

**PERANCANGAN APLIKASI PENGAMANAN DATA
MENGUNAKAN 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 :



Sugiyatno, S.Kom., M.Kom.

NIDN : 0313077206

Ahmad Fathurrozi, S.E., M.M.S.I.

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

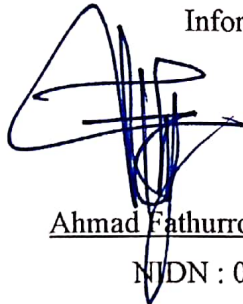
Penguji II : Sugiyatno, S.Kom., M.Kom.

NIDN : 0313077206

MENGETAHUI,

Ketua Program Studi

Informatika

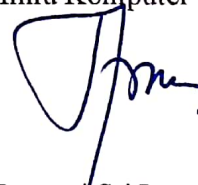


Ahmad Fathurrozi, S.E., M.M.S.I.

NIDN : 0327117402

Dekan Fakultas

Ilmu Komputer



Dr. Dra. Tyastuti Sri Lestari, M.M.

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%. Aplikasi 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-Eksklusif** (*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-eksklusif 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 izin 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 kehadiran 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 Bhayangkara 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 senantiasa 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

LEMBAR PERSETUJUAN PEMBIMBING.....	i
LEMBAR PENGESAHAN.....	ii
LEMBAR PERNYATAAN.....	iii
ABSTRAK.....	iv
ABSTRACT.....	v
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah.....	3
1.3 Tujuan dan Manfaat.....	3
1.4 Batasan Masalah.....	3
1.5 Sistematika Penulisan.....	4
BAB II LANDASAN TEORI.....	5
2.1 Tinjauan Pustaka.....	5
2.2 Kriptografi.....	8
2.2.1 Terminologi dalam Kriptografi.....	9
2.2.2 Tujuan Kriptografi.....	11
2.2.3 Jenis-jenis Algoritma Kriptografi.....	12
2.3 RSA (Rivest Shamir Adleman).....	14
2.3.1 Cara kerja RSA.....	15
2.3.2 Perhitungan RSA.....	18
2.4 AES (Advanced Encryption Standard).....	20

2.4.1 Cara kerja AES.....	21
2.4.2 Perhitungan AES.....	22
2.5 HTML.....	29
2.6 CSS.....	29
2.7 JavaScript.....	30
2.8 Penggunaan HTML, CSS, dan JavaScript.....	31
2.9 Web API.....	33
2.10 Metode RAD (Rapid Application Development).....	34
BAB III METODOLOGI PENELITIAN.....	36
3.1 Objek Penelitian.....	36
3.1.1 Struktur Organisasi.....	36
3.2.2 Fungsi dan Tanggung Jawab.....	37
3.2 Kerangka Berpikir.....	39
3.3 Metode Penelitian.....	42
3.4 Analisis Sistem Berjalan.....	42
3.5 Permasalahan.....	45
3.6 Analisis Sistem Usulan.....	46
3.7 Analisis Kebutuhan Sistem.....	49
BAB IV PERANCANGAN SISTEM DAN IMPLEMENTASI.....	50
4.1 Pemodelan Proses.....	50
4.1.1 <i>Use Case Diagram</i>	50
4.1.2 <i>Activity Diagram</i>	50
4.1.3 <i>Sequence Diagram</i>	55
4.1.4 <i>Class Diagram</i>	58
4.2 Pembahasan Algoritma.....	59
4.3 Implementasi Sistem.....	60
4.4 Pengujian.....	67
BAB V PENUTUP.....	73
5.1 Kesimpulan.....	73
5.2 Saran.....	73

DAFTAR PUSTAKA.....	75
LAMPIRAN.....	77



DAFTAR TABEL

Tabel 2.1 Deskripsi Penelitian Sebelumnya	5
Tabel 2.2. Tabel Konstan <i>Rcon</i>	22
Tabel 2.3. Tabel Substitusi untuk Transformasi <i>Subbytes</i>	25
Tabel 4.1 Hasil Pengujian.....	67
Tabel 4.2 Perbandingan Ukuran File Sebelum dan Sesudah Enkripsi 1.....	69
Tabel 4.3 Perbandingan Ukuran File Sebelum dan Sesudah Enkripsi 2.....	70
Tabel 4.4 Perbandingan Ukuran File Sebelum dan Sesudah Enkripsi 3.....	70



DAFTAR GAMBAR

Gambar 2.1 Proses enkripsi dan dekripsi	9
Gambar 3.1 Kerangka Berpikir	40
Gambar 3.2 <i>Flowmap</i> Analisis Sistem Berjalan	43
Gambar 3.3 <i>Flowmap</i> Analisis Usulan Sistem	47
Gambar 3.4 <i>Flowchart</i> Proses Enkripsi Dekripsi.....	48
Gambar 4.1 <i>Use Case Diagram</i>	50
Gambar 4.2 <i>Activity Diagram</i> Login.....	51
Gambar 4.3 <i>Activity Diagram</i> Pembangkitan Kunci	52
Gambar 4.4 <i>Activity Diagram</i> Enkripsi Teks/File.....	53
Gambar 4.5 <i>Activity Diagram</i> Enkripsi Teks/File.....	54
Gambar 4.6 <i>Sequence Diagram</i> Login	55
Gambar 4.7 <i>Sequence Diagram</i> Pembangkitan Kunci	56
Gambar 4.8 <i>Sequence Diagram</i> Enkripsi Teks/File	57
Gambar 4.9 <i>Sequence Diagram</i> Dekripsi Teks/File.....	57
Gambar 4.10 <i>Class Diagram</i>	59
Gambar 4.11 Algoritma pada Sistem	60
Gambar 4.12 Halaman Pembangkitan Kunci Sebelum.....	60
Gambar 4.13 Halaman Pembangkitan Kunci Sesudah.....	61
Gambar 4.14 Halaman Enkripsi Teks Sebelum.....	62
Gambar 4.15 Halaman Enkripsi Teks Sesudah.....	62
Gambar 4.16 Halaman Dekripsi Teks Sebelum.....	63
Gambar 4.17 Halaman Dekripsi Teks Sesudah	63
Gambar 4.18 Halaman Enkripsi File Sebelum.....	63
Gambar 4.19 Halaman Enkripsi File Sesudah.....	64
Gambar 4.20 File Sebelum Enkripsi.....	64

Gambar 4.21 File Sesudah Enkripsi.....	65
Gambar 4.23 Halaman Dekripsi File Sebelum.....	65
Gambar 4.24 Halaman Enkripsi File Sesudah.....	66
Gambar 4.25 File Sesudah Dekripsi.....	66



DAFTAR LAMPIRAN

<i>Source Code</i>	77
Plagiarisme.....	93
Biodata Mahasiswa.....	94
Kartu Bimbingan Skripsi.....	95

