Jurnal Elektronik Ilmu Komputer Udayana
Volume 13, No 4. May 2025

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Implementasi Fitur Keamanan Enkripsi End-To-End Pada Aplikasi Bimbingan Online Tugas Akhir Berbasis Website

I Putu Krisna Megadana[a1], I Gusti Ngurah Anom Cahyadi Putra[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]krisnamegadana104@student.unud.ac.id
[2]anom.cp@unud.ac.id

Abstract

Data security Is one of the main challenges in digital era, especially in web-based applications used for online final assignment guidance services. This study aims to implement an end-to-end encryption security feature using the RSA algorithm in a web-based online guidance application. The RSA algorithm was selected for its reliability as a public key cryptography method, enabling data to be accessed only by parties possessing the corresponding private key. The research process includes system requirement analysis, system design, RSA algorithm implementation for data encryption and decryption, and application security testing. Testing results demonstrate that this feature provides robust data protection, ensuring Ensuring that information is accessible only to authorized individuals. senders and recipients. Through the application of this security feature, this research is expected to enhance user trust in online guidance services, safeguard personal data, and serve as a reference for other developers in implementing secure and efficient encryption technologies.

Keywords: *Data Security, End-to-End Encryption, RSA, Web Application, Online Guidance*

1. Pendahuluan

Dalam era digital saat ini, layanan bimbingan online semakin populer dan diterima secara luas sebagai solusi alternatif untuk memperoleh akses ke pembelajaran tanpa harus berada di ruang kelas secara fisik. Teknologi berbasis web memberikan kemudahan akses informasi yang cepat, fleksibilitas, dan kenyamanan. Namun, kemajuan ini diiringi dengan meningkatnya risiko keamanan, khususnya dalam melindungi data sensitif pengguna seperti informasi pribadi dan catatan bimbingan [6].

Masalah keamanan menjadi salah satu perhatian utama karena aplikasi berbasis web rentan terhadap serangan siber, seperti penyadapan, manipulasi data, dan pencurian identitas. Menurut laporan terbaru, insiden kebocoran data meningkat setiap tahunnya, yang sering kali menyebabkan hilangnya kepercayaan pengguna terhadap platform online. Oleh karena itu, perlindungan data melalui sistem keamanan yang efektif menjadi kebutuhan mendesak, terutama dalam layanan yang melibatkan interaksi pengguna secara langsung [10].

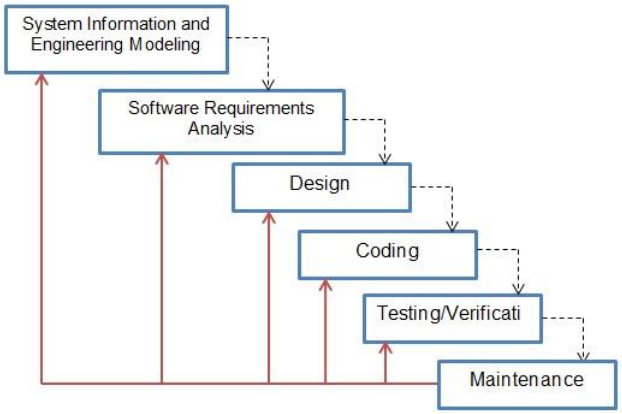
Algoritma RSA (Rivest-Shamir-Adleman) adalah salah satu metode kriptografi berbasis kunci publik terkemuka, telah terbukti andal dalam melindungi data melalui proses enkripsi dan dekripsi. Keunggulan utama RSA terletak pada kemampuan enkripsi data menggunakan kunci publik yang hanya dapat didekripsi oleh kunci privat yang sesuai. Metode ini menjamin bahwa data Hanya dapat diakses oleh pihak yang memiliki otoritas, sehingga mencegah akses tidak sah [3][1].

Dalam konteks layanan bimbingan online, implementasi fitur keamanan berbasis enkripsi end-to-end menggunakan algoritma RSA sangat relevan. Fitur ini tidak hanya melindungi privasi pengguna, tetapi juga meningkatkan kepercayaan terhadap sistem. Dengan mengintegrasikan teknologi enkripsi ini, layanan bimbingan online dapat menawarkan pengalaman yang lebih aman dan andal kepada pengguna, memastikan bahwa data sensitif tetap terlindungi sepanjang proses bimbingan.

2. Metode Penelitian

2.1. Waterfall

Metode Waterfall, atau dikenal sebagai Linear Sequential Model, merupakan pendekatan sistematis dan berurutan dalam pengembangan perangkat lunak. Model ini pertama kali diperkenalkan oleh Winston Royce pada tahun 1970 dan tetap menjadi salah satu model yang banyak digunakan dalam software engineering (SE). Model Waterfall terdiri dari beberapa tahapan yang harus diselesaikan secara berurutan, dimulai dari spesifikasi kebutuhan, perencanaan, permodelan, konstruksi, deployment, hingga pemeliharaan [5][8]. Karakteristik utama model ini adalah sifatnya yang linear, di mana setiap tahapan harus diselesaikan sebelum melanjutkan ke tahap berikutnya tanpa dapat kembali ke tahap sebelumnya seperti pada gambar 1.



Gambar 1. Diagram Waterfall

2.2. Analisis Kebutuhan Sistem

Tahapan ini bertujuan untuk memahami secara mendalam kebutuhan fungsional dan non-fungsional yang diperlukan oleh sistem yang akan dibangun. Kebutuhan fungsional berfokus pada fitur dan fungsi utama yang mendukung operasional sistem, seperti penerapan algoritma RSA untuk menjaga kerahasiaan data seperti pada gambar 2.

No	Deskripsi Kebutuhan Fungsional
KF1	Sistem yang dibangun dapat menampilkan halaman yang memiliki fitur-fitur untuk mendukung bimbingan online, seperti pengiriman pesan dan dokumen.
KF2	Sistem mampu menerima input file dokumen dalam format *.pdf.
KF3	Sistem mampu melakukan enkripsi data pengguna atau catatan bimbingan menggunakan algoritma RSA sebelum data dikirim.
KF4	Sistem mampu mendekripsi data pengguna atau catatan bimbingan terenkripsi di sisi penerima menggunakan kunci privat.
KF5	Sistem mampu pengunduhan dan pengunggahan file kepada pengguna penerima/pengirim.
KF6	Sistem mampu mengelola validasi kunci publik dan kunci privat untuk memastikan proses enkripsi dan dekripsi berjalan dengan benar.
KF7	Sistem mampu menyimpan data pengguna dan catatan bimbingan dalam bentuk terenkripsi di database untuk menjaga kerahasiaan.
KF8	Sistem mampu melakukan forgot password yang akan di kirimkan ke email
KF9	Sistem mampu melakukan perhitungan lama revisi dan lama review
KF10	Sistem mampu melakukan update data pengguna

Gambar 2. Analisis kebutuhan fungsional

p-ISSN: 2301-5373
e-ISSN: 2654-5101

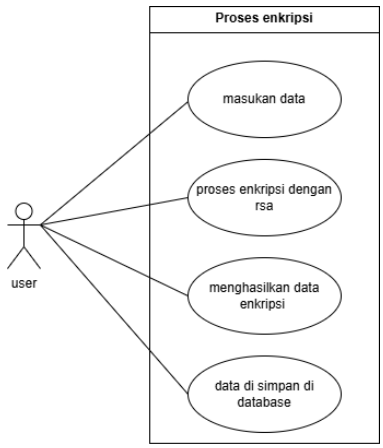
Tabel 1. Analisis Kebutuhan non-fungsional

No.	Perangkat	Keterangan
1.	Laptop	Asus Zenbook Pro Duo
2.	Processor	Intel(R) Core(TM) i7-10510U
3.	Monitor	16 inches
4.	RAM	16 GB
5.	SSD	475 GB
6.	Windows	Sistem operasi windows 11
7.	Dekstop	
8.	Visual Studio Code	*Text editor* yang digunakan untuk membangun aplikasi website
9.	Xampp	*Database* yang di gunakan untuk menyimpan data
10.	Browser	Untuk menjalankan aplikasi website yang sudah di buat

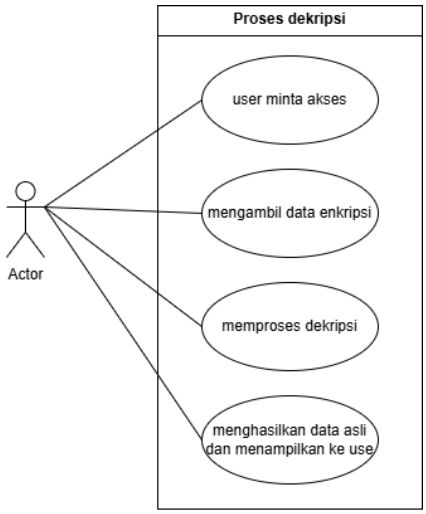
Pada tabel 1, dapat di lihat kebutuhan non-fungsional mencakup aspek-aspek teknis yang menunjang performa, keamanan, dan efisiensi sistem.

