



Universitas Esaunggul

Pengamanan Dokumen Digital menggunakan Algoritma RSA dalam Sistem Manajemen File Berbasis Web

Azkiya Zahrul Umam¹, Raihan Fadhli Ramadhan², Ramadhan Tri Rizky Saputra³, Jefry Sunupurwa Asri⁴

¹Universitas Esa Unggul, azkiya.simdig32@student.esaunggul.ac.id ²Universitas Esa Unggul,
raihanfadhiliir@student.esaunggul.ac.id ³Universitas Esa Unggul, ramadhantririzky@gmail.com

⁴Universitas Esa Unggul, jefry.sunupurwa@esaunggul.ac.id

pendahuluan



Pada era modern saat ini, penggunaan internet telah menjadi kebutuhan primer masyarakat global. Perkembangan teknologi informasi memungkinkan berbagai aktivitas dilakukan secara daring (online), seperti pengiriman data, transaksi keuangan, hingga pengelolaan dokumen penting. Namun, seiring dengan meningkatnya ketergantungan terhadap sistem berbasis web, muncul pula risiko ancaman keamanan data, seperti pencurian informasi, penyadapan data, dan peretasan sistem. Serangan seperti data breach, unauthorized access, dan man-in-the-middle attack seringkali menargetkan file atau dokumen yang dikirim melalui jaringan internet (Singh & Supriya, 2020).



Universitas Esaunggul

METODELOGI

METODE

Systematic Literature Review

PROTOKOL

PRISMA

SUMBER LITELATUR

Google Scholar



Universitas Esaunggul

TEMUAN UTAMA

- RSA efektif untuk distribusi kunci dan autentikasi (Stallings, 2017)
- RSA memiliki komputasi lebih lambat dibanding algoritma simetris(Kahn Academy Cryptography, 2021)
- Pendekatan hybrid RSA–AES direkomendasikan untuk sistem file (NIST SP 800-57, 2022)



detikinet

Senin, 12 Jan 2026 13:17 WIB

Oknum Pegawai Akses Data Pribadi, Tata Kelola KAI Dinilai Amburadul

Pakar keamanan siber, Alfons Tanujaya, menilai tata kelola data PT KAI amburadul. Hal itu berkaitan dengan penyalahgunaan data penumpang yang viral di X.

Bahaya! 2,5 Miliar Pengguna Gmail Jadi Target Phishing Usai Peretasan

Adi Fida Rahman - detikinet

Senin, 25 Agu 2025 08:15 WIB



MONITOR INDONESIA

Home > Ekonomi

Data SIM Diduga Bocor 1,3 Miliar! IAW: Ini Bahaya Digital dari Dalam Negeri



Rolia Pakpahan

Diperbarui 28 Juli 2025 15:36 WIB



DISCUSSION (Interpretasi, Perbandingan, Kekuatan, Implikasi)

Interpretasi Utama dari Temuan

Literatur menunjukkan bahwa RSA efektif untuk menjaga confidentiality dan authentication pada sistem manajemen file berbasis web dalam konteks kriptografi klasik
(Rivest, Shamir, & Adleman, 1978; Stallings, 2017; NIST SP 800-57, 2022)

Perbandingan

- Stallings (2017) dan Kahn Academy Cryptography Review (2021) yang menyatakan bahwa RSA kuat secara keamanan namun kurang efisien untuk data berukuran besar
- Berbeda dengan studi yang hanya menekankan keamanan teoritis, beberapa penelitian terbaru merekomendasikan pendekatan hybrid RSA-AES untuk implementasi praktis (NIST SP 800-57, 2022)

Kekuatan

- RSA mendukung distribusi kunci publik dan autentikasi secara aman
- (Diffie & Hellman, 1976; Rivest et al., 1978)

Implikasi

- Implikasi Teoretis:
Menguatkan posisi RSA sebagai algoritma kriptografi asimetris yang masih relevan dalam literatur keamanan informasi klasik (Stallings, 2017; NIST, 2022)
- Implikasi Praktis:
Sistem manajemen file berbasis web disarankan menggunakan skema hybrid RSA-AES untuk menyeimbangkan keamanan dan performa (NIST SP 800-57, 2022)