pol. (Purn) Dr. Drs. Bambang Karsono, S.H., M,M selaku Rektor Universitas Bhayangkara Jakarta Raya.
2. Ibu Herlawati, S.Si., M.M., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
3. Bapak Rakhmat Purnomo, S.Pd., S.Kom., M.Kom., selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
4. Ibu Sri Rezeki, S.Kom., M.Kom., selaku Penasehat Akademik Kelas A2 angkatan 2017 Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
5. Bapak Ahmad Fathurrozi, S.E., M.M.S.I., selaku Dosen Pembimbing Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
6. Keluarga tercinta, Bapak dan Kakak yang selalu memberikan dukungan dan do’a untuk penulis.
7. Stephan Verbücheln yang selalu menemani dan memberi dukungan serta bantuan dalam menjalani proses penelitian ini.
8. Saudari Neina Corina, Eno Widyasari dan seluruh teman-teman seperjuangan di Program Informatika Angkatan 2017 yang selalu memberikan dukungan selama ini.

Karena kebaikan dari beliau-beliau, maka penulis dapat menyelesaikan skripsi ini dengan baik. Penulis menyadari bahwa penyusunan laporan ini tidak luput dari kesalahan dan kekurangan, maka dengan segala kerendahan hati, penulis menerima kritik dan saran yang membangun dari pembaca.

Akhir kata, semoga Allah Yang Maha Pengasih dan Maha Penyayang melimpahkan berkah dan anugerah-Nya kepada semua pihak dan membalas semua amal ibadahnya. Penulis berharap semoga Skripsi ini dapat memberikan manfaat bagi pihak yang memerlukan.

Bekasi, 19 Juli 2021



Penulis

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN