Penerapan ECDSA Dan BLAKE2B Untuk Membentuk Tanda Tangan Digital Sebagai Autentikasi Dokumen

Luthfi Amaludin[1], Alam Rahmatulloh[2]

Jurusan Informatika, Universitas Siliwangi, Jl. Mugarsari, Kel. Mugarsari, Kec. Tamansari, Kota Tasikmalaya 46196, Indonesia[1, 2]

217006102@student.unsil.ac.id[1], alam@unsil.ac.id [2]

Abstrak – Dokumen digital rentan terhadap risiko pemalsuan dan manipulasi, sehingga membutuhkan mekanisme autentikasi yang andal. Penelitian ini bertujuan mengatasi celah dalam sistem keamanan dokumen elektronik dengan mengeksplorasi kombinasi *Elliptic Curve Digital Signature Algorithm* (ECDSA) dan fungsi *hash BLAKE2b.* Pendekatan yang digunakan melibatkan implementasi algoritma menggunakan *library secp256k1* pada *Python*, serta pengujian menyeluruh pada dokumen PDF dan DOCX. Proses penandatanganan digital mencakup hashing dokumen menggunakan *BLAKE2b* untuk menghasilkan message digest unik, yang kemudian ditandatangani dengan kunci privat ECDSA. Verifikasi dilakukan dengan mencocokkan *hash* baru terhadap tanda tangan digital menggunakan kunci publik. Hasil menunjukkan kombinasi algoritma ini memiliki keunggulan signifikan, dengan waktu verifikasi 10,89% lebih cepat dibandingkan proses penandatanganan. Perbedaan ini diakibatkan oleh variasi kompleksitas operasi pada setiap tahapan. Meskipun metode ini bekerja dengan baik untuk dokumen PDF, ditemukan kendala teknis pada file DOCX terkait keterbatasan panjang *hash*. Penelitian ini menawarkan pendekatan inovatif untuk meningkatkan autentikasi dokumen digital, memberikan jaminan integritas dan keaslian dokumen elektronik. Hal ini juga membuka peluang untuk eksplorasi lebih lanjut dalam pengembangan sistem tanda tangan digital yang lebih efisien.

Kata Kunci – Tanda Tangan Digital, ECDSA, BLAKE2b, Dokumen Digital, Autentikasi

I. PENDAHULUAN

Dokumen adalah aset yang penting dan sumber informasi yang diperlukan oleh suatu instasnsi, organisasi, negara, maupun individu [1]. Dokumen elektronik sebagai pengganti dokumen konvensional berbasis kertas dalam pelayanan publik memiliki berbagai keunggulan, mulai dari fleksibilitas tinggi, kemudahan pencarian dan transfer, efisiensi penyimpanan, hingga sistem pengarsipan dan pemulihan data yang lebih aman [2]. Pemalsuan atau perubahan dalam suatu dokumen dapat diantisipasi dengan dokumen digital sebagai salah satu solusi. Meski demikian, pengamanan pada dokumen digital ini masih perlu dilakukan untuk menghindari perubahan isi dokumen oleh pihak yang tidak bertanggung jawab [3]. Untuk itu, strategi pengamanan dokumen yang baik perlu diadakan supaya informasi yang dikirim dapat dipastikan otensitasnya dan hanya dapat diterima oleh penerima yang berhak saja [4]. Autensitas dokumen dapat diketahui melalui penerapan *digital signature*. Konsep ini merupakan hasil dari pengembangan bidang kriptografi modern yang berfungsi untuk memastikan keaslian suatu berkas dan bersifat *non-repudiation* (anti penyangkalan) [5].

Tanda tangan digitial (*digital signature*) merupakan model matematika yang mengidentifikasi pengirim dan membuktikan keaslian pemiliki dokumen [6]. Proses verifikasi identitas yang dilakukan oleh setiap pihak dalam suatu komunikasi disebut otentikasi. Ketika sebuah pihak menerima data dari pihak lainnya, diperlukan suatu mekanisme pemeriksaan untuk memastikan bahwa informasi tersebut benar-benar berasal

dari sumber yang diklaim dan tidak mengalami perubahan selama proses transmisi [7].

