Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 1, Januari 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

IMPELEMENTASI ALGORITMA AES DAN RSA UNTUK KEAMANAN PADA APLIKASI WEB CHAT TEAM SYNC

Bagas Hadista Mulyadi[1], Muhammad innuddin [2], Ondi Asroni [3], Muhamad Azwar [4], kurniadin Abdul Latif[5]

[123,]Program Studi Teknologi Informasi Universitas Bumigora, [45,]Program Studi Ilmu Komputer Universitas Bumigora

Jln. Ismail Marzuki No.22, Universitas Bumigora, Cilinaya, Cakranegara, Mataram 83127
[1] remafigas@gmail.com, [2] Inn@universitasbumigora.ac.id, [3] ondi@universitasbumigora.ac.id,
[4] kurniadin@universitasbumigora.ac.id, [5] azwar@universitasbumigora.ac.id

Abstract

The growth of information technology increases the demand for strong security in web-based chat applications that handle sensitive data exchange. This study implements a hybrid cryptosystem combining AES-256 for message encryption and RSA-2048 for secure key distribution in the messaging feature of the Team Sync web application. End-to-end encryption is applied on the client side using JavaScript-based cryptographic libraries, ensuring that the server cannot access message content. The evaluation includes encryption–decryption testing, key security analysis, and message fidelity assessment. The results show that the system performs accurate and lossless encryption and decryption while supporting efficient real-time communication. Therefore, the RSA–AES hybrid approach is proven effective in enhancing confidentiality, integrity, and user privacy within the Team Sync application.

Keywords: RSA-2048, AES-256, Kriptosistem Hybrid, End-to-End Encryption, Keamanan Chat,Team Sync

Abstrak

Perkembangan teknologi informasi meningkatkan kebutuhan akan keamanan data, khususnya pada aplikasi web chat yang digunakan untuk pertukaran informasi sensitif. Penelitian ini mengimplementasikan kriptosistem hybrid yang mengombinasikan AES-256 untuk enkripsi pesan dan RSA-2048 untuk distribusi kunci pada fitur pesan aplikasi web Team Sync. Mekanisme end-to-end encryption diterapkan di sisi klien menggunakan pustaka kriptografi berbasis JavaScript guna memastikan server tidak dapat mengakses isi pesan. Evaluasi meliputi pengujian enkripsi–dekripsi, analisis keamanan kunci, serta uji fidelity pesan. Hasil pengujian menunjukkan bahwa proses enkripsi dan dekripsi berjalan akurat tanpa kehilangan data serta mampu mendukung komunikasi real-time secara efisien. Dengan demikian, kombinasi RSA dan AES terbukti efektif dalam meningkatkan kerahasiaan, integritas, dan privasi pesan pada aplikasi Team Sync.

Kata Kunci: RSA-2048, AES-256, Kriptosistem Hybrid, End-to-End Encryption, Keamanan Chat,Team Sync

1. PENDAHULUAN

Kemajuan teknologi informasi, khususnya pada bidang jaringan komunikasi dan internet telah membawa perubahan besar pada kehidupan sehari-hari. Penyebaran data dan informasi menjadi lebih mudah karena adanya telah menjadikan internet sebagai sarana utama untuk distribusi dan pertukaran data. Dalam proses pertukaran tersebut, aspek kerahasiaan dan integritas data yang dikirim menjadi faktor

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 1, Januari 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

penting dalam sistem keamanan yang harus diperhatikan. Setiap data yang dikirim berpotensi mengalami serangan, yang dapat menyebabkan hilangnya integritas data tersebut. [1].

Dalam penggunaan aplikasi percakapan daring atau chatting, keamanan menjadi aspek yang sangat krusial karena banyaknya data pribadi dan sensitif yang dikirim melalui platform tersebut. Pengguna kerap membagikan informasi penting seperti identitas, lokasi, nomor telepon, hingga data finansial. Berbagai ancaman dapat muncul, seperti peretasan yang berpotensi menimbulkan pencurian data, penyalahgunaan informasi oleh pihak yang tidak bertanggung jawab, serta kejahatan siber seperti penipuan identitas dan pencucian uang. Selain itu, kebocoran data juga bisa disebabkan oleh adanya celah dalam sistem keamanan aplikasi maupun server penyimpanan. Oleh karena itu, perlindungan data menjadi elemen utama dalam penggunaan aplikasi chatting, terutama di era digital ketika isu privasi dan keamanan informasi semakin menjadi perhatian besar bagi para pengguna.[2].

Dalam penelitian [3] yang berjudul Implementasi Algoritma Md5 Untuk Keamanan Login Website Dijelaskan bahwa diperlukan mekanisme keamanan pada proses login untuk mencegah kemungkinan serangan atau penyalahgunaan oleh pihak yang tidak berwenang. Untuk mencapai tujuan tersebut, peneliti menggunakan algoritma MD5 yang diintegrasikan ke dalam sistem login pada situs web. Dalam prosesnya, kata sandi pengguna terlebih dahulu diubah menjadi nilai hash MD5 sebelum disimpan di basis data. Saat pengguna melakukan login, kata sandi yang dimasukkan juga dikonversi menjadi hash dan kemudian dibandingkan dengan nilai hash yang sudah tersimpan di database. Penerapan skrip MD5 ini dilakukan menggunakan bahasa pemrograman PHP.

Hasil penelitian menunjukkan bahwa penggunaan algoritma MD5 cukup efektif dalam meningkatkan keamanan proses login dengan cara mengenkripsi kata sandi pengguna..sementara itu Dalam penelitian [4] yang berjudul *"Analisa dan Implementasi Keamanan Pesan Chatting Menggunakan Algoritma Challenge Response"*, dijelaskan bahwa kemajuan teknologi informasi berbasis komputer memberikan banyak keuntungan, terutama dalam meningkatkan efisiensi dengan mengurangi elemen yang tidak diperlukan. Namun, di balik manfaat tersebut, juga terdapat risiko kejahatan seperti pencurian data, penipuan, dan pemerasan. Contohnya, kebocoran informasi rahasia perusahaan kepada pihak pesaing dapat menimbulkan kerugian besar, seperti terbukanya data terkait produk yang sedang dikembangkan, algoritma yang digunakan, atau teknik dalam proses produksi. Oleh sebab itu, dibutuhkan sistem keamanan informasi yang mampu memberikan perlindungan dan batasan tertentu terhadap potensi ancaman tersebut**..**Dalam penelitian [5] berjudul *"Sistem Informasi Decrypt Respon Bridging BPJS Kesehatan dengan Algoritma AES-256"*, dijelaskan bahwa kebijakan *bridging* antara BPJS Kesehatan dengan rumah sakit telah berlangsung sejak lama berdasarkan perjanjian kerja sama yang disepakati. Sistem *bridging* ini terus mengalami perkembangan, dari versi 1 hingga versi 2 saat ini. Pada *bridging* versi 1, pertukaran data berlangsung lebih sederhana karena data yang dikirimkan belum melalui proses enkripsi. Namun, demi meningkatkan keamanan, pada *bridging* versi 2 seluruh data yang dipertukarkan untuk setiap layanan rumah sakit sudah dienkripsi dalam bentuk bahasa mesin sehingga tidak dapat dibaca secara langsung. Kondisi ini menjadi tantangan bagi pihak rumah sakit karena mereka harus melakukan dekripsi agar data kembali ke bentuk normal yang dapat dipahami seperti sebelumnya.

Adapun Penelitian ini berfokus pada peningkatan keamanan aplikasi SMS pengaduan kecurangan Pemilu yang berfungsi sebagai sarana bagi masyarakat untuk melaporkan berbagai bentuk pelanggaran kepada KPU secara aman. Dalam penelitian tersebut digunakan metode algoritma RSA untuk melindungi data. Hasilnya menunjukkan bahwa aplikasi mampu melakukan proses enkripsi atau pengacakan pesan dengan baik, dengan nilai avalanche effect sebesar 10,44%. Uji brute force pada panjang kunci 16-bit memerlukan waktu sekitar 3,7 milidetik untuk setiap percobaan dalam menemukan 32.768 kemungkinan kunci privat. [6].

Dengan demikian,tujuan dari penelitian ini adalah menerapkan kombinasi algoritma AES dan RSA sebagai kriptosistem hybrid pada fitur pengiriman pesan aplikasi Team Sync, mengimplementasikan mekanisme end-to-end encryption di sisi klien, serta mengevaluasi efektivitasnya dalam menjaga kerahasiaan, integritas, dan privasi pesan pada komunikasi real-time.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 1, Januari 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

2. TINJAUAN PUSTAKA

2.1 Kriptografi

Menurut bahasa Kriptografi memiliki asal kata dari *crypto* yang artinya rahasia dan g*raphy* yang artinya tulisan. Kriptografi dapat diartikan menjadi tulisan rahasia, secara istilah dapat diartikan menjadi suatu teknik matematika yang terkait dengan keamanan [7]. Teknik kriptografi terbagi dari simetri dan asimetri, metode ini digunakan untuk mengamankan informasi sehingga dapat menjaga kerahasiaan, integritas, autentikasi data dan non-repudiation.

Kriptografi dibutuhkan karena informasi sangat penting untuk segala aspek karena kebutuhan keamananan informasi berubah dari masa ke masa. Perubahan kebutuhan ini ada karena transformasi atau pemakaian perlengkapan kebutuhan primer menjadi pertukaran data, dari mulai cara tradisional yang membutuhkan mekanisme penyimpanan atau administrasi secara lengkap dan membutuhkan ruang yang besar, memakai otomatisasi komputer personal, sampai transfer informasi lewat penggunaan jaringan, baik intranet atau internet yang sekarang menjadi keperluan [8].

2.2 Tujuan Kriptgrafi

Ada empat tujuan mendasar dari ilmu kriptografi yang juga merupakan aspek keamanan informasi yaitu [9]:

1. Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data adalah berrhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak- pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Autentifikasi adalah berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, dan waktu pengiriman.
4. Penyangkalan (non-repudiation) adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh orang yang mengirimkan atau membuatnya.

2.3 Proses Enkripsi dan Dekripsi

Terdapat beberapa cara untuk melakukan enkripsi dan dekripsi, yaitu [10]:

A.Proses Enkripsi

1. Enkripsi dengan kunci simetris, menggunakan satu kunci rahasia yang sama (private key) untuk melakukan proses enkripsi dan dekripsi. Kunci ini dibuat oleh pihak pengirim data, kemudian dikirimkan kepada penerima agar dapat digunakan untuk membuka hasil enkripsi. Keunggulan metode ini terletak pada kecepatan pemrosesan data, sehingga sangat efektif diterapkan dalam pengamanan data berkecepatan tinggi.
2. Enkripsi dengan kunci asimetris, memanfaatkan dua kunci yang berbeda, yaitu satu kunci untuk proses enkripsi dan satu lagi untuk dekripsi. Kunci enkripsi bersifat terbuka (public key), sedangkan kunci dekripsi bersifat rahasia (private key). Kelebihan metode ini adalah tidak memerlukan saluran khusus untuk pertukaran kunci serta memiliki jumlah kunci yang lebih efisien dibandingkan dengan enkripsi simetris. Namun, kekurangannya terletak pada kecepatan enkripsi dan dekripsi yang lebih lambat.
3. Enkripsi menggunakan fungsi Hash (satu arah), yang juga dikenal sebagai fungsi hash kriptografis, adalah metode efisien untuk mengubah string input dengan panjang bervariasi menjadi output dengan panjang tetap yang disebut nilai hash. Fungsi ini bersifat satu arah, sehingga data yang sudah diubah tidak dapat dikembalikan ke bentuk aslinya. Contohnya adalah penggunaan MD5 untuk mengamankan kata sandi (password).

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 1, Januari 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

B. Proses Dekripsi

Proses dekripsi adalah kebalikan dari enkripsi, di mana ciphertext diubah kembali menjadi plaintext. Proses ini memerlukan kunci privat yang sesuai dengan yang digunakan saat enkripsi.

1. Metode Algoritma AES (Advanced Encryption Standard)

AES (Advanced Encryption Standard) adalah algoritma kriptografi yang digunakan untuk melindungi data. AES merupakan algoritma cipher blok simetris yang mampu melakukan enkripsi (mengubah data menjadi bentuk yang tidak bisa dibaca atau cipher text) dan dekripsi (mengembalikan cipher text ke bentuk asli atau plain text). Algoritma ini menggunakan kunci kriptografi dengan panjang 128, 192, atau 256 bit untuk proses enkripsi dan dekripsi pada blok data sebesar 128 bit.

2.Rivest-Shamir-Adleman (RSA)

RSA merupakan salah satu algoritma enkripsi yang paling sering menimbulkan perdebatan, bersama dengan DES (Data Encryption Standard). Hingga saat ini, belum ada yang berhasil membobol keamanan DES maupun RSA, namun belum ada pula bukti ilmiah yang meyakinkan mengenai keamanan kedua metode enkripsi tersebut. Untuk mengenkripsi informasi maupun mendekripsi pesan yang sudah terenkripsi, sebuah algoritma memerlukan data biner yang disebut kunci [11].

RSA termasuk algoritma asimetris yang berarti memiliki sepasang kunci, yaitu kunci publik dan kunci privat. Dalam RSA hanya digunakan satu algoritma untuk melakukan enkripsi dan deskripsi. Peberdaannya hanya terletak pada eksponen yang digunakan. Kunci public (n, e) sebagai kunci enkripsi dan kunci privat (n, d) sebagai kunci deskripsi dimana d, e dan n adalah bilangan bulat positif [12]

2.4 Keamanan

Masalah keamanan adalah salah satu elemen paling penting dalam sebuah website. Keamanan jaringan terdiri dari serangkaian perangkat yang dibuat untuk menjaga data selama proses transmisi agar terhindar dari akses, perubahan, dan gangguan oleh pihak yang tidak berwenang. Dalam hal ini, penting untuk memahami bahwa keamanan jaringan melibatkan berbagai teknik dan teknologi yang bertujuan melindungi integritas, kerahasiaan, dan ketersediaan data. Upaya ini meliputi penggunaan firewall, sistem deteksi intrusi, serta enkripsi data untuk mencegah akses ilegal dan memastikan data yang dikirim tetap aman dari modifikasi maupun pencurian. [13].

2.5 flowchart

Flowchart adalah istilah lain dari diagram alur. Di mana, diagram tersebut berisikan langkah atau proses untuk mengoperasikan sebuah program. Umumnya, langkah-langkah atau proses yang terjadi akan dituliskan dalam diagram alur dengan garis atau anak panah sebagai penghubung dari tiap langkahnya [14]. Flowchart digunakan untuk memodelkan alur proses sistem agar lebih mudah dianalisis dan divisualisasikan. Dalam penelitian ini, flowchart tidak hanya berfungsi sebagai representasi prosedural, tetapi juga menggambarkan tahapan kriptografi seperti pembangkitan kunci, enkripsi pesan, pengiriman melalui server, serta proses dekripsi di sisi penerima. Dengan demikian, flowchart membantu memperjelas hubungan antara teori kriptografi dengan implementasi program[15].

2.6 Web

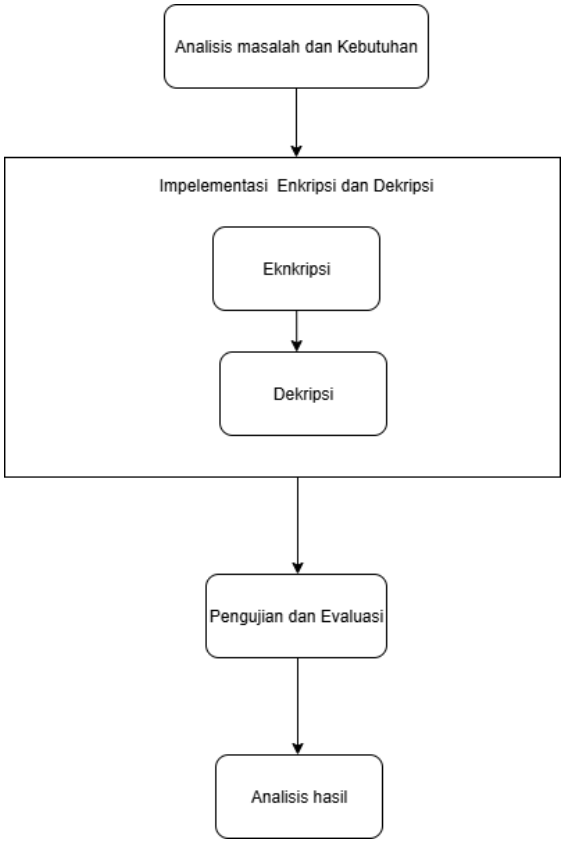
Web adalah istilah umum untuk World Wide Web. Web merupakan bagian dari Internet yang terdiri dari halaman-halaman yang bisa diakses melalui browser Web. Walaupun Web merupakan komponen terbesar dari internet, keduanya tetap berbeda satu sama lain. [16]. Web hanya menyediakan layanan berbasis HTTP dan dijalankan melalui browser. Dalam konteks penelitian ini, implementasi E2EE dilakukan pada aplikasi web real-time yang berjalan menggunakan JavaScript di sisi klien [17].

3. METODOLOGI PENELITIAN

3.1. Tahapan Penelitian

Penelitian menggunakan metodologi eksperimen terapan. Tahapan yang ada dalam penelitian dapat ditemukan pada gambar berikut ini :

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 1, Januari 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi



Gambar 1. Alur Penelitian

3.2 Analisis Masalah dan Kebutuhan

Tahap awal penelitian ini fokus pada identifikasi masalah keamanan pesan pada aplikasi web chat, terutama pada Team Sync.

Pada tahap ini, dilakukan analisis kebutuhan fungsional, termasuk proses enkripsi dan dekripsi pesan, serta kebutuhan non-fungsional seperti performa sistem dan kemudahan pemakaian. Selain itu, ditentukan bahwa sistem akan menggunakan kombinasi algoritma RSA dan AES sebagai metode utama untuk menjaga keamanan data

3.3 Enkripsi

Pada tahap ini peneliti menggunakan Enkripsi untuk Mengubah pesan asli menjadi bentuk terenkripsi agar aman.Proses Enkripsi menggunakan AES yang merupakan standar algoritma kriptografi modern yang dikembangkan oleh NIST sebagai pengganti DES. Algoritma ini mendukung panjang kunci 128, 192, dan 256 bit, di mana variasi panjang kunci menentukan jumlah putaran yang dijalankan pada proses enkripsi dan dekripsi**.**

3.4.Dekripsi

Pada tahap ini peneliti Mengembalikan pesan terenkripsi menjadi pesan asli agar bisa dibaca kembali. Pada sisi penerima, kunci AES terlebih dahulu didekripsi menggunakan private key RSA sebagai pasangan dari public key pengirim. Setelah kunci AES diperoleh, ciphertext diproses melalui dekripsi AES untuk mengembalikan pesan ke bentuk plaintext yang dapat dibaca.

3.5 Pengujian dan Evaluasi

Pengujian dilakukan untuk memastikan bahwa sistem yang dikembangkan dapat beroperasi secara maksimal, baik dari sudut pandang kinerja maupun keamanan. Berikut adalah beberapa metode pengujian yang digunakan

1. Uji kompleksitas kunci Pengujian ini mengevaluasi tingkat kesulitan pemecahan kunci enkripsi. Kompleksitas kunci yang tinggi menunjukkan bahwa mekanisme keamanan mampu menahan serangan brute force dan kriptanalisis.
2. Uji Fidelity digunakan Uji fidelity digunakan untuk menilai kesesuaian antara plaintext dan hasil dekripsi. Nilai fidelity yang tinggi mengindikasikan bahwa rekonstruksi pesan berlangsung akurat dan integritas data terjaga.
3. Evaluasi Performa Menggunakan MSE dan PSNR

- **MSE** mengukur tingkat perbedaan antara data asli dan data hasil dekripsi; nilai rendah menunjukkan kesalahan minimal.
- **PSNR** menilai kualitas sinyal setelah proses enkripsi–dekripsi; nilai tinggi menandakan kualitas rekonstruksi yang baik dan minim noise.

3.6 Analisis Hasil

Tahapan akhir dilakukan dengan menganalisis hasil pengujian guna menilai efektivitas dan efisiensi sistem yang telah dibangun. Proses analisis ini mencakup evaluasi terhadap tingkat keamanan serta kinerja algoritma hybrid RSA–AES, sekaligus memberikan rekomendasi perbaikan yang dapat digunakan untuk pengembangan sistem di masa depan.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 1, Januari 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

4 HASIL DAN PEMBAHASAN

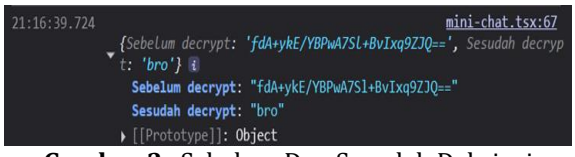
Implementasi algoritma AES-256 dan RSA-2048 dilakukan dengan integrasi pustaka crypto JavaScript pada sisi klien. Pengujian menghasilkan:

Tidak ditemukan kehilangan data atau ketidak cocokan antara pesan asli dan pesan hasil dekripsi.

Berikut log sebelum enkripsi pesan dan kirim pesan:

Gambar 2. Sebelum Dan Sesudah Enkripsi

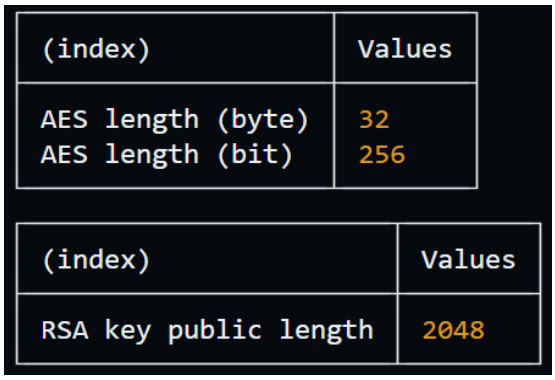
Gambar 2 diatas akan memperlihatkan hasil dari proses sebelum dan sesudah enkripsi pesan. Sebelum dienkripsi, isi dari pesan tersebut akan terlihat jelas dalam bentuk teks biasa, yaitu 'bro!'. Setelah proses enkripsi dijalankan, pesan yang sama berubah menjadi rangkaian karakter acak panjang seperti ***'fdA+ykE/YBPwA7Sl+BvIxq9ZJQ=='***. Perubahan nantinya akan menunjukkan bahwa pesan asli yang mudah dibaca oleh user berhasil disamarkan menjadi kode acak,yang nantinya tidak akan bisa dipahami tanpa kunci dekripsi. Dengan demikian, pesan yang dikirim menjadi lebih terlindungi karena hanya penerima yang memiliki kunci yang tepat dapat mengakses isi pesan tersebut.



Gambar 3. Sebelum Dan Sesudah Dekripsi

Gambar 3 menunjukkan hasil uji dekripsi pesan. Sebelum proses dekripsi, pesan akan masih berupa rangkaian karakter acak seperti "fdA+yKE/YBPwA7SL+BvIxq9ZJQ==", yaitu ciphertext yang tidak bisa dipahami oleh user. Setelah dilakukan dekripsi dengan kunci yang sudah sesuai,maka ciphertext tersebut berhasil dikembalikan menjadi teks aslinya, yaitu 'bro!'.

Uji Kompleksitas Kunci



(index)	Values
AES length (byte)	32
AES length (bit)	256

(index)	Values
RSA key public length	2048

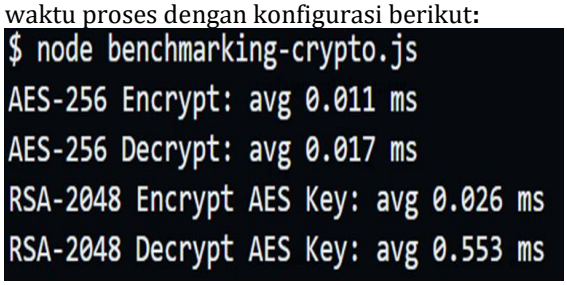
Gambar 4. Panjang AES dan RSA

Pada gambar 4 menunjukan tentang Kombinasi antara RSA-2048 dan AES-256 ini merupakan standar industri dalam skema enkripsi hybrid karena menggabungkan:

Kecepatan dan efisiensi dari enkripsi simetris (AES)

dengan keamanan distribusi kunci dari enkripsi asimetris (RSA).

Berikut benchmark pengujian yang dilakukan untuk mengukur Performa enkripsi dan dekripsi, dilakukan pengujian terhadap waktu proses dengan konfigurasi berikut:



Gambar 5. Hasil Uji Performa Enkripsi Dan Dekripsi AES dan RSA

Gambar 5 diatas menunjukkan hasil pengujian kecepatan enkripsi dan dekripsi menggunakan dua algoritma, yaitu AES-256 dan RSA-2048. Untuk AES-256, proses enkripsi rata-rata hanya membutuhkan waktu sekitar 0,011 milidetik, sementara proses dekripsinya sedikit lebih lama, yaitu 0,017 milidetik. Ini menandakan bahwa AES bekerja sangat cepat baik untuk mengenkripsi maupun membuka pesan.

Sementara itu, pada RSA-2048, yang digunakan untuk mengamankan kunci AES, proses enkripsi kunci rata-rata memakan waktu 0,026 milidetik, sedangkan proses dekripsinya jauh lebih lama, yaitu sekitar 0,553 milidetik. Hal ini wajar karena RSA adalah algoritma asimetris yang memang lebih berat secara komputasi dibandingkan AES. ini sejalan dengan penelitian

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 1, Januari 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

sebelumnya oleh Hermawan [6],yang juga menekanakan bahwa system yang dikembangkan dapat mengetahui proses yang benar dan salah sehingga nantinya akan mengeluarkan hasil yang diinginkan,sehingga perlu adanya hasil pengujian terhadap pembangkit kunci.

Tabel 1. Hasil Uji Performa Enkripsi Dan Dekripsi AES dan RSA

Algoritma	**Operasi**	**Rata rata waktu eksekusi**
AES-256	Enkripsi payload	0.011ms
AES-256	Dekripsi payload	0.017ms
RSA-2048	Enkripsi kunci AES	0.026ms
RSA-2048	Dekripsi kunci AES	0.553ms

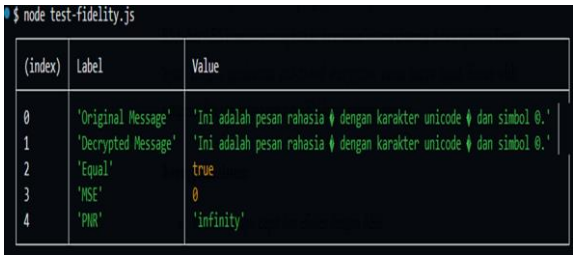
Pada tabel 1 diatas peneliti melakukan Pengujian,yang dimana dengan dilakukan sebanyak 1000 iterasi dengan menggunakan spesifikasi sistem seperti berikut:

a. CPU: Ryzen 5 4600G
b. RAM: 16 GB
c. Node.js v22.17.0
d. Library: *crypto native Node.js*

Hasil pengujian menunjukkan bahwa:

a. AES-256 sangat efisien untuk enkripsi data besar secara real-time.
b. RSA-2048 cukup cepat untuk digunakan dalam proses enkripsi satu arah terhadap kunci AES, karena proses ini hanya dilakukan sekali per sesi/pesan.

