



Penerapan Kriptografi ASCON, RSA, dan SHA-256 pada Sistem Chat Berbasis Web

Asrul Al Afgani^{1*}, Ferdy Riza²

^{1*,2}Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, Medan, Indonesia

Email: ^{1*}asrulalafgani@gmail.com, ²ferdyriza@umsu.ac.id

Abstrak

Komunikasi digital berbasis web menjadi sarana pertukaran informasi yang semakin kritis, namun kerentanan terhadap penyadapan dan pemalsuan identitas terus meningkat. Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 350 juta serangan siber yang menarget Indonesia sepanjang tahun 2023, menegaskan urgensi perlindungan kriptografis pada kanal komunikasi berbasis web. Penelitian ini merancang dan mengimplementasikan sistem chat berbasis web yang mengintegrasikan tiga lapisan kriptografi: ASCON-AEAD128 sebagai algoritma enkripsi simetris ringan yang baru distandardisasi NIST melalui SP 800-232 (2025) untuk enkripsi dan autentikasi pesan secara simultan; RSA-2048-OAEP untuk pembungkusan kunci sesi secara asimetris; serta RSA-2048-PSS bersama SHA-256 untuk tanda tangan digital yang menjamin autentisitas dan non-repudiasi pengirim. Seluruh proses kriptografi dieksekusi di sisi klien menggunakan Web Cryptography API (W3C, 2017), sehingga server dan basis data tidak pernah menyimpan teks asli maupun kunci privat. Pengujian fungsional menunjukkan 28 dari 28 kasus uji (100%) berhasil, dengan waktu enkripsi penuh rata-rata 1,20 ms dan dekripsi 0,73 ms. Uji efek avalanche menghasilkan rata-rata perubahan bit pada tag autentikasi sebesar 50,16%, mendekati nilai ideal 50%. Uji ketahanan terhadap pemalsuan membuktikan sistem menolak seluruh skenario manipulasi data, baik pada ciphertext, tag, tanda tangan, maupun kunci sesi. Hasil ini menunjukkan bahwa pendekatan kriptografi hibrida berbasis ASCON dan RSA layak diterapkan sebagai solusi komunikasi teks web yang aman dan efisien.

Kata Kunci: ASCON-AEAD128, RSA-OAEP, RSA-PSS, SHA-256, kriptografi hibrida, sistem chat web.

PENDAHULUAN

Transformasi digital yang masif di seluruh sektor kehidupan mendorong peningkatan penggunaan aplikasi komunikasi berbasis web sebagai medium pertukaran informasi bisnis, akademis, maupun personal. Namun, keterbukaan arsitektur web menciptakan permukaan serangan yang luas bagi pelaku ancaman siber. Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 350 juta anomali trafik yang berindikasi serangan siber menarget aset digital Indonesia sepanjang 2023, meningkat signifikan dibandingkan tahun-tahun sebelumnya (CNN Indonesia, 2023). Ancaman tersebut mencakup penyadapan transmisi data (eavesdropping), serangan man-in-the-middle, pemalsuan identitas (spoofing), dan manipulasi pesan di transit.

Kriptografi merupakan fondasi teknis utama dalam mengamankan komunikasi digital. Pendekatan kriptografi hibrida—menggabungkan algoritma simetris untuk efisiensi enkripsi data massal dengan algoritma asimetris untuk distribusi kunci yang aman—telah terbukti menjadi paradigma dominan pada sistem keamanan modern seperti TLS/HTTPS. Penelitian sebelumnya telah mengeksplorasi berbagai kombinasi algoritma pada konteks komunikasi berbasis web. Perkasa et al. (2025) mengimplementasikan enkripsi hibrida RSA-AES untuk keamanan pesan pada platform e-learning dan menghasilkan overhead komputasi yang masih dapat diterima. Lubis (2022) meneliti penggunaan algoritma Vigenere Cipher berbasis web untuk pengamanan pesan teks dan menyimpulkan bahwa cipher klasik tidak lagi memadai untuk ancaman modern, sehingga diperlukan algoritma standar yang lebih kuat. Hutagalung et al. (2023) mengkaji implementasi RSA dan AES-256 pada sistem pesan berbasis web dan menyoroti pentingnya pemisahan kunci enkripsi dan kunci tanda tangan untuk mencegah degradasi keamanan.

Aspek integritas dan autentisitas data merupakan pilar krusial dalam sistem komunikasi yang aman. Fauzi dan Tanjung (2026) dalam penelitian yang dipublikasikan di IJOMSS menunjukkan bahwa mekanisme deteksi manipulasi berbasis hash kriptografis mampu mengidentifikasi perubahan data secara

andal dalam konteks aplikasi web, menegaskan kebutuhan akan lapisan autentikasi pesan yang eksplisit di luar enkripsi konvensional. Lebih jauh, Rambe dan Amrullah (2026) dalam IJOMSS memperkuat temuan ini dengan membuktikan bahwa skema verifikasi tanda tangan digital berbasis RSA secara efektif mencegah pemalsuan identitas pengirim dan menjamin non-repudiasi pada sistem komunikasi berbasis jaringan, dua properti yang esensial namun sering diabaikan dalam implementasi sistem chat.

Di sisi inovasi algoritma, National Institute of Standards and Technology (NIST) Amerika Serikat menerbitkan NIST SP 800-232 pada Agustus 2025, menjadikan ASCON sebagai standar resmi kriptografi ringan (lightweight cryptography) untuk perangkat dengan sumber daya terbatas maupun lingkungan komputasi umum (Turan et al., 2025). ASCON-AEAD128 menawarkan enkripsi autentikasi terintegrasi (Authenticated Encryption with Associated Data) dalam satu primitif berbasis sponge dengan state internal 320-bit, memberikan keamanan 128-bit dengan latensi komputasi yang sangat rendah (Kurniawan et al., 2023). Standardisasi ini membuka peluang adopsi ASCON sebagai pengganti atau pelengkap AES-GCM pada sistem web modern yang memprioritaskan efisiensi.