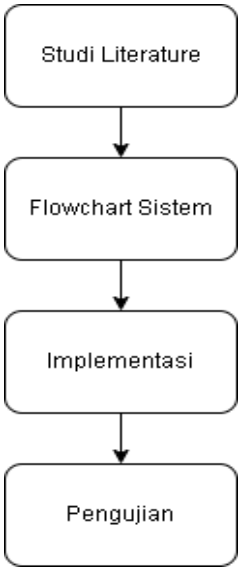
Berbagai penelitian terdahulu yang telah mengkaji penerapan *digital signature* untuk otentikasi dokumen digital. Penelitian [8] , penerapan kombinasi *digital signature* ECDSA dan SHA-3 menghasilkan proses tanda tangan digital yang efisien dengan waktu tanda tangan rata-rata sebesar 0,00286 detik. Pada penelitian [9] , melakukan penerapan *digital signature* ECDSA pada file tipe PDF. Lalu penelitian [10] , mengkombinasikan algoritma Elgamal dan SHA-256 untuk membentuk tanda tangan digital. Penelitia [11] , penggabungan SHA-256 dan RSA yang ditingkatkan serta penggunaan QR code pada proses akses tanda tangan digital dan otentikasi menjadi lebih mudah. Penelitian [12] , menunjukkan kinerja waktu ECDSA pada *multi-signature* dokumen dengan waktu rata-rata sekitar 0,001052 detik. Pada penelitian [13], menerapkan digital signature menggunakan ECDSA dan 2 jenis fungsi hash yang berbeda yaitu SHA-1 dan Keccak, menggunakan fungsi hash Keccak m emberikan waktu yang lebih singkat untuk pembangkitan kunci 0,8199 detik dan penandatanganan 0,0075 detik, sedangkan SHA-1 lebih cepat yaitu 0,0155 detik. Penelitian [14], menunjukkan bahwa algoritma ECDSA unggul dalam hal penggunaan waktu pada proses pembuatan pasangan kunci, proses penandatanganan dokumen, dan proses verifikasi dokumen.

Diklaim bahwa BLAKE2 lebih cepat daripada SHA untuk melakukan *hashing* pada sebuah *plaintext*. Ada dua varian utama dari BLAKE2 : BLAKE2b untuk platform 64-bit dan BLAKE2 untuk arsitektur yang lebih kecil. BLAKE2 pada platform 64-bit seringkali lebih cepat dari MD5 tetapi tetap memberikan keamanan yang setara dengan SHA-3. Dengan padding minimal, BLAKE2 tidak hanya lebih cepat, tetapi juga lebih sederhana untuk diimplementasikan, menjadikannya pilihan yang menarik bagi yang mencari antara keseimbangan antara kinerja tinggi dan keamanan yang kuat [15].

Algoritma seperti ECDSA telah terbukti efisien dalam proses pembuatan tanda tangan digital, sementara SHA-3 menawarkan tingkat keamanan yang tinggi. Namun, penggunaan SHA-3 masih memerlukan sumber daya komputasi yang lebih besar dibandingkan algoritma lain seperti BLAKE2, yang diklaim lebih cepat dan tetap aman, serta kemampuannya dalam memastikan autentisitas, integritas, dan non-repudiation dokumen digital.

Penelitian ini bertujuan untuk menerapkan kombinasi algoritma ECDSA dan BLAKE2b dalam pembentukan tanda tangan digital untuk autentikasi dokumen digital dan untuk mengevaluasi kecepatan dan keamanan dari kombinasi kedua algoritma tersebut.

II. ANALISA DAN PERANCANGAN SISTEM



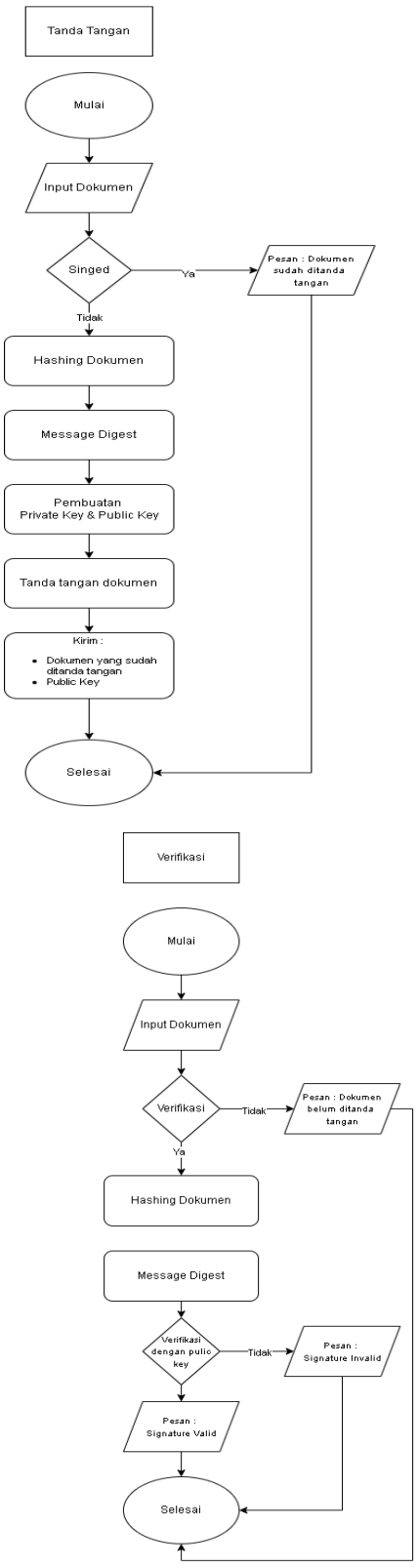
Gambar 1 Tahapan Penelitian

A. Studi Literatur

Tahapan studi literatur dilakukan untuk mengumpulkan dan menganalisis informasi dari berbagai sumber bacaan, termasuk jurnal ilmiah, buku, artikel, laporan penelitian, internet dan sumber bacaan lainnya. Dengan melakukan studi literatur, diperoleh pemahaman komprehensif mengenai topik yang diteliti dan penelitian yang dilakukan relevan.