Uji Fidelity dan Konsistensi



Gambar 6. Hasil Uji Fidelity Dan Konsistensi AES dan RSA

Gambar 6 ini menunjukan hasil dari pengujian *fidelity* untuk memastikan apakah pesan setelah dienkripsi dan didekripsi kembali sama persis dengan pesan aslinya. Pada gambar diatas terlihat bahwa Original Message berisi teks *"Ini adalah pesan rahasia dengan karakter unicode dan simbol ©."* dan Decrypted Message menampilkan isi yang sama persis.

Kolom Equal bernilai true, yang berarti tidak terdapat perbedaan antara pesan asli dan hasil dekripsi. Nilai MSE (Mean Squared Error) tercatat 0, menunjukkan tidak ada kesalahan atau perbedaan data. Sementara itu, nilai PSNR (Peak Signal-to-Noise Ratio) tampil sebagai infinity, menandakan bahwa hasil dekripsi benar-benar sama persis dengan pesan asli tanpa adanya perubahan.

5 KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa penerapan algoritma AES-256 dan RSA-2048 pada aplikasi web chat Team Sync berhasil sesuai dengan desain awal dan mampu meningkatkan keamanan komunikasi secara signifikan. Enkripsi pesan yang menggunakan AES efektif dalam melindungi isi pesan, sementara kunci AES diamankan dengan RSA untuk memastikan distribusi kunci yang aman. Melalui konsep end-to-end encryption, hanya pengirim dan penerima yang dapat mengakses pesan tanpa intervensi dari server. Hasil pengujian membuktikan bahwa proses enkripsi dan dekripsi berjalan dengan tepat serta memiliki tingkat fidelity yang sangat baik. Uji kompleksitas kunci dan pengukuran performa dengan MSE dan PSNR juga menegaskan bahwa sistem ini menawarkan keamanan yang kuat dan efisiensi tinggi, sehingga cocok untuk komunikasi secara real-time.Berikut ada beberapa rekomendasi saran untuk pengembangan sistem dan penelitian selanjutnya adalah sebagai berikut:

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 1, Januari 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

1. Peningkatan manajemen kunci, misalnya dengan mengintegrasikan Key Management System (KMS) untuk penyimpanan kunci privat yang lebih aman.
2. Optimalisasi performa kriptografi dengan mempertimbangkan algoritma yang lebih ringan untuk perangkat dengan spesifikasi rendah.
3. Penambahan lapisan keamanan, seperti tanda tangan digital atau two-factor authentication (2FA) untuk memperkuat otentikasi pesan.
4. Pengujian pada lingkungan produksi atau skenario nyata guna mengevaluasi stabilitas, keamanan, dan skalabilitas sistem secara lebih komprehensif.

6 UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada universitas, dosen pembimbing, serta semua rekan yang telah memberikan dukungan, bimbingan, dan bantuan dalam pengumpulan data, sehingga penelitian ini dapat diselesaikan dengan sukses dan berjalan lancar.

DAFTAR PUSTAKA:

[1] A. Sebastian, "Implementasi dan Perbandingan Performa Algoritma Hash SHA-1, SHA-256, dan SHA-512," pp. 1–18, 2007, [Online]. Available: https://www.academia.edu/26267183/Fungsi_Hash_dan_Algoritma_SHA_256

[2] E. End-to-end and I. Juniarmi, "Analisis Keamanan Data pada Aplikasi Chatting Menggunakan," vol. 1, no. 2, pp. 30–38, 2024.

[3] F. M. Fauzi, U. K. Indonesia, I. Afrianto, and U. K. Indonesia, "Implementasi Algoritma Md5 Untuk Keamanan Login Website Implementasi Algoritma Md5 Untuk Keamanan," vol. d, no. August, pp. 1–5, 2023.

[4] M. F. Bahari, "Analisa Dan Implementasi Keamanan Pesan Chatting Menggunakan Algoritma Challenge Response," *Anal. Dan Implementasi Keamanan Pesan Chatting Menggunakan Algoritm. Chall. Response*, vol. 1, no. 2, pp. 49–53, 2022, doi: 10.47065/jussi.v1i2.1442.