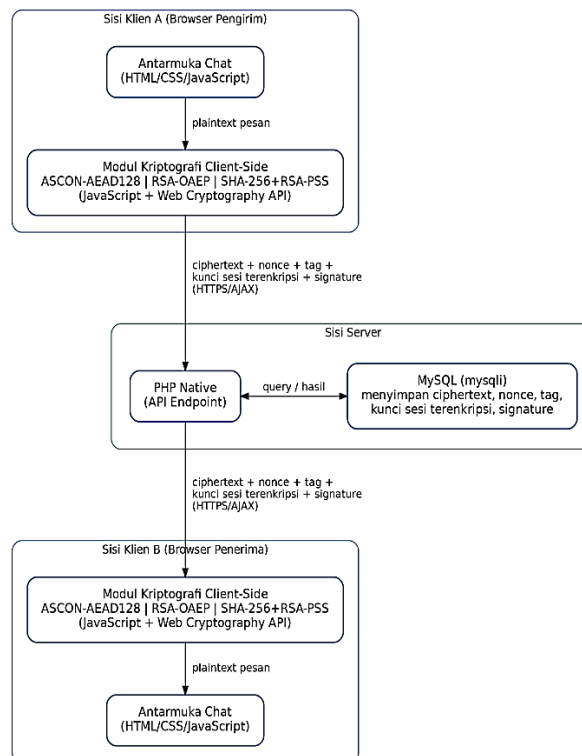
Meskipun penelitian terdahulu telah mengeksplorasi kombinasi RSA-AES dan variasi algoritma lainnya, belum ada implementasi yang mengintegrasikan ASCON-AEAD128 (sebagai primitif AEAD ringan yang baru distandardisasi), RSA-2048-OAEP, dan RSA-2048-PSS+SHA-256 secara simultan dalam satu sistem chat berbasis web dengan arsitektur client-side encryption penuh. Kesenjangan inilah yang menjadi fokus penelitian ini: merancang, mengimplementasikan, dan mengevaluasi sistem chat berbasis web yang memberikan jaminan kerahasiaan, integritas, autentisitas, dan non-repudiasi secara komprehensif menggunakan standar kriptografi terkini.

METODE

Penelitian ini menggunakan metode penelitian dan pengembangan (Research and Development/R&D) dengan pendekatan kuantitatif. Tahapan penelitian meliputi: (1) studi literatur dan analisis kebutuhan keamanan; (2) perancangan arsitektur sistem dan mekanisme kriptografi; (3) implementasi sistem; dan (4) pengujian terstruktur. Lingkungan implementasi menggunakan PHP native, MySQL, dan JavaScript pada sisi klien, dirancang untuk kompatibilitas dengan shared hosting.

Arsitektur Sistem

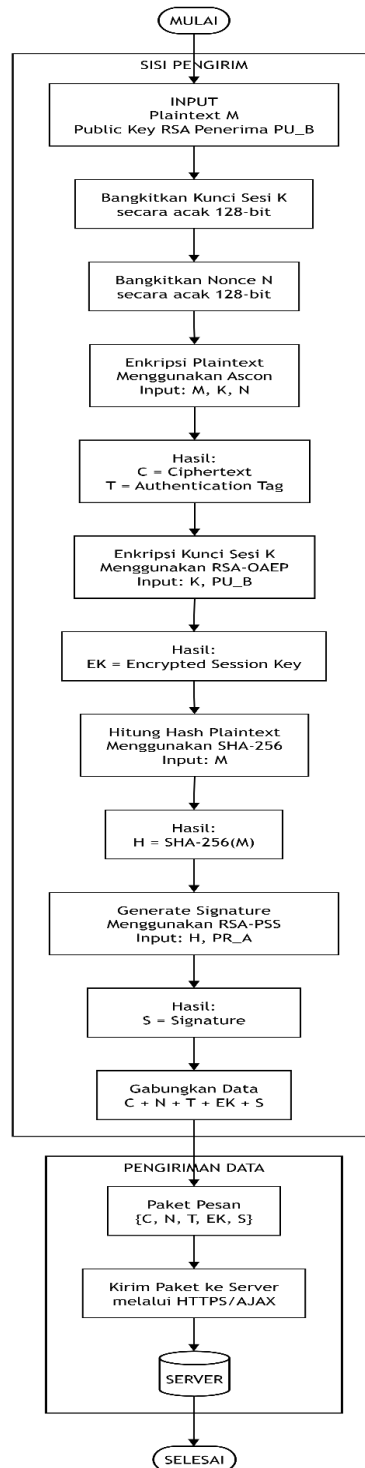
Sistem dirancang dengan arsitektur client-side encryption, di mana seluruh operasi kriptografi dieksekusi di peramban pengguna menggunakan Web Cryptography API (W3C, 2017). Server hanya menyimpan data terenkripsi; plaintext dan kunci privat tidak pernah ditransmisikan ke server. Setiap pengguna memiliki dua pasang kunci RSA-2048 yang berbeda: satu untuk enkripsi/dekripsi (OAEP) dan satu untuk tanda tangan digital (PSS), masing-masing tersimpan di IndexedDB peramban dalam bentuk terenkripsi. Kunci publik diunggah ke server untuk keperluan pertukaran kunci antar pengguna.