pISSN: 2252-486X
eISSN: 2548-4710

B. Flowchart Sistem



Gambar 2 Flowchart Sistem

Proses penandatanganan dimulai dengan penginputan dokumen, diikuti oleh pemeriksaan apakah dokumen sudah pernah ditandatangani. Jika belum, dokumen tersebut di-*hash* menggunakan algoritma BLAKE2b untuk menghasilkan *message digest*, lalu ditandatangani menggunakan kunci privat yang dihasilkan oleh algoritma ECDSA. Tanda tangan digital dan kunci publik kemudian dikirimkan kepada penerima.

Proses verifikasi dimulai ketika penerima menginput dokumen, kunci publik, dan tanda tangan digital. Sistem memeriksa apakah dokumen sudah ditandatangani. Jika sudah, dokumen di-hash ulang untuk menghasilkan *message digest* baru. Verifikasi dilakukan dengan membandingkan hasil hash baru dengan tanda tangan digital menggunakan kunci publik. Jika valid, dokumen dianggap asli; jika tidak, dokumen dinyatakan telah dimodifikasi.

C. Implementasi

Implementasi algoritma ECDSA dilakukan dengan memanfaatkan library secp256k1 pada bahasa pemrograman Python untuk efisiensi komputasi pada kurva SECP256K1. Dokumen yang akan ditandatangani kemudian di-*hash* menggunakan algoritma BLAKE2b untuk menghasilkan representasi unik yang lebih pendek. Tanda tangan digital dihasilkan dengan menggunakan kunci privat dan hash pesan tersebut. Proses verifikasi tanda tangan dilakukan dengan menggunakan kunci publik untuk memastikan integritas dan keaslian pesan.

D. Pengujian

Pengujian dilakukan untuk mengevaluasi kinerja dan usability dari sistem tanda tangan digital berbasis ECDSA dan BLAKE2b. Data uji yang digunakan meliputi dokumen teks, PDF, dan DOCX dengan ukuran bervariasi. Pengujian dilakukan dari sistem yang telah dibuat. Meliputi pengujian penandatanganan dan verifikasi. Pengjujian tersebut dilakukan untuk melihat pengaruh algoritma ECDSA kurva SECP256K1 dengan fungsi hash BLAKE2b pada dokumen digital untuk autentikasi.

III. IMPLEMENTASI DAN PEMBAHASAN

A. *Penandatanganan*

Penerapan penandatanganan menggunakan algoritma ECDSA kurva SECP256K1 dan fungsi *hash* BLAKE2b meliputi :

1. Mulai → Input Dokumen Digital
   Menggunakan *library magic* untuk menentukan tipe file berdasarkan MIME type.

2. Memeriksa Tanda Tangan, Fungsi: *check_existing_signature*, Memeriksa apakah metadata PDF memiliki elemen /Signature dan /SignerName serta memeriksa file docProps/custom.xml dan mencari properti bernama DigitalSignature untuk file DOCX.

3. Hashing Dokumen dengan BLAKE2b,

$$\text{Hash}=H(T1\|T2\|\cdots\|Tn),$$

Dimana $T_1, T_2, \ldots, T_n$adalah teks dari setiap halaman (untuk PDF) atau setiap paragraf (untuk DOCX).

4. Pembuatan Kunci dengan ECDSA (Kunci Privat dan Publik), Kunci privat dihasilkan dari bilangan acak, dan kunci publik dihitung sebagai:

$$K = k \times g$$

5. Tandatangani Hash (H) dengan Kunci Privat, : Proses ECDSA menghasilkan tanda tangan dalam bentuk pasangan nilai (r,s)

$$(r, s) = ((k \times G)_x mod\ n,$$
$$k^{-1}(h + r \times d) mod\ n)$$

B. *Verifikasi*

Proses verifikasi yang dilakukan dengan menggunakan algoritma ECDSA SECP256K1 dan fungsi *hash* BLAKE2b, sebagai berikut :