2.3. Use case Diagram

Diagram use case adalah sebuah diagram yang berfungsi untuk menggambarkan berbagai aktivitas yang dapat dijalankan oleh suatu sistem [7]. Berikut adalah gambaran Use case diagram enkripsi dan dekripsi pada gambar 3 dan gambar 4.



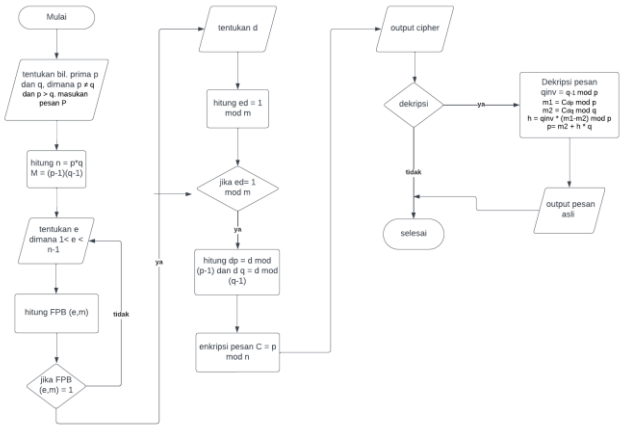
Gambar 3. Use case enkripsi



Gambar 4. Use case dekripsi

2.4. Implementasi Algoritma Rsa

Pada tahap implementasi, algoritma RSA diterapkan untuk memastikan data pengguna seperti NIM, NIP, email, dan password dienkripsi sebelum disimpan atau ditransmisikan. Proses ini melibatkan pembangkitan kunci publik dan privat menggunakan openssl, serta pengintegrasian proses enkripsi dan dekripsi ke dalam alur kerja sistem. Basis data MySQL digunakan untuk menyimpan data terenkripsi, sementara server lokal XAMPP digunakan untuk simulasi dan pengujian sistem [9][4]. Sebelum melibatkan openssl untuk pembangkit kunci publik dan private ada perhitungan manual yang di buat , seperti yang ditunjukkan pada gambar 5 di bawah ini.



Gambar 5. Flowchart Rsa

2.5. Tahap Pengujian

Proses pengujian meliputi pengujian black-box guna memastikan bahwa setiap fitur beroperasi sesuai dengan spesifikasi yang ditetapkan, serta pengukuran efisiensi sistem dalam melakukan proses enkripsi dan dekripsi dan pengujian rsactftool untuk memastikan public key dan private key tidak dapat di eksploitasi. Hasil pengujian menunjukkan bahwa algoritma RSA mampu diintegrasikan secara efisien tanpa mengorbankan performa sistem

p-ISSN: 2301-5373
e-ISSN: 2654-5101

3. Hasil dan Pembahasan

3.1. Hasil Waktu Proses

Penerapan algoritma RSA telah berhasil diintegrasikan ke dalam sistem bimbingan online. Hasil pengujian menunjukkan bahwa fitur enkripsi dan dekripsi mampu menjaga kerahasiaan data seperti NIM, NIP, email, dan password pengguna. Rata-rata waktu proses enkripsi adalah 0,002117 detik, sementara rata-rata waktu proses dekripsi adalah 0,004294 detik, menunjukkan efisiensi yang tinggi tanpa mengurangi performa sistem data dapat diamati pada gambar 6 dan gambar 7.

ID	Nama	Email	Waktu Dekripsi (detik)
2108561113	Wayan Budi Santoso	budisantoso@gmail.com	0.004749
2108561112	Ayu Made Lestari	madelestari@gmail.com	0.003564
2108561111	Gede Rama Setiawan	ramasetiawan@gmail.com	0.003774
2108561110	Kadek Yulia Dewi	yuliadewi@gmail.com	0.003542
2108561109	Putu Wayan Aditya	wayanaditya@gmail.com	0.003738
2108561108	Nyoman Eka Widiastuti	ekawidiastuti@gmail.com	0.006296
2108561107	Komang Bagus Pratama	baguspratama@gmail.com	0.005852
196903011991032001	Dr. Ketut Arta Wijaya, M.Eng	artawijaya@gmail.com	0.003516
198602171998112004	Kadek Dwi Prasetyo, S.T., M.Kom	dwiprasetyo@gmail.com	0.003823
198210101996031007	Dr. Gede Bayu Wirawan, M.T.	bayuwirawan@gmail.com	0.004091
RATA - RATA	0.004294 detik		

Gambar 6. Hasil pengujian waktu proses dekripsi

ID	Nama	Email	Waktu Enkripsi (detik)
2108561113	Wayan Budi Santoso	budisantoso@gmail.com	0.001966
2108561112	Ayu Made Lestari	madelestari@gmail.com	0.002189
2108561111	Gede Rama Setiawan	ramasetiawan@gmail.com	0.001898
2108561110	Kadek Yulia Dewi	yuliadewi@gmail.com	0.001904
2108561109	Putu Wayan Aditya	wayanaditya@gmail.com	0.002122
2108561108	Nyoman Eka Widiastuti	ekawidiastuti@gmail.com	0.002068
2108561107	Komang Bagus Pratama	baguspratama@gmail.com	0.001900
196903011991032001	Dr. Ketut Arta Wijaya, M.Eng	artawijaya@gmail.com	0.001960
198602171998112004	Kadek Dwi Prasetyo, S.T., M.Kom	dwiprasetyo@gmail.com	0.002001
198210101996031007	Dr. Gede Bayu Wirawan, M.T.	bayuwirawan@gmail.com	0.003165
RATA - RATA	0.002117 detik		

Gambar 7. Hasil pengujian waktu proses enkripsi

3.2. Hasil Black-box

Pengujian black-box menunjukkan tabel 2 hasil pengujian black-box proses enkripsi bahwa sistem mampu menjalankan semua fitur yang dirancang dengan baik, termasuk validasi login, update profil, dan pengelolaan data bimbingan. Implementasi ini memberikan perlindungan yang optimal terhadap data sensitif, meningkatkan kepercayaan pengguna terhadap layanan bimbingan online.

Masukan pengguna	Keluar yg diharapkan	Pengamatan	Kesimpulan
NIM /NIP, Nama, Email, Password	1. Data berhasil dienkripsi. 2. Data terenkripsi disimpan ke database.	1. Sistem berhasil menerima input NIM/NIP, Nama, Email, Password. 2. Sistem berhasil mengenkripsi data. 3. Data terenkripsi berhasil disimpan ke database.	Sesuai

Tabel 2. Pengujian Black-box Proses enkripsi

Pengujian black-box, sebagaimana ditunjukkan pada Tabel 3 hasil pengujian black-box proses dekripsi, membuktikan bahwa sistem dapat menjalankan semua fitur yang telah dirancang dengan baik, termasuk validasi login, update profil, dan pengelolaan data bimbingan. Implementasi ini memberikan perlindungan yang optimal terhadap data sensitif, meningkatkan kepercayaan pengguna terhadap layanan bimbingan online.

Masukan Pengguna	Keluar yang Diharapkan	Pengamatan	Kesimpulan
Data terenkripsi	1. Data terenkripsi berhasil didekripsi. 2. Data hasil dekripsi ditampilkan kepada pengguna.	1. Sistem berhasil menerima input data terenkripsi. 2. Sistem berhasil mendekripsi data. 3. Data hasil dekripsi berhasil ditampilkan kepada pengguna.	Sesuai

Tabel 3. Pengujian Black-box Proses enkripsi

3.3. Hasil Rsactf Tool

Pengujian dilakukan menggunakan RsaCtfTool dengan parameter --attack all untuk mengevaluasi kelemahan dalam implementasi kunci RSA 2048-bit pada file public.pem. Berbagai serangan diterapkan, termasuk System Primes GCD Attack, FactorDB Attack, Fermat's Factorization, Pollard's Rho, Wiener's Attack, dan Dixon's Method, namun semuanya gagal karena ukuran modulus yang besar. Beberapa metode mengalami batasan teknis, seperti Pollard's Rho yang mengalami timeout dan Wiener's Attack yang tidak efektif karena eksponen privat tidak cukup kecil. Partial D Attack tidak dapat dijalankan karena kurangnya informasi tentang kunci privat, sementara metode berbasis faktorisasi seperti ECM dan GNFS memerlukan waktu yang terlalu lama untuk memecahkan modulus.

Hasil pengujian menunjukkan bahwa RSA 2048-bit tetap kuat terhadap berbagai serangan berbasis kelemahan umum, menegaskan keamanannya dalam skenario dunia nyata dapat di lihat pada gambar 8.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Gambar 8. Pengujian rsactf tool

4. Kesimpulan

Merujuk pada hasil penelitian ini berhasil mengimplementasikan fitur keamanan enkripsi end-to-end pada aplikasi bimbingan online tugas akhir berbasis website menggunakan algoritma RSA. Pengujian black-box menunjukkan bahwa proses enkripsi dan dekripsi data, validasi login, serta pengelolaan catatan bimbingan berjalan sesuai skenario. Data seperti NIM/NIP, nama, email, dan catatan bimbingan terenkripsi dengan aman dan hanya dapat diakses setelah didekripsi. Waktu proses enkripsi rata-rata tercatat 0,002117 detik, sedangkan dekripsi 0,004294 detik. Variasi waktu dipengaruhi oleh panjang data, namun tetap efisien untuk data kecil hingga sedang. Selain itu, pengujian keamanan dengan RsaCtfTool menunjukkan bahwa kunci RSA 2048-bit yang digunakan tidak memiliki kelemahan signifikan, membuktikan keandalan algoritma ini dalam melindungi data. Implementasi ini meningkatkan keamanan data pengguna dan mencegah akses tidak sah, sehingga memperkuat kepercayaan pengguna terhadap layanan bimbingan online. Penelitian ini juga memberikan kontribusi dalam pengembangan aplikasi web yang aman melalui enkripsi berbasis RSA.

References

[1] S. Sholikhatin, A. Kuncoro, A. Munawaroh, G. Setiawan, "Comparative Study of RSA Asymmetric Algorithm and AES Algorithm for Data Security," Edu Komputika Journal, vol. 9, no. 1, pp. 60-67, 2023.

[2] D. Balasubramanian, M. Arun, K. R. Sekar, "An Improved RSA Algorithm for Enhanced Security," Indian Journal of Cryptography and Network Security, vol. 2, no. 1, pp. 1-4, 2022

[3] A. Muzakir, M. Rahman, "Security Testing Using RSA and RSA-CRT Algorithms in E-Memo Systems," Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, vol. 8, no. 2, pp. 571-578, 2017.

[4] F. M. Wahid, "Analysis of the Waterfall Method for System Development," J. Ilmu-ilmu Inform. dan Manaj. STMIK, vol. 1, no. 1, pp. 1-5, 2020.

[5] K. Wijaya, R. Suparianto, E. Istiawan, "Framework Implementation in Dynamic Website Development," JSK, vol. 4, no. 2, pp. 7-11, 2020.

[6] Asriyanik. 2017. Studi Terhadap Advanced Encryption Standard (AES) dan Algoritma Knapsnack dalam Pengamanan Data. Jurnal Santika : Jurnal Ilmiah Sains dan Teknologi, 7(1), 533-561.

[7] Hasugian, P. S. 2018. Perancangan website sebagai media promosi dan informasi. Journal Of Informatic Pelita Nusantara, 3(1).

[8] Sieghart, S. (2023). The Influence of Fonts on the Reading Performance in Easy-to-Read Texts: A Legibility Study with 145 Participants. Design Issues, 39(3), 30-44.

[9] Josi, A. 2017. Penerapan metode prototiping dalam pembangunan website desa (studi kasus desa sugihan kecamatan rambang). Jurnal Teknologi Informasi Mura, 9(1).

[10] Ridho, R., Bisri, C., & Harahap, A. M. 2023. Penerapan Kriptografi Enkripsi Dan Deskripsi Dalam Pendataan Pasien Klinik Mama Harfas Tembung Menggunakan Visual Basic. Jurnal Penelitian Dan Pengkajian Ilmiah Eksakta, 2(1), 30-33.