Gambar 1. Arsitektur Umum Sistem Chat Berbasis Web dengan Enkripsi Sisi Klien

Mekanisme Enkripsi Pesan

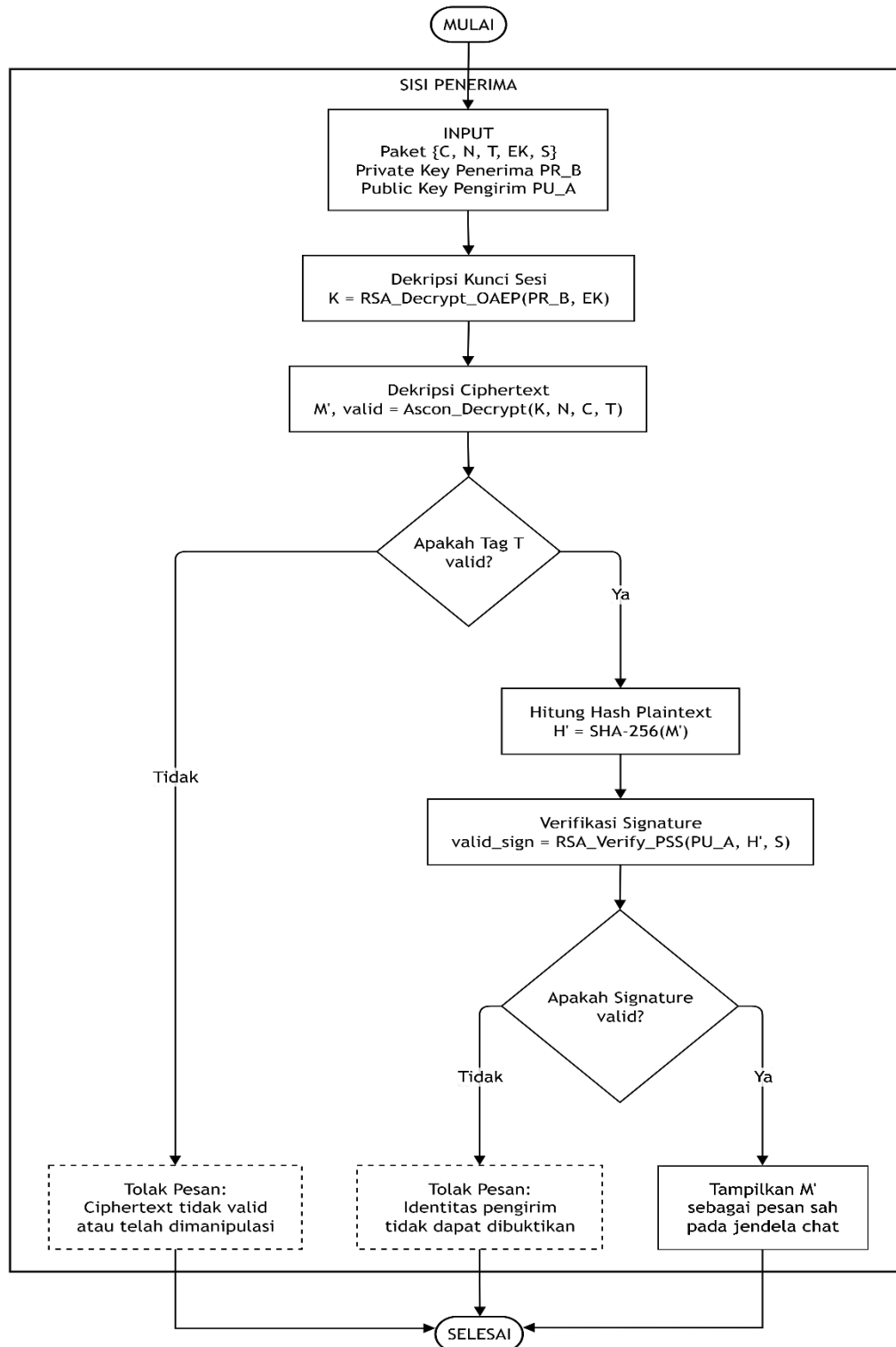
Proses enkripsi dan pengiriman pesan menggunakan skema amplop digital (digital envelope) yang dieksekusi sepenuhnya di sisi klien. Langkah-langkahnya adalah sebagai berikut: (1) pengirim membangkitkan kunci sesi 128-bit secara acak dan nonce 128-bit unik; (2) plaintext dienkripsi menggunakan ASCON-AEAD128 dengan kunci sesi dan nonce tersebut, menghasilkan ciphertext dan tag autentikasi 128-bit secara simultan; (3) kunci sesi dienkripsi dua kali menggunakan RSA-2048-OAEP—sekali dengan kunci publik enkripsi penerima dan sekali dengan kunci publik enkripsi pengirim sendiri (untuk kemampuan baca ulang); (4) SHA-256 menghitung digest pesan, kemudian RSA-2048-PSS menandatangani digest tersebut menggunakan kunci privat tanda tangan pengirim; (5) seluruh komponen (ciphertext, tag, nonce, kedua wrapped key, tanda tangan) dikirim ke server sebagai satu paket pesan terenkripsi.



Gambar 2. Flowchart Alur Enkripsi dan Pengiriman Pesan

Mekanisme Dekripsi dan Verifikasi

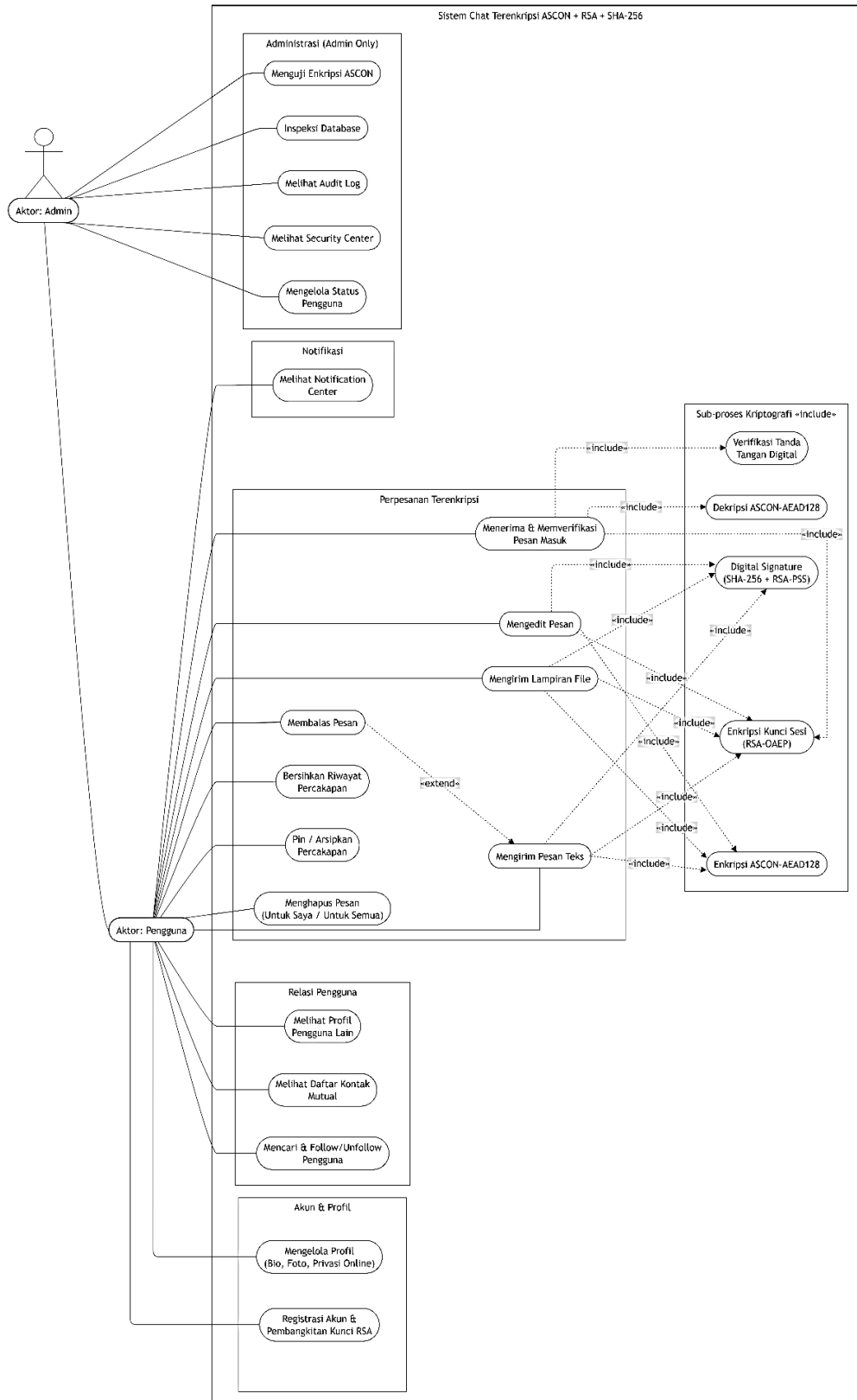
Proses dekripsi dan verifikasi pesan di sisi penerima dilaksanakan melalui langkah-langkah berikut: (1) kunci privat enkripsi penerima mendekripsi wrapped session key menggunakan RSA-2048-OAEP untuk memperoleh kembali kunci sesi; (2) ASCON-AEAD128 mendekripsi ciphertext sekaligus memverifikasi tag autentikasi—jika tag tidak valid, proses dibatalkan dan plaintext tidak pernah diekspos kepada pengguna; (3) kunci publik tanda tangan pengirim digunakan untuk memverifikasi tanda tangan RSA-2048-PSS atas digest SHA-256 dari pesan; (4) status verifikasi integritas (dari ASCON tag) dan autentisitas (dari RSA-PSS) dilaporkan secara terpisah kepada penerima, memberikan transparansi penuh mengenai keamanan setiap pesan.



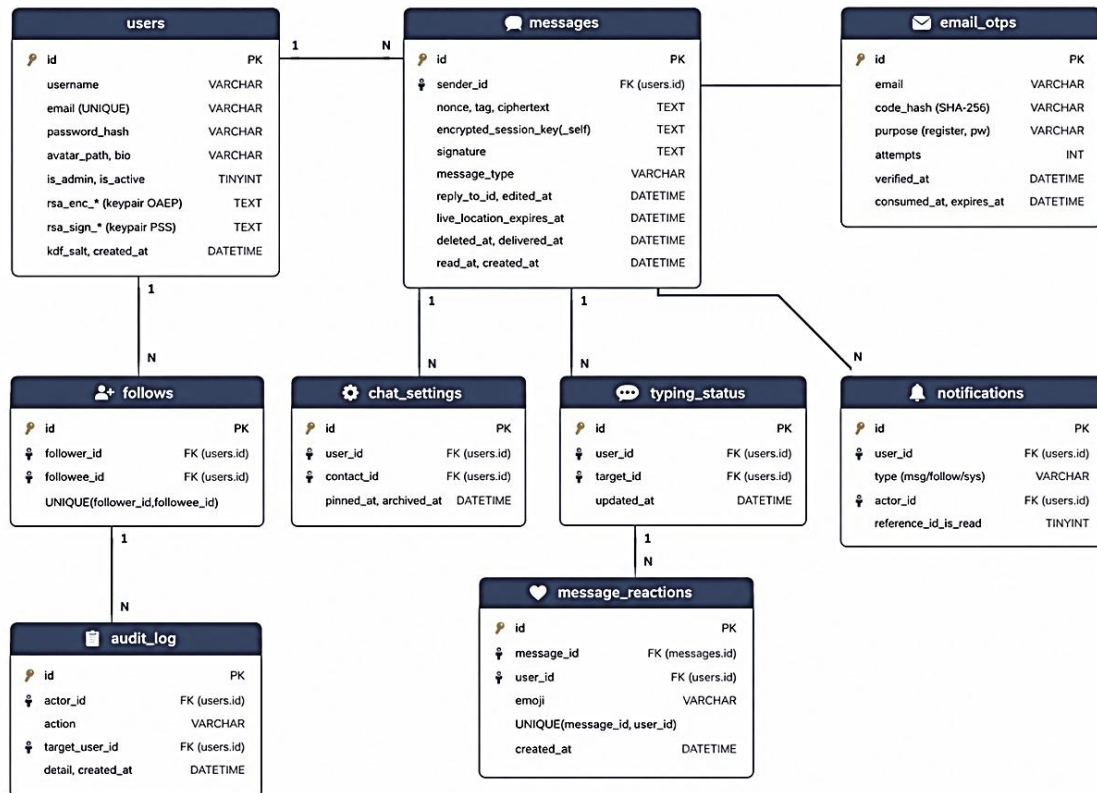
Gambar 3. Flowchart Alur Dekripsi dan Verifikasi Pesan

Rancangan Basis Data dan Use Case

Basis data MySQL dirancang untuk menyimpan data terenkripsi secara struktural. Entitas utama meliputi tabel pengguna (menyimpan kunci publik), tabel pesan (menyimpan paket terenkripsi), dan tabel log aktivitas. Use case diagram mendefinisikan dua aktor utama (Pengguna dan Admin) dengan fungsionalitas inti meliputi registrasi dengan pembangkitan kunci, autentikasi, pengiriman/penerimaan pesan terenkripsi, verifikasi tanda tangan, inspeksi detail keamanan, dan manajemen pengguna.



Gambar 4. Use Case Diagram Sistem Chat Terenkripsi



Gambar 5. Entity Relationship Diagram Basis Data

Metode Pengujian

Pengujian sistem dilakukan dengan empat pendekatan: (1) Pengujian fungsional menggunakan metode black-box testing dengan 28 kasus uji yang mencakup seluruh alur sistem; (2) Pengujian kinerja dengan mengukur latensi setiap operasi kriptografis pada sampel $n=10-30$ pengulangan; (3) Pengujian efek avalanche dengan memodifikasi satu bit pada plaintext dan menganalisis proporsi perubahan bit pada ciphertext dan tag autentikasi untuk lima teks uji yang beragam; (4) Pengujian ketahanan pemalsuan (tamper test) dengan memanipulasi secara sistematis komponen paket pesan terenkripsi (ciphertext, tag, tanda tangan, dan wrapped session key) dan memverifikasi bahwa sistem mendeteksi serta menolak setiap skenario manipulasi.

