PENERAPAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES)* PADA FITUR PEMESANAN PINJAMAN BUKU MELALUI *OPAC* PERPUSTAKAAN UIGM

SKRIPSI

Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 pada
Program Studi Teknik Informatika

Oleh:

Usda Nilawati
2019.11.0054

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER DAN SAINS
UNIVERSITAS INDO GLOBAL MANDIRI
2024

PENERAPAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES)* PADA FITUR PEMESANAN PINJAMAN BUKU MELALUI *OPAC* PERPUSTAKAAN UIGM

SKRIPSI

Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Program Studi Teknik Informatika

Oleh:

Usda Nilawati
2019.11.0054

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER DAN SAINS
UNIVERSITAS INDO GLOBAL MANDIRI
2024

LEMBAR PENGESAHAN SKRIPSI

Penerapan Algoritma Kriptografi AES pada Fitur Pemesanan Pinjaman Buku melalui OPAC Perpustakaan UIGM

Oleh

Usda Nilawati

NPM : 2019.11.0054

Palembang , 02 Februari 2024

Pembimbing I

Dr. Shinta Puspasari, S.Si., M.Kom
NIK : 2015.01.0132

Pembimbing II

Ir. Nazori Suhandi, M.M
NIK:1999.01.0008

Mengetahui,
Dekan Fakultas Ilmu Komputer dan Sains

Rudi Heriansyah, S.T., M.Eng., Ph.D
NIK:2022.01.0315

LEMBAR PERSETUJUAN DEWAN PENGUJI

Pada hari Jumat tanggal 26 Januari 2024 telah dilaksanakan ujian sidang skripsi :

Nama	:	Usda Nilawati
NPM	:	2019.11.0054
Judul	:	Penerapan Algoritma Kriptografi AES pada Fitur Pemesanan Pinjaman Buku melalui OPAC Perpustakaan UIGM

Oleh Prodi Teknik Informatika Fakultas Ilmu Komputer Universitas Indo Global Mandiri Palembang

Palembang, 2 Februari 2024

Penguji 1,

Rudi Heriansyah, S.T., M.Eng., Ph.D
NIK: 2022.01.0315

Penguji 2,

Lastri Widya Astuti, S.Kom., M.Kom
NIK: 2003.01.0063

Penguji 3,

Ir. Nazori Suhandi, M.M
NIK: 1999.01.0008

Menyetujui,
Ka. Prodi Teknik Informatika

Zaid Romegar Mair, S.T., M.Cs
NIK: 2021.01.0307

SURAT KETERANGAN REVISI SKRIPSI
PROGRAM STUDI TEKNIK INFORMATIKA (S1)
FASILKOM UNIVERSITAS INDO GLOBAL MANDIRI

Kami yang bertanda tangan dibawah ini, menerangkan bahwa :

Nama : Usda Nilawati
NPM : 2019.11.0054
Judul : Penerapan Algoritma Kriptografi AES pada Fitur Pemesanan Pinjaman Buku melalui OPAC Perpustakaan UIGM

Mahasiswa yang namanya tercantum diatas, telah selesai merevisi penulisan SKRIPSI

Palembang, 2 Februari 2024

Penguji 1,

Rudi Heriansyah, S.T., M.Eng., Ph.D
NIK: 2022.01.0315

Penguji 2,

Lastri Widya Astuti, S.Kom., M.Kom
NIK: 2003.01.0063

Penguji 3,

Ir. Nazori Suhandi, M.M
NIK: 1999.01.0008

Menyetujui,
Ka. Prodi Teknik Informatika

Zaid Romegar Mair, S.T., M.Cs
NIK: 2021.01.0307

MOTO DAN PERSEMBAHAN

Bismillaahirrahmaannirrahiim,

Alhamdulillah puji syukur kepada Allah SWT, Karya ini merupakan bentuk rasa syukur saya kepada sang pencipta karena telah memberikan banyak sekali nikmat yang tak terduga kepada saya hingga saat ini, termasuk memberikan saya kesempatan untuk melanjutkan pendidikan pada perguruan tinggi dengan beasiswa bidikmisi meskipun harus perpanjang semester dan bayar sendiri biaya pendidikan selama satu semester:)

Sebagai satu-satunya anak yang bisa melanjutkan pendidikan pada Perguruan Tinggi dengan khusus saya mempersembahkan skripsi ini untuk keluarga besar saya, terutama kedua Orang Tua saya Almarhum Bapak Umar dan Ibu Hasuna yang sangat saya cintai. Terima kasih banyak atas semua bentuk cinta kasih sayang yang sudah diberikan kepada saya dan teruntuk Ibu saya terima kasih banyak atas semua keringat dan perjuangan yang luar biasa hebatnya untuk memenuhi setiap keinginan dan kebutuhan kami anakmu, serta dukungan dan doa yang tidak pernah ada habisnya yang selalu menyertai perjalanan saya, saya sangat bangga terlahir menjadi putri Bapak dan Ibu. Kepada Kakak-kakak, Adik serta keponakan saya yang turut memberikan dukungan serta doa yang menjadi motivasi tersendiri bagi saya sehingga saya bisa sampai pada titik ini. Skripsi ini saya persembahkan untuk kalian, sebagai bentuk terijabahnya salah satu dari sekian banyak nya doa yang kalian langitkan pada-Nya untukku. Semoga ini menjadi kebanggaan tersendiri bagi Keluarga dan semoga akan berguna bagi orang-orang sekitar.

"Selalu ada harga dalam sebuah proses. Nikmati saja lelah-lelah ini. Lebarkan lagi rasa sabar itu Semua yang kau investasikan untuk menjadikan dirimu serupa yang kau impikan, mungkin tidak akan selalu berjalan lancar. Tapi, gelombang-gelombang itu yang nanti bisa kau ceritakan"

(Boy Candra)

PENERAPAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES)* PADA FITUR PEMESANAN PINJAMAN BUKU MELALUI *OPAC* PERPUSTAKAAN UIGM

ABSTRAK

Perpustakaan berperan penting dalam dunia pendidikan, saat ini perpustakaan sudah menggunakan sistem katalog yang bisa diakses secara *online* melalui *Online Public Access Catalog* (*OPAC*). Penggunaan *OPAC* sangat membantu mempermudah pengguna perpustakaan dalam mencari koleksi buku perpustakaan. Namun penggunaan *OPAC* juga memiliki resiko keamanan yang perlu diperhatikan, maka dari itu perlu diterapkan sebuah teknik kriptografi untuk mengamankan data. Teknik kriptografi yang digunakan adalah metode *AES* (*Advanced Encryption Standard*) 128-bit. Proses enkripsi pada *AES* 128-bit melibatkan transisi *state* secara berulang dalam 10 putaran. Setiap putaran melibatkan empat transformasi dalam urutan *SubBytes, ShiftRows, MixColumns*, dan *AddRoundKey*, kecuali pada putaran terakhir (tidak melakukan transformasi *MixColoumns*). Hasil pengujian menunjukkan bahwa sistem yang dibuat berhasil mengamankan data yang semula berbentuk *plain text* menjadi *cipher text.*, Panjangnya karakter pesan yang akan dienkripsi mempengaruhi kecepatan waktu proses. Kecepatan rata-rata dari waktu proses pengujian algoritma *AES* 128-bit pada proses enkripsi adalah 4,78 detik dan pada proses dekripsi adalah 2,635 detik.

Kata Kunci: Kriptografi, Algoritma *AES*, Perpustakaan, *OPAC*

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) CRYPTOGRAPHY ALGORITHM ON BOOK BORROWING ORDER FEATURE OF THE UIGM'S LIBRARY OPAC

ABSTRACT

Libraries play an important role in the world of education, currently libraries use catalog system which can be accessed online via OPAC (Online Public Access Catalog). Using OPAC really helps make it easier for library users to search for library book collections. However, the use of OPAC also has security risks that need considered, therefore it is necessary to apply cryptographic techniques to secure data. The cryptographic technique used is the 128-bit AES (Advanced Encryption Standard) method. The encryption process on 128-bit AES involves repeated state transitions in 10 rounds. Each round involves four transformations in order SubBytes, ShiftRows, MixColumns, and AddRoundKey, except for the last round (no MixColumns transform). The test result show that the system created was successful in securing data that was originally in plain text form into cipher text. The character length of the message to be encrypted affects the processing time speed. The average speed of the 128-bit AES algorithm testing processing time in the encryption process is 4,78 seconds and in the decryption process is 2,635 seconds.

