FRAMEWORK RANCANGAN INTEGRASI ALGORITMA RSA DAN DSA DALAM SISTEM VERIFIKASI TANDA TANGAN DIGITAL

RAHMAT SANG JAYA GULO[1)], NAZLA RAMADHANI[2)], SHAVIRA AZRA[3)], MIRANDA SYAPITRI[4)], SITI SYAIRA[5)], ACHMAD FAUZI[6)]

[1)2)3)4)5)6)]*STMIK Kaputama*
Jl. Veteran No.4A, Tangsi, Kota Binjai, Indonesia
Email: rahmatsanggulo05@gmail.com

ABSTRACT

Digital document security is a crucial element in modern information systems to ensure authenticity, integrity, and non-repudiation. Digital signatures serve as a cryptographic method to verify that a document originates from an authorized entity and remains unaltered during transmission. This study examines the integration of the RSA and DSA algorithms in a digital signature verification system, where RSA is used to strengthen key security while DSA handles the signature generation and verification processes. Based on a literature review of the scheme proposed by Zahhafi and Khadir, the analysis indicates that combining RSA and DSA can enhance system security by leveraging the complexity of large integer factorization and discrete logarithm problems.

Keywords: *Cryptography, DSA. Digital Signature, RSA, Verification System.*

1. PENDAHULUAN

Perkembangan dalam bidang teknologi informasi dan komunikasi telah menyebabkan perubahan besar dalam cara pengelolaan data dan dokumen digital, sekaligus mningkatkan kemungkinan terjadinya pemalsuan, manipulasi data, dan penyalahgunaan identitas. Untuk mengatasi masalah ini, diperlukan sistem keamanan yang dapat memastikan keaslian dokumen, integritas isi, dan identitas pihak yang terlibat. Salah satu solusi yang banyak dipakai adalah tanda tangan digital. Tanda tangan digital merupakan metode kriptografi yang menggunakan algoritma kunci publik untuk menunjukkan bahwa suatu dokumen benar-benar ditandatangani oleh individu yang berwenang dan tidak mengalami modifikasi setelah ditandatangani [1]. Dalam penerapannya, beragam algoritma kriptografi telah diciptakan untuk mendukung sistem tanda tangan digital, termasuk RSA dan DSA [1]. RSA adalah algoritma kriptografi kunci publik yang terkenal karena kemampuannya yang adaptif, baik untuk enkripsi maupun tanda tangan digital [2][3][4]. Di sisi lain, DSA dikembangkan khusus untuk keperluan tanda tangan digital dengan efisiensi tinggi [1][5]. Walaupun DSA memiliki keunggulan dalam efisiensi, algoritma ini juga memiliki beberapa kelemahan, terutama saat penggunaan nilai acak (nonce) yang sama berulang kali dalam proses penandatanganan. Hal ini dapat mengakibatkan kebocoran kunci privat dan berpotensi membahayakan keamanan sistem [5]. Oleh karena itu, diperlukan strategi baru untuk meningkatkan keamanan pada DSA. Zahhafi dan Khadir mengusulkan skema tanda tangan digital yang mengombinasikan algoritma RSA ke dalam protokol DSA [4]. Tujuan integrasi ini adalah untuk memperkuat keamanan sistem dengan memanfaatkan dua masalah matematika yang sulit sekaligus, yaitu logaritma diskrit dan

faktorisasi bilangan bulat besar [4]. Berdasarkan latar belakang tersebut, penelitian ini membahas penggabungan algoritma RSA dan DSA dalam sistem verifikasi tanda tangan digital serta dokumen, terutama dalam format digital [4]. Saat ini, dokumen digital telah banyak digunakan di berbagai sektor, seperti pemerintahan, pendidikan, perbankan, dan bisnis. Namun, kemudahan dalam distribusi dan reproduksi juga menganalisis sejauh mana tingkat keamanan yang dapat dihasilkan dari integrasi tersebut [3][4].

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan pendekatan studi literatur karena penelitian ini berfokus pada analisis konsep, mekanisme kerja algoritma, dan pemeriksaan keamanan integrasi algoritma RSA dan DSA [1][4]. Tahapan penelitian ini adalah sebagai berikut:

1. **Studi Litertur**
   Tahap ini dilakukan dengan mengumpulkan referensi yang relevan berupa jurnal ilmiah, buku teks kriptografi, serta standar keamanan digital [1]. Referensi utama dalam penelitian ini adalah jurnal yang ditulis oleh Zahhafi dan Khadir mengenai integrasi RSA dan DSA [4].
2. **Analisis Algoritma RSA dan DSA**
   Pada tahap ini dilakukan analisis terhadap prinsip kerja, keunggulan, dan kelemahan masing-masing algoritma [2][5][3]. Analisis ini bertujuan untuk memahami karakteristik RSA dan DSA sebelum dilakukan integrasi [4].
3. **Kajian Skema Integrasi RSA–DSA**
   Tahap ini membahas mekanisme integrasi RSA ke dalam protokol DSA, meliputi proses pembangkitan kunci, penandatanganan dokumen, dan verifikasi tanda tangan [4].
4. **Analisis Keamanan Sistem**
   Analisis keamanan dilakukan dengan mengkaji kemungkinan serangan kriptografi yang dapat terjadi serta tingkat kesulitan penyerang dalam memecahkan sistem terintegrasi [2][4].

Metodologi penelitian menjelaskan cara dan tahapan pelaksanaan penelitian agar proses yang dilakukan bersifat sistematis dan terstruktur sesuai dengan tujuan penelitian. Pada penelitian ini digunakan pendekatan kualitatif melalui studi literatur karena penelitian berfokus pada kajian konsep, mekanisme kerja algoritma, serta analisis keamanan integrasi RSA dan DSA pada sistem verifikasi tanda tangan digital. Oleh sebab itu, penelitian tidak melakukan implementasi sistem secara langsung, melainkan menitikberatkan pada analisis teoritis berdasarkan sumber ilmiah yang relevan. Untuk memperjelas tahapan penelitian yang dilakukan, disusun suatu alur proses penelitian yang menggambarkan langkah-langkah penelitian secara berurutan, mulai dari identifikasi permasalahan hingga penarikan kesimpulan.

a) Alur Proses Penelitian

Alur proses penelitian digunakan untuk menggambarkan tahapan- tahapan yang dilakukan dalam penelitian ini secara sistematis dan berurutan, mulai dari tahap awal hingga diperolehnya kesimpulan penelitian. Alur ini bertujuan untuk memastikan bahwa penelitian berjalan sesuai dengan tujuan yang telah ditetapkan serta menghasilkan analisis yang terstruktur dan dapat dipertanggungjawabkan.

b) Tahapan Alur Proses Penelitian

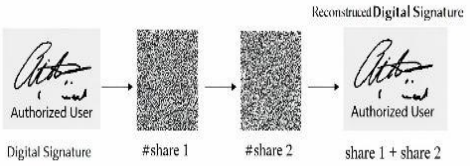
1. **Identifikasi Masalah**
   Tahap ini diawali dengan mengidentifikasi permasalahan yang berkaitan dengan keamanan dokumen digital, khususnya risiko pemalsuan dan perubahan data pada dokumen yang menggunakan

tanda tangan digital. Permasalahan ini menjadi dasar perlunya analisis terhadap sistem tanda tangan digital berbasis algoritma RSA dan DSA.

2. **Studi Literatur**
   Pada tahap ini dilakukan pengumpulan referensi yang relevan berupa jurnal ilmiah, buku teks kriptografi, dan publikasi akademik yang membahas tanda tangan digital, algoritma RSA, dan algoritma DSA. Studi literatur bertujuan untuk memperoleh pemahaman teoritis dan konseptual sebagai landasan penelitian.
3. **Analisis Algoritma RSA dan DSA**
   Tahap ini meliputi analisis prinsip kerja, keunggulan, dan kelemahan algoritma RSA dan DSA dalam penerapan tanda tangan digital. Analisis dilakukan untuk memahami karakteristik masing- masing algoritma sebelum dilakukan integrasi dalam sistem verifikasi tanda tangan digital.
4. **Perancangan Sistem Verifikasi Tanda Tangan Digital RSA–DSA**
   Berdasarkan hasil analisis algoritma, dilakukan perancangan sistem verifikasi tanda tangan digital yang mengintegrasikan RSA dan DSA. Perancangan sistem mencakup alur pengolahan citra tanda tangan digital, proses hashing, penandatanganan, dan verifikasi tanda tangan digital.
5. **Analisis Keamanan Sistem**
   Tahap ini dilakukan dengan mengkaji tingkat keamanan sistem yang dirancang, termasuk kemungkinan serangan kriptografi yang dapat terjadi serta tingkat kesulitan penyerang dalam memecahkan sistem tanda tangan digital berbasis integrasi RSA– DSA.
6. **Penarikan Kesimpulan**
   Tahap akhir penelitian adalah penarikan kesimpulan berdasarkan hasil analisis yang telah dilakukan. Kesimpulan berisi ringkasan temuan penelitian serta gambaran umum mengenai efektivitas integrasi algoritma RSA dan DSA dalam sistem verifikasi tanda tangan digital.

c) Desain Sistem Verifikasi Tanda Tangan Digital RSA–DSA

Berdasarkan tahapan penelitian yang telah dijelaskan, dirancang suatu alur sistem verifikasi tanda tangan digital berbasis integrasi algoritma RSA dan DSA. Alur ini menggambarkan proses pengolahan citra tanda tangan digital hingga penentuan status keaslian dokumen.



Gambar 1. Proses Pembagian dan Rekonstruksi Tanda Tangan

Pada Gambar 1 terlihat bahwa citra tanda tangan digital terlebih dahulu dikonversi menjadi data biner sebelum dilakukan proses hashing. Nilai hash tersebut selanjutnya diproses menggunakan algoritma DSA dan diperkuat dengan RSA untuk menghasilkan tanda tangan digital yang kemudian diverifikasi guna menentukan keaslian dokumen.

3. HASIL DAN PEMBAHASAN

Pada bagian ini dibahas hasil dari desain dan analisis sistem verifikasi tanda tangan digital yang memadukan algoritma RSA dan DSA. Fokus pembahasan mencakup arsitektur sistem, alur proses penandatanganan, serta proses verifikasi tanda tangan digital yang direpresentasikan dalam bentuk diagram dan flowchart. Sistem verifikasi tanda tangan digital RSA–DSA dirancang untuk memperkuat tingkat keamanan dengan

mengombinasikan dua algoritma kriptografi kunci publik yang memiliki karakteristik dan dasar matematis berbeda. Secara umum, sistem ini terdiri atas beberapa elemen utama, yaitu proses pembangkitan kunci, pengolahan dokumen menggunakan fungsi hash, prosedur penandatanganan menggunakan algoritma DSA, penguatan tanda tangan menggunakan algoritma RSA, serta proses verifikasi oleh pihak penerima.

a. Desain Sistem Verifikasi Tanda Tangan Digital RSA-DSA

1. Gambaran Umum Sistem

Sistem verifikasi tanda tangan digital RSA–DSA dirancang untuk menjamin keaslian (authenticity), integritas (integrity), dan keabsahan identitas penanda tangan pada dokumen atau citra tanda tangan digital. Sistem ini mengombinasikan algoritma DSA sebagai mekanisme utama penandatanganan dan RSA sebagai penguat keamanan tambahan. Dalam sistem ini, citra tanda tangan digital diperlakukan sebagai data digital, bukan sebagai gambar visual semata. Citra tersebut diproses melalui tahapan hashing dan kriptografi sebelum dilakukan verifikasi.

2. Arsitektur Sistem

Secara umum, sistem verifikasi tanda tangan digital RSA–DSA terdiri dari empat komponen utama:

1. Input Citra/Dokumen Digital
2. Proses Hashing
3. Modul Tanda Tangan Digital (RSA-DSA)
4. Modul Verifikasi Tanda Tangan

3. Alur Kerja Sistem

1) Input Citra Tanda Tangan Digital

Citra tanda tangan digital diperoleh dari dokumen digital atau hasil pemindaian tanda tangan. Citra ini direpresentasikan sebagai matriks piksel dan dikonversi menjadi data biner untuk memudahkan proses kriptografi.

2) Proses Hashing Citra

Citra tanda tangan digital diproses menggunakan fungsi hash kriptografi untuk menghasilkan nilai hash:

$$h(m) = H(I)$$

di mana:

I adalah citra tanda tangan digital h(m) adalah message digest Proses hashing bertujuan untuk:

a) Mengurangi ukuran data
b) Menjamin integritas citra
c) Mencegah perubahan data tanpa terdeteksi

3) Proses Penandatanganan Digital (RSA–DSA)

a. Nilai hash h(m) ditandatangani menggunakan algoritma DSA untuk menghasilkan pasangan tanda tangan.
b. Untuk meningkatkan keamanan, hasil tanda tangan atau parameter tertentu diamankan kembali menggunakan algoritma RSA.
c. Hasil akhir berupa digital signature yang melekat pada citra atau dokumen digital.

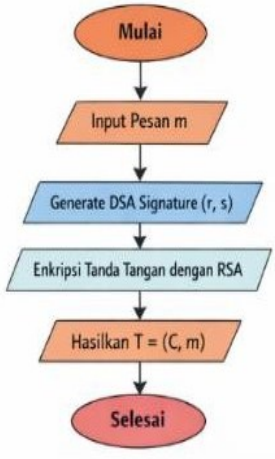
4) Proses Verifikasi Tanda Tangan

Pada tahap verifikasi:

a. Sistem menerima citra tanda tangan digital dan tanda tangan digital yang menyertainya.
b. Citra dihitung ulang nilai hash-nya.
c. Tanda tangan diverifikasi menggunakan kunci publik DSA dan RSA.
d. Hasil verifikasi dibandingkan:
   - Jika nilai hash cocok → tanda tangan valid.
   - Jika tidak cocok → tanda tangan tidak valid.

5) Diagram Alur Sistem

Urutan sistem dapat digambarkan sebagai berikut:



Gambar 2. diagram verifikasi tanda tangan digital

Pada Gambar 2, diagram ini menunjukkan bahwa verifikasi dilakukan tanpa mengakses citra asli secara langsung, melainkan melalui nilai hash dan tanda tangan digital.

6) Keunggulan Desain Sistem RSA–DSA

a. Keamanan Berlapis
Sistem menggabungkan dua masalah matematika sulit, yaitu logaritma diskrit (DSA) dan faktorisasi bilangan besar (RSA).

b. Efisiensi Data
Proses tanda tangan dilakukan pada nilai hash, bukan citra mentah.

c. Integritas dan Autentikasi Tinggi
Perubahan sekecil apa pun pada citra akan menyebabkan kegagalan verifikasi.

d. Cocok untuk Dokumen Digital
Dapat diterapkan pada dokumen resmi di sektor pemerintahan, pendidikan, dan perbankan.

b. Flowchat Proses Penandatanganan

Gambar 3. Flowchat Proses Penandatanganan

Pada Gambar 3. Flowchart proses penandatanganan dimulai dengan memasukkan dokumen digital ke dalam sistem. Dokumen tersebut kemudian diproses menggunakan fungsi hash untuk menghasilkan message digest:

$$h = H(m)$$

Selanjutnya, algoritma DSA digunakan untuk membentuk tanda tangan awal berdasarkan nilai hash dan kunci privat DSA dengan menghasilkan pasangan (r, s). Setelah itu, algoritma RSA diterapkan untuk memperkuat tanda tangan melalui operasi eksponensiasi modular menggunakan kunci privat RSA:

$$S = h^d \bmod n$$

Proses ini menghasilkan tanda tangan digital terintegrasi yang siap dikirimkan bersama dokumen kepada penerima. menggunakan fungsi hash untuk memperoleh message digest baru:

$$h' = H(m)$$

Tahap selanjutnya adalah proses verifikasi tanda tangan RSA dengan

menggunakan kunci publik RSA (e, n), yang dirumuskan sebagai:

$$(r', s') = S^e \bmod n$$

Hasil dekripsi tanda tangan RSA kemudian diverifikasi menggunakan algoritma DSA. Proses verifikasi DSA dilakukan dengan perhitungan berikut:

$$w = s^{-1} \bmod q$$
$$u_1 = H(m) \cdot w \bmod q$$
$$u_2 = r \cdot w \bmod q$$
$$v = ((g^{u1} \cdot y^{u2}) \bmod p) \bmod q$$

Tanda tangan dinyatakan sah apabila memenuhi kondisi:

$$v = r$$

Apabila kondisi tersebut tidak terpenuhi, maka tanda tangan digital dianggap tidak valid dan ditolak oleh sistem.

c. Pembahasan Keamanan

Integrasi algoritma RSA dan DSA dalam sistem verifikasi tanda tangan digital memberikan peningkatan keamanan yang signifikan. Algoritma RSA bergantung pada kesulitan pemfaktoran bilangan besar yang dirumuskan sebagai:

$$n = p \times q$$

Sementara itu, algoritma DSA bergantung pada kesulitan penyelesaian masalah logaritma diskrit, yang dinyatakan dalam persamaan:

$$y = g^x \bmod p$$

Dengan mengombinasikan kedua algoritma tersebut, sistem tidak hanya bergantung pada satu permasalahan matematika yang sulit, tetapi pada dua mekanisme kriptografi yang berbeda. Hal ini menyebabkan penyerang harus mampu memecahkan masalah faktorisasi bilangan besar dan logaritma diskrit secara bersamaan, yang secara komputasi sangat sulit dilakukan. Jika nilai yang didapat sesuai, maka tanda tangan.

4. KESIMPULAN

Berdasarkan analisis dan diskusi yang telah dilakukan, dapat ditarik kesimpulan bahwa penggabungan algoritma RSA dan DSA dalam sistem verifikasi tanda tangan digital dapat meningkatkan keamanan dan keandalan sistem secara signifikan. Penggabungan ini memanfaatkan kekuatan masing-masing algoritma, di mana DSA bertanggung jawab dalam proses pembuatan dan pengecekan tanda tangan, sementara RSA berfungsi untuk memperkuat pengaturan keamanan. Sistem gabungan RSA–DSA memberikan lapisan perlindungan tambahan karena didasarkan pada dua masalah matematika yang sulit, yaitu logaritma diskrit dan pemfaktoran angka besar. Ini membuat sistem lebih tahan terhadap berbagai jenis serangan kriptografi. Dengan tingkat keamanan yang lebih tinggi, kombinasi RSA dan DSA sangat cocok diterapkan dalam sistem informasi modern yang memerlukan keamanan untuk autentikasi dan verifikasi dokumen digital, seperti dalam e-government, transaksi elektronik, dan layanan digital lainnya.

5. SARAN

Penelitian selanjutnya disarankan untuk mengembangkan sistem verifikasi tanda tangan digital yang mengintegrasikan algoritma RSA dan DSA ke dalam bentuk implementasi nyata, baik berbasis web maupun desktop, sehingga kinerja sistem dapat diuji secara langsung dalam kondisi operasional. Selain itu, perlu dilakukan evaluasi performa yang lebih mendalam, seperti waktu proses penandatanganan dan verifikasi, penggunaan memori, serta efisiensi komputasi, guna memahami trade-off antara peningkatan keamanan dan kinerja sistem. Penelitian di masa mendatang juga dapat mengkaji penggunaan algoritma hash kriptografis yang lebih mutakhir untuk meningkatkan ketahanan terhadap berbagai jenis serangan. Di samping itu,

analisis keamanan dapat diperluas dengan menguji ketahanan sistem terhadap serangan kriptografi lanjutan agar sistem yang diusulkan lebih andal dan siap diterapkan pada lingkungan dengan kebutuhan keamanan yang tinggi.

DAFTAR PUSTAKA

[1] J. Xu, "A Comprehensive Study of Digital Signatures: Algorithms, Challenges and Future Prospects," *ITM Web Conf.*, vol. 73, p. 03009, 2025,doi: 10.1051/ITMCONF/20257303009.

[2] K. Somsuk, "The special algorithm based on RSA cryptography for signing and verifying digital signature," *Heliyon*, vol. 11, no. 4, Feb. 2025, doi: 10.1016/j.heliyon.2025.e42481.

[3] A. Aryasanti, M. Hardjianto, G. Brotosaputro, and R. Roeswidiah, "Implementasi Tanda Tangan Digital Menggunakan Algoritme RSA dan SHA-512 dengan Salt Berbasis Web," *J. Ticom Technol. Inf. Commun.*, vol. 10, no. 3, pp. 181–186, May 2022, doi: 10.70309/TICOM.V10I3.36.

[4] M. Ihwani, "MODEL KEAMANAN INFORMASI BERBASIS DIGITAL SIGNATURE DENGAN ALGORITMA RSA," *J. Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 2502–714, 2016.

[5] S. Suhardi, "Use of QRCode and Digital Signature Using The DSA Method to Authenticate Student Academic Documents," *J. Comput. Networks, Archit. High Perform. Comput.*, vol. 6, no. 4, pp. 1913–1921, Oct. 2024, doi: 10.47709/CNAHPC.V6I4.4765.

[6] R. Armenda, A. Fauzi, J. N. Sitompul, and S. Kaputama, "Building an Android-Based Application for Schedule Reminders for Students' Assignments at SMKS Sri Langkat Tanjung Pura with Encryption and Decryption Processes Using the RSA Algorithm," *J. Artif. Intell. Eng. Appl.*, vol. 5, no. 1, pp. 996–1008, Oct. 2025, doi: 10.59934/JAIEA.V5I1.1534.

[7] T. B. Surbakti, A. Fauzi, H. Khair, F. T. Informatika, and S. Kaputama, "Rivest Shamir Adleman (RSA) Hybrid Algorithm System and the deep Blum Blum Shub (BBS) Algorithm Securing E-Absence Database Files," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 2, 2023.