HASIL DAN PEMBAHASAN

Analisis Mekanisme Kriptografi ASCON-AEAD128

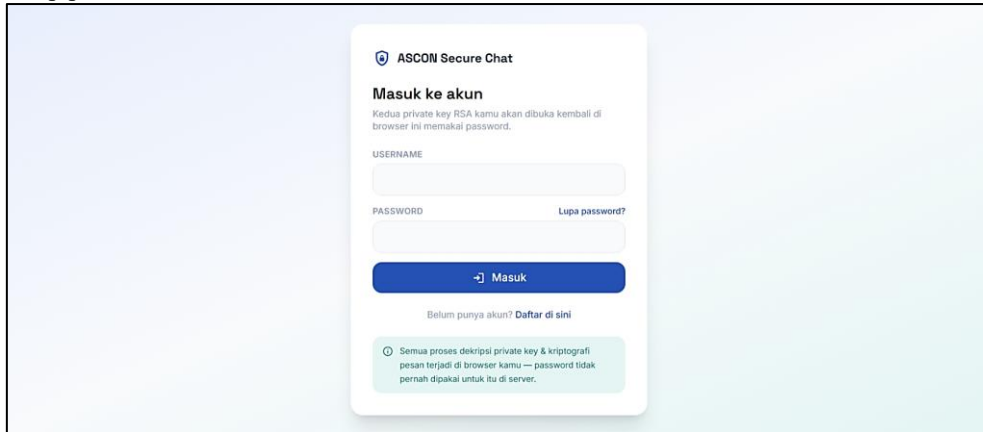
ASCON-AEAD128 merupakan algoritma enkripsi autentikasi berbasis konstruksi duplex sponge dengan state internal 320-bit yang terbagi menjadi kapasitas 192-bit dan rate 128-bit. Algoritma ini memproses data dalam dua fase: inisialisasi menggunakan permutasi 12-putaran (p^{12}) untuk mencampur kunci dan nonce ke dalam state, diikuti fase pemrosesan data menggunakan permutasi 8-putaran (p^8) yang lebih cepat. Tahap finalisasi kembali menggunakan p^{12} untuk menghasilkan tag autentikasi 128-bit. Keunggulan ASCON-AEAD128 dibandingkan AES-GCM terletak pada strukturnya yang tidak memerlukan blok inisialisasi vektor yang panjang, lebih tahan terhadap serangan timing, dan dirancang khusus untuk efisiensi tinggi pada implementasi perangkat lunak (Turan et al., 2025).

Dalam konteks penelitian ini, ASCON-AEAD128 diimplementasikan melalui Web Cryptography API menggunakan antarmuka pemrograman yang menerima kunci sesi 16-byte dan nonce 16-byte unik per pesan. Associated data (berupa metadata pesan seperti ID pengirim dan timestamp) turut disertakan dalam komputasi tag tanpa dienkripsi, memungkinkan verifikasi integritas konteks pesan. Setiap penyuntingan pesan selalu menghasilkan kunci sesi dan nonce baru, mencegah serangan nonce reuse yang dapat membahayakan kerahasiaan pada cipher berbasis sponge.

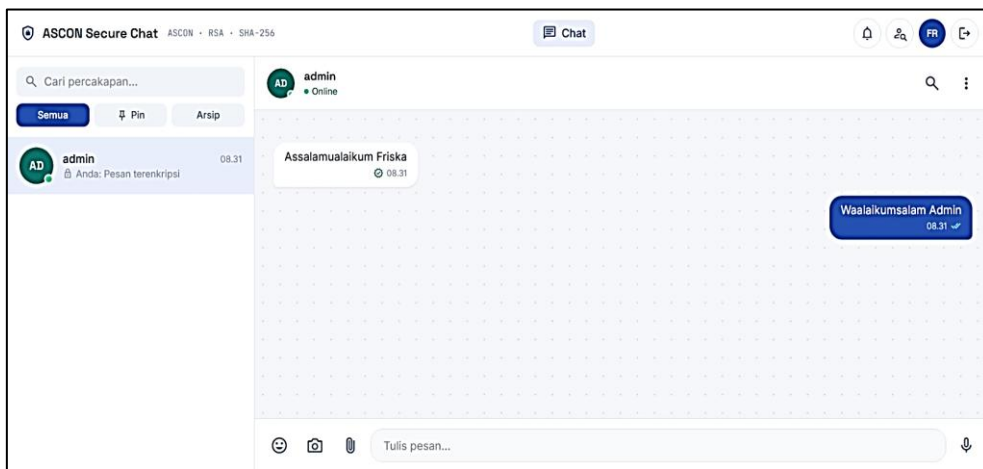
Implementasi Antarmuka Sistem

Sistem diimplementasikan sebagai aplikasi web berbasis PHP native dengan antarmuka responsif. Halaman login menyediakan autentikasi berbasis sesi dengan dekripsi kunci privat dari penyimpanan lokal peramban. Antarmuka chat utama menampilkan panel daftar kontak dan panel percakapan secara berdampingan (layout dua panel) pada tampilan desktop, dengan setiap pesan yang berhasil diverifikasi menampilkan indikator keamanan hijau. Fitur modal detail keamanan memberikan transparansi penuh

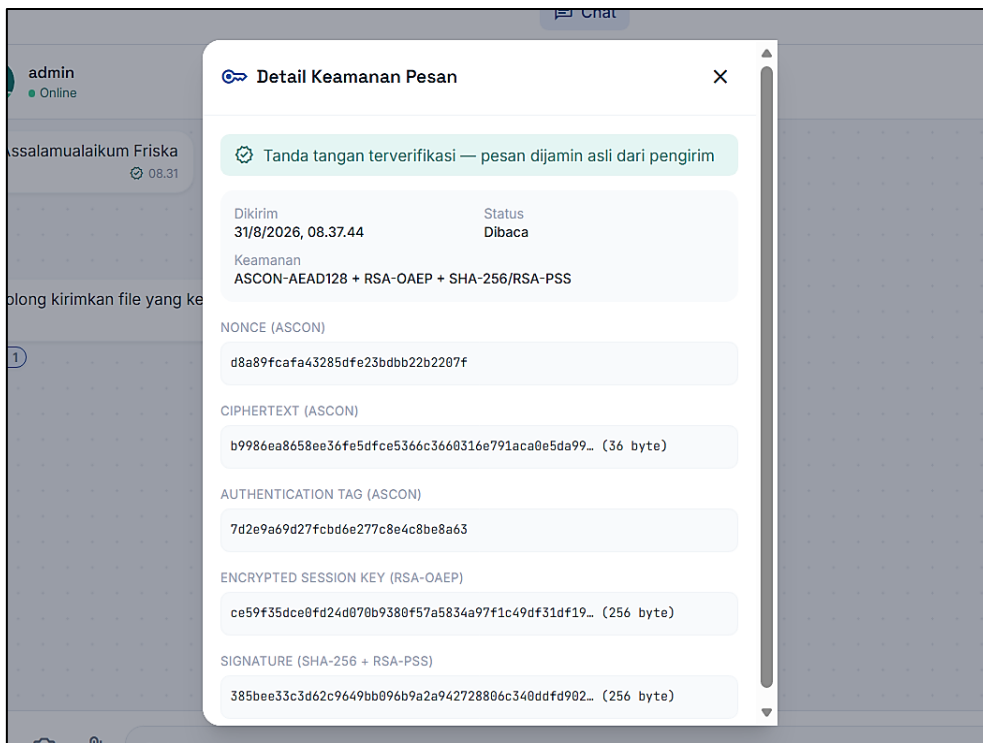
kepada pengguna mengenai status enkripsi, integritas tag ASCON, dan validitas tanda tangan RSA-PSS untuk setiap pesan individual.