Keywords: Cryptography, AES Algorithm, Library, OPAC.

KATA PENGANTAR

Puji dan syukur penulis persembahkan kepada Tuhan Yang Maha Esa karena akhirnya laporan penelitian ini bisa terselesaikan tepat pada waktunya. Penelitian ini penulis buat dengan judul **PENERAPAN ALGORITMA KRIPTOGRAFI *ADVANCED ENCRYPTION STANDARD (AES)* PADA FITUR PEMESANAN PINJAMAN BUKU MELALUI *OPAC* PERPUSTAKAAN UIGM** dibuat sebagai salah satu syarat untuk menyelesaikan studi pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri.

Penulisan skripsi ini tidak luput dari bantuan orang-orang sekitar, maka dari itu Penulis mengucapkan banyak terima kasih atas bantuan yang diberikan selama penyusunan Skripsi ini kepada:

1. Kedua Orang Tua, Alm. Ayah Umar bin Ibrahim dan Ibu Hasuna. Terima kasih banyak atas semua hal yang sudah diperjuangkan untuk saya. Terima kasih atas doa-doa yang dilangitkan kepada-Nya untuk kebaikan saya, hingga akhirnya saya bisa sampai pada titik ini.
2. Dr. Marzuki Alie, S.E., MM, selaku Rektor Universitas Indo Global Mandiri Palembang.
3. Rudi Heriansyah, S.T., M.Eng., Ph.D, selaku Dekan Fakultas Ilmu Komputer dan Sains.
4. Zaid Romegar Mair, S.T., M.Cs, selaku Ketua Program Studi Teknik Informatika.
5. Dewi Sartika, M.Kom, Selaku Eks. Ketua Prodi masa jabatan 2019-2023 telah banyak membantu proses perkuliahan selama masa jabatan.
6. Dr. Shinta Puspasari, S.Si., M.Kom, selaku Dosen Pembimbing I.
7. Ir. Nazori Suhandi, M.M, selaku Dosen Pembimbing II.
8. Dr. Rendra Gustriansyah, S.T., M.Kom, selaku Pembimbing Akademik.
9. Dosen-dosen serta staf yang ada di Fakultas Ilmu Komputer dan Sains Universitas Indo Global Mandiri Palembang.
10. Seluruh keluarga besar, Kakak-kakak dan adik yang telah memberikan dukungan serta semangat selama proses penulisan skripsi ini. Dukungan dari

mereka lah yang memberikan motivasi tersendiri bagi saya untuk berkomitmen dalam menyelesaikan skripsi ini.

11. Seluruh petugas perpustakaan Universitas Indo Global Mandiri yang telah mengizinkan saya untuk melakukan penelitian disana serta telah membantu saya dalam proses pengumpulan data
12. Satra Nurdi, terima kasih banyak sudah menemani dan memberi banyak dukungan pada proses ini, serta selalu siap memberikan bantuan jika dibutuhkan..
13. Teman-teman seperjuangan yang bersama-sama membantu, memberikan dukungan dan saran dalam proses pengerjaan skripsi ini.
14. Terakhir, terima kasih kepada diri sendiri yang telah bertahan sejauh ini, berusaha semaksimal mungkin melakukan yang terbaik dan telah berusaha konsisten berprogres dalam penyelesaian skripsi ini.

Terima kasih atas semua bentuk bantuan yang sudah diberikan, saya bersyukur bisa menyelesaikan skripsi ini tepat pada waktunya. Semoga amal baik yang telah diberikan mendapatkan balasan dari Allah SWT.

Penyusunan Skripsi ini belum begitu sempurna tentunya masih ada kekurangan untuk itu saya selaku penulis sangat mengharapkan saran dan kritik yang sifatnya membangun agar dapat digunakan demi perbaikan dan pengembangan penelitian ini nantinya. Saya juga berharap agar penelitian ini dapat memberikan banyak manfaat bagi yang membacanya.

Palembang, 11 Januari 2024

Penulis,

Usda Nilawati

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN