PERANCANGAN APLIKASI PENGAMANAN DATA MENGGUNAKAN ALGORITMA RSA (RIVEST SHAMIR ADLEMAN) DAN AES (ADVANCED ENCRYPTION STANDARD) BERBASIS WEB

SKRIPSI

Oleh:
Dika Alfiani Fauzan
201910225114

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BHAYANGKARA JAKARTA RAYA
2023

LEMBAR PERSETUJUAN PEMBIMBING

Judul Skripsi	:	Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web
Nama Mahasiswa	:	Dika Alfiani Fauzan
Nomor Pokok Mahasiswa	:	201910225114
Program Studi/Fakultas	:	Informatika/Ilmu Komputer
Tanggal Lulus Ujian Skripsi	:	

Bekasi, 20/07/2023

MENYETUJUI,

Pembimbing I	Pembimbing II
Sugiyatno, S.Kom., M.Kom.	Ahmad Fathurrozi, S.E., M.M.S.I.
NIDN : 0313077206	NIDN : 0327117402

LEMBAR PENGESAHAN

Judul Skripsi	:	Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web
Nama Mahasiswa	:	Dika Alfiani Fauzan
Nomor Pokok Mahasiswa	:	201910225114
Program Studi/Fakultas	:	Informatika/Ilmu Komputer
Tanggal Lulus Ujian Skripsi	:	

Bekasi, 20/07/2023

MENGESAHKAN,

Ketua Tim Penguji	:	Kusdarnowo Hantoro, S.Kom., M.Kom. NIDN : 0329076601	.....
Penguji I	:	Rafika Sari, S.Si., M. Si. NIDN : 0329098902	.....
Penguji II	:	Sugiyatno, S.Kom., M.Kom. NIDN : 0313077206	.....

MENGETAHUI,

Ketua Program Studi Informatika	Dekan Fakultas Ilmu Komputer
Ahmad Fathurrozi, S.E., M.M.S.I.	Dr. Dra. Tyastuti Sri Lestari, M.M.
NIDN : 0327117402	NIDN : 0327036701

UNIVERSITAS BHAYANGKARA JAKARTA RAYA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA

LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini :

Nama	: Dika Alfiani Fauzan
NPM	: 201910225114
Program Studi	: Informatika
Fakultas	: Ilmu Komputer
Judul Tugas Akhir	: Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web

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, 20 Juli 2023
Penulis

Dika Alfiani Fauzan

ABSTRAK

Dika Alfiani Fauzan. 2023. Kriptografi adalah metode untuk melindungi pesan rahasia dengan mengubahnya menjadi bentuk yang tidak dapat dimengerti oleh pihak yang tidak berhak. Berbagai algoritma kriptografi, seperti RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard), telah dikembangkan untuk melindungi data dan informasi dari akses yang tidak sah. Kombinasi AES dan RSA sering digunakan bersama-sama untuk mencapai keamanan yang optimal. Penelitian ini bertujuan untuk menerapkan keamanan data pada PT.XYZ dengan menggunakan kombinasi algoritma kriptografi AES dan RSA. AES digunakan untuk mengenkripsi dan mendekripsi dokumen/data, sedangkan RSA berperan sebagai enkripsi dan dekripsi untuk kunci AES. Dengan demikian, kelebihan dari kedua algoritma ini dapat dimanfaatkan untuk mencapai keamanan dan kerahasiaan data yang kuat. Penelitian ini menggunakan pendekatan kuantitatif dengan mengimplementasikan algoritma AES dan RSA dalam aplikasi web menggunakan bahasa pemrograman HTML, PHP, CSS, dan JavaScript. Aplikasi ini juga memanfaatkan Web API untuk proses enkripsi dan dekripsi data. Hasil dari penelitian ini adalah aplikasi web yang dapat mengenkripsi dan mendekripsi dokumen/data menggunakan AES dan RSA. Aplikasi ini juga dapat melakukan pertukaran kunci dengan menggunakan algoritma RSA. Implementasi AES dan RSA dalam aplikasi ini berhasil memperlihatkan bahwa semua file dan teks yg dienkripsi dapat berubah menjadi file berekstensi (*.encrypted*) yang tidak dapat dibuka tanpa kunci privat, serta dapat dikembalikan ke file aslinya dalam proses dekripsi dan tidak mengalami perubahan, dengan tingkat keberhasilan 100%. plikasi web dengan kombinasi algoritma kriptografi AES dan RSA pada PT.XYZ menunjukkan waktu enkripsi dan dekripsi yang relatif cepat, dengan rata-rata waktu kurang dari 1 detik. Waktu enkripsi dan dekripsi yang efisien ini menunjukkan kinerja yang baik dari implementasi kriptografi dalam melindungi data dan informasi pada aplikasi ini.

Kata Kunci : Pengamanan Data, Pembangkitan Kunci, Enkripsi, Deskripsi, Algoritma RSA, Algoritma AES

ABSTRACT

Dika Alfiani Fauzan. 2023. Cryptography is a method to protect secret messages by transforming them into a form that is unintelligible to unauthorized parties. Various cryptographic algorithms, such as RSA (Rivest Shamir Adleman) and AES (Advanced Encryption Standard), have been developed to safeguard data and information from unauthorized access. The combination of AES and RSA is often used together to achieve optimal security. This research aims to implement data security at PT.XYZ using a combination of AES and RSA cryptographic algorithms. AES is used for encrypting and decrypting documents/data, while RSA serves as the encryption and decryption for the AES key. Thus, the advantages of both algorithms can be utilized to achieve strong data security and confidentiality. This research adopts a quantitative approach by implementing AES and RSA algorithms in a web application using HTML, PHP, CSS, and JavaScript programming languages. The application also leverages Web API for data encryption and decryption processes. The result of this research is a web application that can encrypt and decrypt documents/data using AES and RSA. The application also enables key exchange using the RSA algorithm. The implementation of AES and RSA in this application successfully demonstrates that all encrypted files and texts can be transformed into (.encrypted) files that cannot be opened without the private key, and they can be restored to their original form during the decryption process without any changes, with a success rate of 100%. The web application with a combination of AES and RSA cryptographic algorithms at PT.XYZ exhibits relatively fast encryption and decryption times, with an average time of less than 1 second. This efficient encryption and decryption time indicates the good performance of cryptography implementation in safeguarding data and information in this application.

Keywords* : *Data Protection, Key Generation, Encryption, Description, Algorithm AES, Algorithm RSA

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

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

Nama	: Dika Alfiani Fauzan
NPM	: 201910225114
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 :

"Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web"

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, 20 Juli 2023

Yang Menyatakan,

Dika Alfiani Fauzan

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT atas segala karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **"APLIKASI PENGAMANAN DATA MENGGUNAKAN ALGORITMA RSA (RIVEST SHAMIR ADLEMAN) DAN AES (ADVANCED ENCRYPTION STANDARD) BERBASIS WEB"** yang disusun sebagai syarat untuk mencapai Sarjana S1 Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya.

Penulis menyadari bahwa skripsi ini dapat selesai karena adanya bantuan dan dukungan dari berbagai pihak. Oleh karena itu penulis mengucapkan terima kasih kepada:

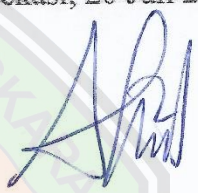
1. Bapak Irjen pol (Purn) Dr. Drs. Bambang Karsono, SH, MM. Selaku Rektor Universitas Bhayangkara Jakarta Raya.
2. Ibu Dr. Dra. Tyastuti Sri Lestari, M.M. selaku Dekan Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
3. Bapak Ahmad Fathurrozi, S.E., M.M.S.I. selaku Kepala Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Bhayangakra Jakarta Raya.
4. Bapak Sugiyatno, S.Kom., M.Kom. selaku Dosen Pembimbing 1 di Universitas Bhayangkara Jakarta Raya yang telah memberikan bimbingan dan arahan guna terwujudnya penulisan skripsi ini.
5. Bapak Ahmad Fathurrozi, S.E., M.M.S.I. selaku Dosen Pembimbing 2 di Universitas Bhayangkara Jakarta Raya yang telah memberikan bimbingan dan arahan guna terwujudnya penulisan skripsi ini.
6. Seluruh Dosen Program Studi Informatika yang senantias memberikan ilmu yang sangat bermanfaat.

   Tak lupa penulis mengucapkan terima kasih yang sebesar-besarnya khususnya kepada:
7. Orang tua saya, Ibu Sri Jayaningsih dan Bapak Yadi Riyadi yang selalu memberikan doa dan dukungannya kepada saya.

8. Adik-adik saya, Disya dan Cintia, orang terdekat saya, Ichsan dan teman-teman saya, Trya dan Syarifah yang telah memberikan dukungan moril dan bantuan kepada saya selama ini. Serta teman-teman saya yang tidak bisa disebutkan namanya satu-persatu.

Penulis menyadari bahwa penulisan masih jauh dari sempurna, untuk itu, penulis menerima kritik dan saran yang bersifat membangun demi kesempurnaan penulis di masa mendatang. Akhirnya penulis berharap semoga skripsi ini bisa bermanfaat untuk masyarakat luas.

Bekasi, 20 Juli 2023



Dika Alfiani Fauzan

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN