KOMBINASI ALGORITMA *ADVANCED ENCRYPTION STANDART* (AES) DAN METODE PERTUKARAN KUNCI DIFFIE-HELLMAN PADA PENGAMANAN CITRA DIGITAL MEDIS

SKRIPSI

YUGO BAYU PRASTYO
1510511016

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2019

KOMBINASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN METODE PERTUKARAN KUNCI DIFFIE-HELLMAN PADA PENGAMANAN CITRA DIGITAL MEDIS

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Komputer

YUGO BAYU PRASTYO

1510511016

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2019

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan benar.

Nama : Yugo Bayu Prastyo
NIM : 1510511016
Tanggal : 17 Mei 2019

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan di proses sesuai dengan ketentuan yang berlaku.

Jakarta, 17 Mei 2019

Yang Menyatakan,

(Yugo Bayu Prastyo)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional "Veteran" Jakarta, saya yang bertanda tangan di bawah ini :

Nama	: Yugo Bayu Prastyo
NIM	: 1510511016
Fakultas	: Ilmu Komputer
Program Studi	: Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional "Veteran" Jakarta Hak Bebas Royalti Non eksklusif *(Non-exclusive Royalty Free Right)* atas karya ilmiah saya yang berjudul:

Kombinasi Algoritma *Advanced Encryption Standard* (AES) dan Metode Pertukaran Kunci *Diffie-Hellman* Pada Pengamanan Citra Digital Medis

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional "Veteran" Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data *(database)*, merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.
Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada Tanggal : 17 Mei 2019

Yang menyatakan,

(Yugo Bayu Prastyo)

PENGESAHAN

Skripsi diajukan oleh :

Nama : Yugo Bayu Prastyo

NIM : 1510511016

Program Studi : Informatika

Judul Skripsi : **Kombinasi Algoritma *Advanced Encryption Standard* (AES) dan Metode Pertukaran Kunci *Diffie-Hellman* Pada Pengamanan Citra Digital Medis.**

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.

Jayanta, S.Kom.,M.Si.
Penguji I

Ridwan Raafi'udin, S.Kom, M.Kom.
Penguji II

Dr. Ermatita, M.Kom.
Pembimbing I

I Wayan Widi Pradayana, S.Kom.,M.TI.
Pembimbing II

Dr. Ermatita, M.Kom.
Dekan Fakultas Ilmu Komputer

Anita Muliawati, S.Kom.,M.TI
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 21 Juni 2019

KOMBINASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN METODE PERTUKARAN KUNCI DIFFIE-HELLMAN PADA PENGAMANAN CITRA DIGITAL MEDIS

Yugo Bayu Prastyo

ABSTRAK

Data rekam medis merupakan data sensitif yang perlu dijaga tingkat keamanan dan kerahasiaannya. Salah satu bentuk data rekam medis adalah citra medis. Di dalam citra medis terdapat berbagai informasi pribadi mengenai pasien. Dalam melakukan pertukaran informasi citra medis, sering kali data citra tersebut mengalami kebocoran sehingga pihak yang tidak berwenang dapat mengetahui isi citra tersebut. Penelitian ini bertujuan untuk mengembangkan suatu pengamanan citra digital medis yang menggunakan kombinasi algoritma AES pada proses enkripsi-dekripsi data dan algoritma Diffie-Hellman pada proses pertukaran kunci untuk menjaga keamanan dan kerahasiaan citra medis. Algoritma AES digunakan pada proses enkripsi dan dekripsi citra, sedangkan algoritma Diffie-Hellman digunakan untuk mengamankan kunci dari algoritma AES tersebut. Dari hasil penelitian ini, di dapatkan hasil bahwa kombinasi algoritma AES dan Diffie-Hellman berhasil mengamankan citra medis. Algoritma Diffie-Hellman akan menghasilkan kunci yang berbeda – beda yang selanjutnya digunakan sebagai kunci AES. Sedangkan algoritma AES mampu mengenkripsi dan mendekripsi citra medis tanpa merubah isi dari citra tersebut.

Kata kunci: Kriptografi, Citra Medis, Algoritma *Advanced Encryption Standard* (AES), Algoritma Diffie-Hellman, Enkripsi, Dekripsi

COMBINATION OF ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM AND DIFFIE-HELLMAN KEY EXCHANGE METHODS ON MEDICAL DIGITAL IMAGE PACIFIER

Yugo Bayu Prastyo

ABSTRACT

The medical record data is sensitive data that needs to be maintained at the level of security and confidentiality. One of medical record data is a medical image. In the medical image there are various personal information about the patient. In exchanging medical image information, often the image data is leaked so that unauthorized parties can find out the contents of the image. This study aims to develop a medical digital image security that uses a combination of AES algorithms in the process of data encryption and decryption and the Diffie-Hellman algorithm in key exchange processes to maintain the security and confidentiality of medical images. The AES algorithm is used in the process of image encryption and decryption, while the Diffie-Hellman algorithm is used to secure the keys of the AES algorithm. From the results of this study, the results obtained that the combination of AES and Diffie-Hellman algorithms succeeded in securing medical images. The Diffie-Hellman algorithm will produce different keys which are then used as AES keys. While the AES algorithm is able to encrypt and decrypt medical images without changing the contents of the image.

Keyword: *Cryptography, Medical Image, Advanced Encryption Standard (AES) Algorithm, Diffie-Hellman Algorithm*

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala nikmat, rahmat dan hidayah-Nya, shalawat serta salam juga tak lupa tercurahkan kepada Nabi Muhammad SAW, sehingga penulis dapat menyelesaikan skripsi.

Penulisan skripsi ini merupakan salah satu syarat untuk memperoleh gelar sarjana Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta. Rasa terimakasih penulis ucapkan kepada :

1. Dr. Ermatita Zuhairi Sattar, M.Kom. selaku dekan Fakultas Ilmu Komputer dan dosen pembimbing tugas akhir.
2. Anita Muliawati, S.Kom.,M.TI, selaku ketua program studi Informatika Fakultas Ilmu Komputer.
3. Henki Bayu Seta., M.Kom. selaku pembimbing mata kuliah STI yang membantu mengembangkan ide awal skripsi ini..
4. Ibu Vini Indriasari, ST., M.Sc., Ph.D. selaku dosen pembimbing akademik
5. Ibu, Bapak Dosen Informatika UPN "Veteran" Jakarta atas segala ilmu-ilmu bermanfaat yang telah diberikan.
6. Kedua orang tua Puji Ibnu Abidin (Bapak), Wuryani (Ibu), Merri Endah Purwaningsih (Kakak), dan Yoga Ari Nugroho (Adik) yang telah memberikan dukungan, kekuatan dan doa kepada penulis sehingga dapat menyelesaikan skripsi ini.
7. Teman-teman Informatika 2015 yang tidak dapat disebutkan satu persatu yang selalu menemani masa perkuliahan dan memberikan dukungan kepada penulis.

Akhir kata, semoga skripsi ini dapat bermanfaat bagi para pembacanya.

Jakarta, 17 Mei 2019

Penulis

Yugo Bayu Prastyo

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR