Studi Literatur: Algoritma RSA (Rivest-Shamir-Adleman) dalam Keamanan Sistem Manajemen File Berbasis Web

Penulis: Azkiya Zahrul Umam[1], Raihan Fadhli Ramadhan[2], Ramadhan Tri Rizky[3]

1. 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).

Kasus kebocoran data di Indonesia memperlihatkan pentingnya sistem keamanan informasi yang kuat. Contohnya, pada Mei 2020 sebanyak 91 juta data pengguna Tokopedia bocor dan dijual di situs gelap (dark web). Di bulan yang sama, Daftar Pemilih Tetap (DPT) Pemilu 2014 juga bocor dan menyebar di forum peretas, berisi data pribadi seperti NIK, alamat, dan tanggal lahir. Selanjutnya, pada tahun 2021, data pribadi dari BPJS Kesehatan yang berjumlah sekitar 20 juta data juga bocor dan diunggah di komunitas hacker dalam bentuk file Excel yang berisi NIK, nomor HP, email, dan NPWP. Kasus-kasus tersebut menunjukkan lemahnya sistem pengamanan data digital yang digunakan pada berbagai lembaga dan aplikasi daring.

Keamanan data adalah aspek penting untuk menjaga kerahasiaan informasi yang hanya boleh diakses oleh pihak yang berwenang. Salah satu solusi untuk mengatasi ancaman tersebut adalah penerapan kriptografi, yaitu ilmu dan seni dalam menyandikan data agar tidak dapat dibaca oleh pihak yang tidak memiliki otorisasi. Dengan kriptografi, data penting seperti dokumen, identitas pengguna, dan informasi sensitif dapat dienkripsi sebelum dikirim melalui jaringan internet, sehingga meskipun data tersebut berhasil disadap, isinya tetap tidak dapat dibaca.

Penelitian terdahulu oleh Widiarsana et al. (2021) mengembangkan Aplikasi Website Pengamanan File Dokumen Menggunakan Kriptografi RSA dan menunjukkan bahwa algoritma RSA mampu meningkatkan keamanan dokumen digital secara signifikan. Begitu pula dengan Rakhmat Kurniawan (2017) yang menggunakan RSA untuk melindungi file teks, meskipun masih terdapat keterbatasan karena kunci enkripsi dan dekripsi ditetapkan secara statis tanpa pembangkitan kunci dinamis.

Berdasarkan latar belakang tersebut, penelitian ini mengusulkan penerapan algoritma RSA dalam aplikasi manajemen file berbasis web untuk meningkatkan keamanan dokumen digital. Dengan menerapkan proses enkripsi pada sisi klien dan dekripsi di sisi server menggunakan pasangan kunci RSA, diharapkan dapat menjaga kerahasiaan data pengguna dan mengurangi risiko kebocoran informasi saat transmisi melalui jaringan internet.

2. Konsep Dasar Kriptografi

2.1 Definisi Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik penyandian (encryption) dan pembacaan kembali (decryption) pesan agar hanya pihak tertentu yang dapat memahami isi pesan tersebut. Dalam konteks keamanan data digital, tujuan utamanya mencakup empat aspek penting:

1. **Kerahasiaan (Confidentiality)** — menjamin hanya pihak berwenang yang dapat mengakses data.
2. **Integritas (Integrity)** — memastikan data tidak diubah tanpa izin.
3. **Autentikasi (Authentication)** — membuktikan keaslian sumber data.
4. **Non-repudiasi (Non-repudiation)** — memastikan pengirim tidak dapat menyangkal pengiriman data.

2.2 Jenis Kriptografi

Berdasarkan cara penggunaan kunci, kriptografi terbagi menjadi dua jenis utama:

- **Kriptografi Simetris**, menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, contohnya AES (Advanced Encryption Standard) dan DES (Data Encryption Standard).
- **Kriptografi Asimetris**, menggunakan dua kunci yang berbeda: kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Contohnya adalah RSA (Rivest–Shamir–Adleman) dan ECC (Elliptic Curve Cryptography).

Jenis Kriptografi	Jumlah Kunci	Kecepatan	Tingkat Keamanan	Contoh Algoritma	Aplikasi Umum
Simetris	1 (sama untuk enkripsi & dekripsi)	Cepat	Cukup tinggi	AES, DES	Enkripsi data lokal
Asimetris	2 (publik & privat)	Lebih lambat	Sangat tinggi	RSA, ECC	Keamanan web, tanda tangan digital

RSA termasuk dalam algoritma asymmetric key cryptography yang cocok untuk sistem manajemen file berbasis web, karena memungkinkan pengamanan antar pengguna tanpa berbagi kunci rahasia secara langsung (Menezes et al., 2018).

2.3 Algoritma RSA

Algoritma RSA (Rivest–Shamir–Adleman) dikembangkan pada tahun 1976 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman dari MIT. RSA termasuk algoritma kriptografi asimetris yang didasarkan pada kesulitan matematis memfaktorkan bilangan besar menjadi faktor prima.

Proses utama RSA meliputi:

1. Menentukan dua bilangan prima besar, p dan q.
2. Menghitung $n = p \times q$ dan $\varphi(n) = (p-1)(q-1)$.
3. Memilih kunci publik e yang relatif prima terhadap $\varphi(n)$.
4. Menentukan kunci privat d menggunakan rumus $e \times d \equiv 1 \pmod{\varphi(n)}$.
5. Proses enkripsi: c = m^e mod n
6. Proses dekripsi: m = c^d mod n

Semakin besar ukuran kunci (bit length) yang digunakan, maka semakin tinggi tingkat keamanan RSA, namun juga semakin tinggi kebutuhan komputasi.

3. Tinjauan Penelitian Terdahulu

Peneliti & Tahun	Metode / Algoritma	Tujuan Penelitian	Hasil & Temuan	Kelemahan / Keterbatasan
Widiarsana, M.A. et al. (2022) – Aplikasi Website Pengamanan File Dokumen Menggunakan Kriptografi RSA (ojs.unud.ac.id)	RSA	Membangun sistem web untuk mengamankan dokumen (upload/download) menggunakan RSA	Berhasil mengenkripsi dan mendekripsi file dengan tingkat keberhasilan di atas 90%; sistem efektif menjaga kerahasiaan file.	Proses enkripsi lambat untuk file berukuran besar.
Rijanandi, T. et al. (2022) – Designing End-to-End Web-Based Application Encryption with Asymmetric Encryption (journal.ithb.ac.id)	RSA (Asimetris)	Menerapkan enkripsi RSA pada sistem web end-to-end untuk meningkatkan keamanan komunikasi data	Implementasi RSA berhasil mencegah akses tidak sah antar klien dan server; mendukung sistem multiuser.	Belum diuji pada file besar atau integrasi dengan cloud storage.
Sholikhatin et al. (2024) – Comparative Study of RSA Asymmetric Algorithm and AES Algorithm for Data Security (journal.unnes.ac.id)	RSA & AES	Membandingkan efektivitas RSA vs AES dalam menjaga keamanan data digital	RSA lebih unggul dalam distribusi kunci publik dan keamanan komunikasi, AES lebih efisien dalam kecepatan.	RSA kurang efisien untuk enkripsi file besar, namun unggul dalam sistem berbasis web dengan banyak pengguna.

4. Analisis dan Sintesis

Berdasarkan ketiga penelitian terdahulu, dapat diidentifikasi pola umum bahwa algoritma RSA merupakan salah satu metode kriptografi asimetris yang paling sering diterapkan dalam sistem berbasis web untuk menjamin kerahasiaan, integritas, dan autentikasi dokumen digital. RSA unggul dalam skenario di mana diperlukan keamanan pertukaran data antar pengguna, seperti sistem pengarsipan dokumen, layanan berbagi file, serta sistem tanda tangan digital.

Dari hasil sintesis literatur, beberapa poin penting dapat disimpulkan sebagai berikut:

- **Keunggulan utama RSA** terletak pada mekanisme kunci publik dan privat yang memastikan proses enkripsi dan dekripsi hanya dapat dilakukan oleh pihak yang berwenang. Hal ini menjadikan RSA sangat efektif dalam menjaga kerahasiaan dokumen selama proses transmisi data melalui jaringan publik (Aryasanti et al., 2022; Hutasuhut et al., 2019).
- **RSA untuk aplikasi web** terbukti andal untuk aplikasi manajemen file berbasis web, di mana ukuran file relatif kecil hingga menengah dan tingkat keamanan menjadi prioritas utama. Namun, efisiensi RSA menurun signifikan ketika diterapkan untuk enkripsi file berukuran besar atau dalam sistem dengan volume transaksi tinggi karena kompleksitas komputasinya yang tinggi (Ali & Rahman, 2020).
- **RSA untuk sistem multi-user** juga dinilai relevan untuk sistem multi-user, karena kemampuannya dalam mengelola pasangan kunci yang unik untuk setiap pengguna, memungkinkan autentikasi individual dan kontrol akses dokumen yang granular.

5. Arah dan Peluang Penelitian

Berdasarkan hasil tinjauan dari berbagai penelitian sebelumnya, dapat disimpulkan bahwa algoritma RSA masih menjadi salah satu metode kriptografi paling andal dalam menjaga kerahasiaan dan autentikasi data digital, terutama untuk sistem berbasis web.

Namun, perkembangan kebutuhan sistem modern seperti multi-user access, cloud integration, dan file sharing real-time menimbulkan tantangan baru yang membuka ruang bagi penelitian lanjutan.

A. Arah Penelitian

Penelitian diarahkan untuk mengimplementasikan algoritma RSA dalam sistem manajemen file berbasis web guna melindungi dokumen digital dari akses tidak sah. Fokus utama penelitian ini meliputi:

1. **Integrasi RSA dengan Sistem Manajemen File Modern** — Hasil penelitian dari Hutasuhut et al. (2019) dan Aryasanti et al. (2022) menunjukkan efektivitas RSA dalam

menjaga keamanan file di aplikasi web, tetapi keduanya belum menyinggung integrasi dengan sistem manajemen file multi-user atau berbasis cloud storage.

2. **Evaluasi Efektivitas dan Keamanan RSA** — Mengukur tingkat keamanan dan performa RSA terhadap ancaman seperti penyadapan atau perubahan data.
3. **Uji Coba pada Lingkungan Multi-user** — Menguji sejauh mana RSA mampu menjaga kerahasiaan data ketika digunakan oleh beberapa pengguna secara bersamaan.

B. Peluang Penelitian (Research Opportunities)

Bidang Fokus	Deskripsi Peluang Penelitian	Output yang Diharapkan
Manajemen File Web Multi-user	Menerapkan RSA untuk sistem file dengan autentikasi per pengguna dan enkripsi kunci dinamis.	Arsitektur keamanan multiuser berbasis RSA.
Implementasi RSA dalam Sistem Web	Penerapan RSA untuk mengamankan file pada sistem manajemen file berbasis web.	Aplikasi web dengan fitur enkripsi dan dekripsi RSA.
Evaluasi Kinerja RSA	Pengujian kecepatan dan keamanan enkripsi-dekripsi file dengan RSA.	Analisis performa RSA terhadap berbagai ukuran file.

RSA tetap relevan dan kuat untuk aplikasi manajemen file berbasis web karena:

- Memberikan mekanisme autentikasi dan kerahasiaan data yang tinggi melalui sistem kunci publik dan kunci privat.
- Cocok diterapkan pada proses enkripsi dan dekripsi file dalam aplikasi web untuk mencegah akses tidak sah.
- Dapat diimplementasikan dengan mudah pada sistem manajemen file multi-user, sehingga setiap pengguna memiliki kunci keamanan yang unik untuk melindungi dokumennya.

6. Kesimpulan

Berdasarkan hasil telaah literatur dari berbagai penelitian terdahulu, dapat disimpulkan bahwa keamanan data dalam aplikasi web menjadi kebutuhan yang semakin kritis di era digital. Banyaknya kasus kebocoran data di Indonesia maupun global menunjukkan bahwa sistem penyimpanan dan transmisi file tanpa lapisan keamanan yang kuat sangat rentan terhadap ancaman seperti eavesdropping, data tampering, dan unauthorized access (Widiarsana et al., 2021).

Kriptografi, khususnya algoritma RSA (Rivest–Shamir–Adleman), terbukti menjadi salah satu solusi paling efektif untuk menjaga kerahasiaan, integritas, dan autentikasi data. RSA bekerja dengan prinsip kunci publik dan kunci privat, yang membuatnya unggul dibandingkan algoritma simetris seperti DES atau Blowfish dalam konteks distribusi kunci dan keamanan komunikasi (Hutasuhut et al., 2019).

Hasil analisis terhadap ketiga jurnal menunjukkan bahwa:

1. RSA memberikan tingkat keamanan tinggi berkat kompleksitas matematis faktorisasi bilangan prima besar.
2. RSA lebih sesuai untuk pengamanan dokumen dan komunikasi berbasis web, di mana ukuran data relatif kecil hingga sedang dan keamanan lebih diutamakan dibanding kecepatan.

Meskipun demikian, RSA memiliki keterbatasan performa pada file berukuran besar, sehingga penelitian lanjutan dapat diarahkan pada penerapan hybrid cryptosystem untuk menjaga keseimbangan antara kecepatan dan keamanan. Selain itu, belum banyak penelitian yang secara spesifik mengimplementasikan RSA pada sistem manajemen file berbasis web dengan dukungan multi-user dan integrasi cloud, yang membuka ruang penelitian baru.

Dengan demikian, topik "Implementasi Algoritma RSA untuk Keamanan Dokumen pada Aplikasi Manajemen File Berbasis Web" memiliki relevansi yang kuat dan kontribusi praktis dalam bidang keamanan informasi. Penelitian ini tidak hanya memperkuat aspek teoritis penerapan RSA, tetapi juga menawarkan arah baru untuk pengembangan sistem manajemen file aman dan efisien di era digital.

7. Daftar Pustaka

Aryasanti, N. P. D., Pradnyana, I. M. A., & Darma, G. S. (2022). Implementasi Algoritma RSA untuk Enkripsi Data pada Sistem Keamanan Dokumen Digital. Jurnal Ilmiah Teknologi Informasi, 20(1), 55–63. https://doi.org/10.33322/jiti.v20i1.2891

Hutasuhut, R., Siregar, S., & Sihombing, R. (2019). Penerapan Algoritma RSA dalam Pengamanan File pada Sistem Informasi Berbasis Web. Jurnal Teknologi dan Sistem Komputer, 7(3), 221–230. https://doi.org/10.14710/jtsiskom.7.3.221-230

Menezes, A., Van Oorschot, P., & Vanstone, S. (2018). Handbook of Applied Cryptography. CRC Press.

Rijanandi, T., Argo, D., & Syahrizal, M. (2022). Designing End-to-End Web-Based Application Encryption with Asymmetric Encryption Using Waterfall Methodology. Telematika, 15(2), 55–66.

Singh, G., & Supriya, R. (2020). Review on Cryptography and Network Security. International Journal of Computer Applications, 176(9), 1–5.

Widiarsana, M. A., Dewa, I. G., & Yasa, A. A. (2022). Aplikasi Website Pengamanan File Dokumen Menggunakan Kriptografi RSA. Jurnal Ilmiah Lontar Komputer, 13(3), 221–230.