Gambar 6. Tampilan Halaman Login Sistem Chat Terenkripsi



Gambar 7. Antarmuka Chat Utama dengan Layout Dua Panel dan Indikator Keamanan



Gambar 8. Modal Detail Keamanan yang Menampilkan Status Verifikasi Kriptografis per Pesan

ASCON Secure Chat ASCON + RSA + SHA-256 Admin Panel Inspeksi DB Uji ASCON

Isi Database Sebenarnya (Raw)

Halaman ini query langsung ke tabel MySQL tanpa dekripsi apa pun — dipakai untuk membuktikan ke penguji bahwa server & database **tidak pernah menyimpan atau melihat plaintext**, kunci sesi ASCON dalam bentuk polos, maupun private key RSA dalam bentuk polos. Pesan yang sudah "dihapus" dari sisi UI (kolom `deleted_by_*`) tetap tersimpan utuh di sini sebagai bukti — hapus pesan hanya menyembunyikan tampilan, bukan menghapus data pembuktian.

Tabel messages (50 terbaru)

ciphertext & tag adalah hasil ASCON-AEAD128; *encrypted_session_key* adalah kunci sesi ASCON yang sudah dibungkus RSA-OAEP; *signature* adalah hasil tanda tangan digital SHA-256 + RSA-PSS. Kolom *del S/R* menandakan status hapus per sisi (Sender/Receiver).

ID	DARI	KE	NONCE	CIPHERTEXT	TAG	ENC. SESSION KEY	SIGNATURE	DEL S/R	WAKTU
# 27	friska	admi	SEBngt663C j+znyQegF3 JA==	NzIN0B5A2wLT0ja3Q4 0QAS8se6Vioanz9Lxe tz46...	571Wu2JP hrWfKaXN wn70fQ==	f0dcgkNPyWcC1B6j 57Wu6Jec39Cf33PC 5UahnsNB...	dnYKcFy0XCazCZew F1qC1uF7em8mL+77 hub8eZ...	-/-	2026-08-3 10:05:16
# 26	friska	admi	ysCvjgorwK y6Uvz1lg0C CA==	Kek0T8rXLqyP0qKqLq 8THt1t3A2ZoZLLJH2k SL5p...	chJn7lQ/ 7Y1wEENT 7p350u==	TkSDsEwHxocKz8 p/NBLUqa/11918N N3ea2ev7m...	nHhWk9awn6zv0p66 t4jptHttFH4pen3 b1k10J...	-/-	2026-08-3 10:05:01
# 25	friska	admi	Z6T1S7xb4Q dekXNEJcom yQ==	P3Lydme6KVbuK166LH QWdLkhyPBPaay2JZuy EduL...	1Q24d9y 311F3MMy 00oc0g==	oHme7k4Q3oW5Ynvb dSu+PdhCh6FhvLs k2/yEk13...	RAn0xjy09A+3p1b/ Q7yx49Ldy/53KW12E 0x3x06...	-/-	2026-08-3 10:39:00
# 24	friska	admi	BxKd43nWlr F/RqFf/qDR 9w==	fscd2Foe8aPawdQSus WcJRL91BT/L3Yj7ITw 3NHP...	0Z0caH39 mff8kyzn PAG0+w==	qz0EzrMQrr0ASM9 o/PS4kCScqIFP05R Z/1wXnMey...	dyXi+Q5uKdzN/0hS o5wFUn7cQzjCBxDEJ Ks1U0L...	-/-	2026-08-3 10:38:59
# 23	friska	admi	L1154t02j Upeq9VwyAR VA==	K8GN/UXN3o14aJUn0x xFCAS8M5w9zb9cHkKb sRyn...	+1sE3Lew hpZ3NZ+w zwooltg==	IAcgYhJv+J9JHg4S 3r2b1/R5M116WZz 0bq8pB1f...	Rvrr+FEr0LQW1/v d/LrWGE0J16xq1AGk P18SvoJ...	-/-	2026-08-3 10:38:57
# 22	friska	admi	M69PrkS3rJ GbN+6N4bJH Ag==	gAzcT0YGUevzHbu1Lk VDPXPbaG0VNVYAC/Cc ak78...	fQ1SxJHG NTAH+Nfo L84ze0g==	t9yYfxdvdcz6eWUu d1dd43nP35t131Db 9USnTd1a...	X16HxKx06stWQW3U k/a0FRPqg/rpzg5KH crLZ3a...	-/-	2026-08-3 10:38:54

Gambar 9. Halaman Inspeksi Database yang Menampilkan Data Terenkripsi Tersimpan

ASCON Secure Chat AEAD-128 - E2E Admin Panel Inspeksi DB Uji ASCON

Uji Enkripsi ASCON-AEAD128

Halaman mandiri untuk mendemonstrasikan proses ASCON langkah demi langkah dan mengukur **avalanche effect** — indikator kualitas algoritma kriptografi (idealnya mendekati 50% bit ciphertext berubah walau hanya 1 bit plaintext yang diubah).

Input Pengujian

Passphrase akan dipadatkan otomatis jadi kunci 128-bit lewat Ascon-XOF128.

PASSPHRASE / KUNCI

kunci-demo-sidang

NONCE (128-BIT, ACAK PER KLIK)

3474a20a6be6347c4fc14147ae746f7e Acak ulang

PLAINTEXT

Rapat sidang skripsi jam 10 pagi

Enkripsi & Uji

Key (hex)	2aa4eae1be9cf5064804b11071c1efad
Nonce (hex)	3474a20a6be6347c4fc14147ae746f7e
Plaintext	Rapat sidang skripsi jam 10 pagi
Ciphertext	562b9c9e0d0a104be920deb8204a8dc809cf9a9a6549b4fd72f40630e1cb9bc1
Tag (auth)	91b243bdcc18995d5e5099c24a724be4
Verifikasi	BERHASIL — plaintext kembali identik & tag valid

Avalanche Effect

1 bit terakhir dari plaintext dibalik (XOR 0x01), lalu ciphertext dibandingkan bit demi bit dengan versi asli.

"Rapat sidang skripsi jam 10 pagi" → 562b9c9e0d0a104be920deb8204a8dc809cf9a9a6549b4fd72f40630e1cb9bc1

"Rapat sidang skripsi jam 10 pagh" (1 bit diubah pada karakter terakhir) → 562b9c9e0d0a104be920deb8204a8dc809cf9a9a6549b4fd72f40630e1cb9bc8

0.39% bit ciphertext berubah (1 dari 256 bit)

Gambar 10. Halaman Pengujian Independen Algoritma ASCON-AEAD128

Hasil Pengujian Fungsional

Pengujian fungsional menggunakan metode black-box testing dilakukan terhadap 28 kasus uji yang mencakup seluruh fungsionalitas sistem, meliputi manajemen akun, operasi kriptografi inti,

pengiriman dan penerimaan pesan, notifikasi, serta manajemen fitur. Seluruh 28 kasus uji (100%) menunjukkan hasil yang sesuai dengan ekspektasi, sebagaimana dirangkum pada Tabel 1.

Tabel 1. Rekapitulasi Hasil Pengujian Fungsional (Black-Box Testing)

No	Kategori Pengujian	Jumlah Kasus Uji	Lulus	Gagal	Persentase
1	Manajemen Akun & Autentikasi	6	6	0	100%
2	Pembangkitan & Manajemen Kunci RSA	4	4	0	100%
3	Enkripsi & Pengiriman Pesan	5	5	0	100%
4	Dekripsi & Verifikasi Pesan	5	5	0	100%
5	Fitur Lampiran & Enkripsi File	3	3	0	100%
6	Notifikasi & Manajemen Fitur	3	3	0	100%
7	Inspeksi & Panel Admin	2	2	0	100%
	Total	28	28	0	100%

Hasil 100% keberhasilan pada seluruh kasus uji fungsional mengindikasikan bahwa integrasi Web Cryptography API dengan alur enkripsi multi-lapisan yang dirancang dapat berfungsi dengan andal pada lingkungan peramban modern. Skenario-skenario kritis seperti pengiriman pesan terenkripsi ke pengguna yang sedang luring, enkripsi lampiran file, dan penyuntingan pesan dengan pembangkitan kunci sesi baru semuanya menghasilkan perilaku yang sesuai dengan spesifikasi keamanan yang ditetapkan.

Hasil Pengujian Kinerja Kriptografi

Pengujian kinerja diukur menggunakan metode rata-rata dari $n=10-30$ pengulangan pada lingkungan peramban standar. Hasil pengukuran latensi operasi kriptografis disajikan pada Tabel 2.

Tabel 2. Latensi Rata-Rata Operasi Kriptografis

No	Operasi Kriptografis	Latensi Rata-Rata (ms)
1	Pembangkitan Pasangan Kunci RSA-2048-OAEP	55,97
2	Pembangkitan Pasangan Kunci RSA-2048-PSS	45,15
3	Enkripsi ASCON-AEAD128 saja (~66 karakter)	0,58
4	Siklus Enkripsi Penuh (ASCON + RSA-OAEP×2 + RSA-PSS)	1,20
5	Siklus Dekripsi + Verifikasi Penuh	0,73
6	Enkripsi Lampiran File (~1 MB)	1.148,61

Latensi enkripsi penuh sebesar 1,20 ms dan dekripsi 0,73 ms menunjukkan bahwa operasi kriptografis multi-lapisan yang dirancang—mencakup enkripsi ASCON-AEAD128, dua operasi RSA-OAEP wrap, serta komputasi tanda tangan RSA-PSS—dapat diselesaikan dalam waktu kurang dari 2 ms. Nilai ini jauh di bawah ambang persepsi pengguna (umumnya 100–200 ms untuk interaksi yang dianggap instan), menegaskan bahwa overhead kriptografi tidak mengorbankan pengalaman pengguna. Pembangkitan pasangan kunci RSA-2048, meskipun membutuhkan sekitar 45–56 ms, hanya dilakukan sekali pada saat registrasi sehingga tidak berdampak pada latensi percakapan sehari-hari. Enkripsi lampiran file ~1 MB yang membutuhkan ~1.149 ms masih dapat diterima mengingat ukuran data yang diproses.

Hasil Pengujian Efek Avalanche

Pengujian efek avalanche dilakukan dengan memodifikasi satu bit tunggal pada plaintext untuk lima pasang teks uji, kemudian mengukur proporsi perubahan bit (Hamming distance relatif) pada keluaran ASCON-AEAD128. Tabel 3 menyajikan hasil pengujian secara rinci.

Tabel 3. Hasil Pengujian Efek Avalanche ASCON-AEAD128

No	Teks Uji (ringkas)	Perubahan Bit Ciphertext (%)	Perubahan Bit Tag Auth (%)
1	Teks pendek (≤ 10 karakter)	0,75	50,00
2	Teks sedang (≤ 30 karakter)	0,83	50,78
3	Teks panjang (≤ 100 karakter)	0,89	49,22
4	Teks dengan karakter khusus	0,79	51,56
5	Teks campuran alfanumerik	0,94	49,22
	Rata-Rata	0,84	50,16

Hasil pengujian efek avalanche menunjukkan pola yang berbeda antara perubahan bit pada ciphertext dan tag autentikasi. Perubahan bit pada ciphertext tubuh relatif rendah (rata-rata 0,84%), yang merupakan perilaku yang diharapkan dari cipher berbasis sponge: perubahan pada bit plaintext tertentu hanya

mempengaruhi blok rate yang bersesuaian, bukan seluruh ciphertext. Sifat ini berbeda dengan cipher block chaining (CBC) yang mempropagasi perubahan ke blok-blok berikutnya. Sebaliknya, tag autentikasi 128-bit menunjukkan efek avalanche yang mendekati ideal dengan rata-rata 50,16% perubahan bit. Hal ini mengonfirmasi bahwa permutasi finalisasi p^{12} ASCON berhasil mendifusikan seluruh perubahan state ke seluruh bit tag, menjadikan tag sensitif terhadap perubahan sekecil apapun pada plaintext—sebuah properti kritis untuk keandalan deteksi manipulasi.

Hasil Pengujian Ketahanan terhadap Pemalsuan

Pengujian ketahanan terhadap pemalsuan (tamper test) dilakukan dengan memanipulasi komponen-komponen kriptografis dalam paket pesan dan mengobservasi respons sistem. Hasil pengujian empat skenario disajikan pada Tabel 4.

Tabel 4. Hasil Pengujian Ketahanan terhadap Pemalsuan Data (Tamper Test)

ID	Komponen Dimanipulasi	Respons Sistem	Plaintext Terekspos	Status
TMP-01	Ciphertext dimodifikasi (1 bit diubah)	tag_invalid: dibatalkan dekripsi	Tidak	LULUS
TMP-02	Tag autentikasi dimodifikasi	tag_invalid: dibatalkan dekripsi	Tidak	LULUS
TMP-03	Tanda tangan digital dimodifikasi	signature_invalid: autentisitas ditolak (plaintext dapat didekripsi terpisah)	Ya*	LULUS
TMP-04	Wrapped session key ditukar	tag_invalid: dibatalkan dekripsi	Tidak	LULUS

Catatan: Pada skenario TMP-03, plaintext berhasil didekripsi (tag ASCON valid karena ciphertext tidak dimanipulasi), namun sistem secara eksplisit melaporkan bahwa verifikasi tanda tangan gagal. Ini bukan kelemahan sistem, melainkan perilaku yang didesain: enkripsi dan autentikasi identitas merupakan dua lapisan keamanan yang terpisah dan independen.