[5] R. Saepul Rohman, D. A. Firmansah, and E. Ermawati, "Sistem Informasi Decrypt Respon Bridging Bpjs Kesehatan Dengan Algoritma Aes 256," *J. Responsif Ris. Sains dan Inform.*, vol. 4, no. 2, pp. 142–151, 2022, doi: 10.51977/jti.v4i2.761.

[6] A. Hermawan and H. I. E. Ujianto, "Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," *J. Nas. Inform. dan Teknol.*, vol. 5, no. 2, pp. 325–330, 2021.

[7] N. Oper, S. Balafif, and Z. To'o Fathonah Al-Khaliq, "MODIFIKASI ALGORITMA KRIPTOGAFI CAESAR CIPHER MENJADI ALGORITMA KRIPTOGRAFI ASIMETRIS DENGAN METODE AGILE," *J. Inform. Teknol. dan Sains*, vol. 4, no. 3, pp. 179–184, 2022.

[8] M. A. H. Septian Widiyanto, Govindo Adnan, Moh. Fatkuroji, Dwi Wahyu Handoyo, "Pengamanan Pesan Text dengan menggunakan Kriptografi Klasik Metode Shift Chipper dan Metode Substitution Chipper," *Riau J. Comput. Sci.*, vol. 7, no. 01, pp. 9–17, 2021.

[9] S. D. Nurcahya, "Implementasi Aplikasi Kriptografi Metode Kode Geser Berbasis Java," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 5, no. 4, pp. 694–697, 2022, doi: 10.32672/jnkti.v5i4.4690.

[10] A. Abiyuda and L. Nababan, "Jurnal InSeDS (Information System and Data Science) Rancang Bangun Aplikasi Chatting Dengan Wireless LAN Menggunakan Metode Beaufort Cipher," vol. 1, no. 2, 2023.

[11] W. Wahyudi, D. Hartama, I. O. Kirana, S. Sumarno, and I. Gunawan, "Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab. Simalungun," *J. Ilmu Komput. dan Inform.*, vol. 2, no. 1, pp. 57–66, 2022, doi: 10.54082/jiki.19.

[12] E. Ginting, P. Sahara, and S. N. Tambunan, "Ancaman Denial of Service Attack Dalam Eksploitasi Keamanan Sistem Informasi Threat of Denial of Service Attack in Information System Security Exploitation," *UNESJournal Inf. Syst.*, vol. 8, no. 1, pp. 9–9, 2023, [Online]. Available: https://fe.ekasakti.org/index.php/UJIS/article/view/26

[13] I. A. Darmawan, M. F. Randy, I. Yunianto, M. M. Mutoffar, and M. T. P. Salis, "Penerapan Data Mining Menggunakan Algoritma Apriori Untuk Menentukan Pola Golongan Penyandang Masalah Kesejahteraan Sosial," *Sebatik*, vol. 26, no.

Jurnal Manajemen Informatika & Sistem Informasi (MISI)
Volume 9, Nomor 1, Januari 2026.
ISSN 2614-1701 (media cetak)
ISSN 2614-3739 (media online)
DOI : 10.36595/misi.v5i2
http://e-journal.stmiklombok.ac.id/index.php/misi

1, pp. 223–230, 2022, doi: 10.46984/sebatik.v26i1.1622.

[14] B. SOETRISNO and M. M. ST, "Sistem Informasi Pembuatan Berita Acara Penggantian Bearing Pada PT. Spindo Tbk".

[15] K. I. Listyoningrum, D. Y. Fenida, and N. Hamidi, "Inovasi Berkelanjutan dalam Bisnis: Manfaatkan Flowchart untuk Mengoptimalkan Nilai Limbah Perusahaan Sustainable Innovation in Business: Leverage Flowcharts to Optimize the Value of Corporate Waste," vol. 1, no. 4, pp. 100–112, 2023.

[16] Y. Trimarsiah and M. Arafat, "Analisis dan Perancangan Website sebagai Sarana Informasi pada Lembaga Bahasa Kewirausahaan dan Komputer Akmi Baturaja," *J. Ilm. MATRIK*, vol. 19, no. 1, pp. 1–10, 2021.

[17] H. O. L. Wijaya, T. H. B. Aviani, A. Saputra, and Z. R. S. Elsi, "Penerapan Unified Modeling Language Pada Perancangan Sistem Informasi Kartu Kendali Berbasis Web," *Jusikom J. Sist. Komput. Musirawas*, vol. 5, no. 2, pp. 145–149, 2020.