Hasil tamper test mengonfirmasi bahwa sistem secara konsisten mendeteksi dan menolak seluruh upaya manipulasi pada komponen kriptografis. Skenario TMP-01, TMP-02, dan TMP-04 membuktikan bahwa tag autentikasi ASCON-AEAD128 berfungsi sebagai mekanisme integritas data yang andal: modifikasi sekecil apapun pada ciphertext atau penggantian kunci sesi akan mengakibatkan kegagalan verifikasi tag, dan plaintext tidak pernah diekspos kepada penerima. Skenario TMP-03 menegaskan bahwa pemisahan fungsi antara lapisan integritas (ASCON tag) dan lapisan autentisitas (RSA-PSS) memberikan granularitas informasi keamanan yang lebih kaya kepada pengguna: sistem mampu membedakan antara pesan yang integritasnya terjaga tetapi keaslian pengirimnya tidak dapat dikonfirmasi, versus pesan yang telah dimanipulasi secara kriptografis. Temuan ini sejalan dengan hasil penelitian Rambe dan Amrullah (2026) yang menekankan pentingnya pemisahan mekanisme enkripsi dan verifikasi identitas dalam sistem komunikasi yang memenuhi properti non-repudiasi.

KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem chat berbasis web dengan arsitektur *client-side encryption* yang mengintegrasikan kriptografi ASCON-AEAD128, RSA-2048-OAEP, dan RSA-2048-PSS+SHA-256. Serangkaian pengujian menunjukkan bahwa sistem berfungsi dengan tingkat keberhasilan 100% (28/28 kasus uji), membuktikan integrasi tiga mekanisme kriptografi melalui Web Cryptography API dapat diandalkan pada peramban modern. Dari sisi kinerja, proses enkripsi rata-rata hanya membutuhkan 1,20 ms dan dekripsi 0,73 ms, sehingga tetap efisien dan tidak mengganggu pengalaman pengguna, sekaligus menegaskan bahwa ASCON-AEAD128 sebagai primitif kriptografi ringan yang baru distandardisasi NIST dapat diimplementasikan secara praktis pada aplikasi web. Selain itu, tag autentikasi ASCON-AEAD128 menunjukkan efek *avalanche* mendekati ideal (50,16%), yang mengonfirmasi kualitas difusi kriptografis tinggi, sementara uji manipulasi data membuktikan sistem konsisten menolak seluruh skenario pemalsuan. Lebih jauh, arsitektur pemisahan antara lapisan integritas

(ASCON tag) dan autentisitas identitas (RSA-PSS) memberikan granularitas keamanan yang komprehensif, mencakup kerahasiaan, integritas pesan, autentikasi pengirim, dan non-repudiasi. Dengan hasil tersebut, sistem ini layak dikembangkan lebih lanjut, khususnya melalui penambahan fitur Perfect Forward Secrecy menggunakan protokol pertukaran kunci Diffie-Hellman efemeral sebagai arah penelitian berikutnya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Muhammadiyah Sumatera Utara, khususnya Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI UMSU), atas dukungan akademis dan fasilitas yang diberikan selama pelaksanaan penelitian ini. Terima kasih juga disampaikan kepada seluruh responden yang telah berpartisipasi dalam sesi pengujian sistem, serta kepada keluarga dan rekan-rekan mahasiswa yang telah memberikan dukungan moral selama proses penyusunan penelitian..

DAFTAR PUSTAKA

- BSSN. (2024). *Laporan tahunan keamanan siber Indonesia 2023*. Badan Siber dan Sandi Negara.
- CNN Indonesia. (2023, Januari 4). *BSSN: Ada 350 Juta Anomali Trafik di Indonesia Sepanjang 2022*. <https://www.cnnindonesia.com/teknologi/20230104160016-192-896022/bssn-ada-350-juta-anomali-trafik-di-indonesia-sepanjang-2022>
- Fauzi, M. R., & Tanjung, R. (2026). *Implementasi deteksi manipulasi data berbasis hash kriptografis pada aplikasi web*. Indonesian Journal of Multidisciplinary Scientific Studies, 4(6). <https://doi.org/10.33151/ijomss.v4i6.1130>
- Hutagalung, R., Siregar, M. A., & Manurung, H. S. (2023). *Implementasi algoritma RSA dan AES-256 untuk keamanan pesan pada sistem web*. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIK), 10(6), 1247–1256. <https://doi.org/10.25126/jtik.2023106>
- Kaur, H., Agrawal, S., & Bhardwaj, M. (2023). *Performance analysis of ASCON lightweight authenticated encryption in software environments*. arXiv preprint arXiv:2304.06222. <https://arxiv.org/abs/2304.06222>
- Kurniawan, A., Harahap, M., & Lubis, F. A. (2023). *Analisis kinerja ASCON-AEAD128 sebagai algoritma kriptografi ringan pada platform web*. Jurnal Penelitian Teknik Informatika dan Ilmu Komputer (JPTIHK), 7(13), 3412–3421.
- Lubis, S. A. (2022). *Pengamanan pesan teks berbasis web menggunakan algoritma Vigenere Cipher*. Jurnal Cyber Tech, 5(1), 45–53.
- National Institute of Standards and Technology. (2023). *Lightweight cryptography standardization process: NIST selects ASCON*. U.S. Department of Commerce. <https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices>
- Perkasa, D. A., Wibowo, F. W., & Nugroho, H. (2025). *Implementation of RSA-AES hybrid encryption for secure message transmission in web-based e-learning platforms*. Engineering Proceedings, 82(1), 14. <https://doi.org/10.3390/engproc2025082014>
- Rambe, T. H., & Amrullah, M. F. (2026). *Verifikasi tanda tangan digital berbasis RSA untuk autentikasi identitas pada sistem komunikasi jaringan*. Indonesian Journal of Multidisciplinary Scientific Studies, 4(6). <https://doi.org/10.33151/ijomss.v4i6.1131>
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM, 21(2), 120–126. <https://doi.org/10.1145/359340.359342>
- Tempo.co. (2025, Februari 12). *Kebocoran Data Indonesia Meningkat, BSSN Sebut Ratusan Juta Serangan Sepanjang 2024*. <https://tekno.tempo.co/read/1823456/kebocoran-data-indonesia-meningkat>
- Turan, M. S., McKay, K. A., Chang, D., Bassham, L., Kang, J., Lim, H., & Hwang, D. (2025). *Recommendation for lightweight cryptography (NIST SP 800-232 ipd)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-232.ipd>
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022). Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.
- W3C. (2017). *Web Cryptography API (W3C Recommendation)*. World Wide Web Consortium. <https://www.w3.org/TR/WebCryptoAPI/>