1. Sistem menerima dokumen yang sudah ditandatangani, kunci publik dari penandatangan, dan tanda tangan digital yang dihasilkan.
2. Hashing Ulang Dokumen dengan BLAKE2b

$$H'=H(T1\|T2\|\cdots\|Tn)$$

3. Hash baru (H') dihasilkan dari dokumen yang telah di-*hash* ulang
4. Melakukan verifikasi tanda tangan menggunakan kunci publik dan tanda tangan digital.

$$H'=H(D)$$

Mehitung Hash Dokumen

$$e = H'(D) mod\ n$$

n Order dari kurva (jumlah titik dalam kurva elliptic).

$$s^{-1} = s^{-1}\ mod\ n$$

Menghitung Inverse dari s

$$\mu_1 = e \times s^{-1}\ mod\ n$$
$$\mu_2 = e \times s^{-1}\ mod\ n$$

Menghitung μ_1 dan μ_2

Menghitung Titik (x, y)

$$(x, y) = \mu_1 \times G + \mu_2 \times Q$$

G titk generator kurva
Q kunci publik penanda tangan

Mendapatkan Koordinat x

$$v = x\ mod\ n$$

Tanda tangan dianggap valid jika

$$v \equiv r\ mod\ n$$

IV. PENGUJIAN

A. *Pengujian Authentikasi Dokumen Menggunakan Tanda Tangan Digital*

Pengujian authentikasi pada dokumen tipe PDF sebagai berikut,

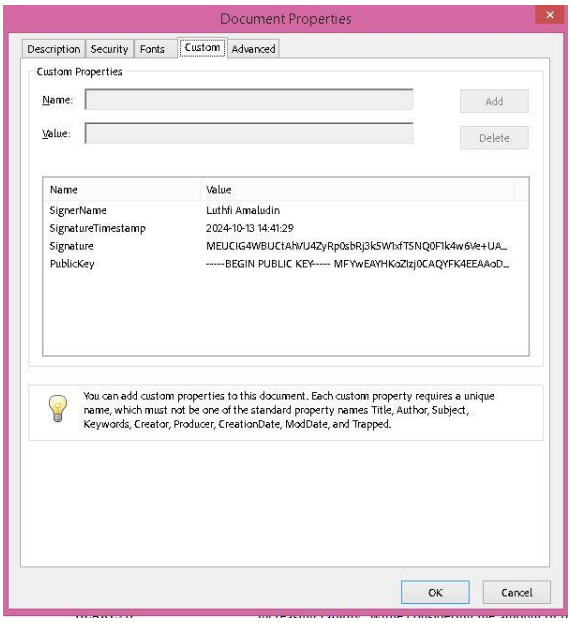
```
Digital Signature System
1. Tanda Tangan
2. Verifikasi
3. Keluar
Masukkan pilihan (1-3): 1
Enter the path to the document: /content/10.5368
Detected MIME type: application/pdf
Detected file type: pdf
Masukkan nama penanda tangan: Luthfi Amaludin

Document berhasil ditanda tangan!
Penandatangan: Luthfi Amaludin
Signature: MEUCIG4WBUCtAhVU4ZyRp0sbRj3k5W1xfTSNQ
Public Key: -----BEGIN PUBLIC KEY-----
MFYwEAYHKoZIzj0CAQYFK4E...
Timestamp: 2024-10-13 14:41:29
Signed document saved as: /content/10.53608-estu
Proses tanda tangan: 0.62 seconds
```

Gambar 3 Proses Penandatanganan file PDF

pISSN: 2252-486X
eISSN: 2548-4710

Gambar 3 menunjukkan proses dari penandatanganan file dengan tipe PDF, ketika proses tanda tangan selesai akan menambahkan _signed pada nama file. Tanda tangan tersebut dapat dilihat dala file PDF pada bagian *Document Properties* pada menu custom.



Gambar 4 *Digital Signature* pada File PDF

Pada menu *Digital Signature System* hasil dari proses verifikasi file PDF dengan nama 10.53608-estudambilisim.1086400-2304059_signed.pdf sebagai berikut

```
Digital Signature System
1. Tanda Tangan
2. Verifikasi
3. Keluar
Masukkan pilihan (1-3): 2
Enter the path to the signed document: /conter
Attempting to verify document: /content/10.536
Detected MIME type: application/pdf
Deteksi tipe file: pdf

Verification Results:
Tanda tangan valid.
Penanda Tangan: Luthfi Amaludin
Signature: MEUCIG4WBUCtAhVU4ZyRp0sbRj3k5W1xfT5
Public Key: -----BEGIN PUBLIC KEY-----
MFYwEAYHKoZIzj0CAQYFK4E...
Document ditanda tangani pada: 2024-10-13 14:4
Proses verifikasi: 0.52 seconds
```

Gambar 5 Proses Verifikasi file PDF

```
Masukkan pilihan (1-3): 1
Enter the path to the document: /cont
Detected MIME type: application/vnd.o
Detected file type: docx
Masukkan nama penanda tangan: Luthfi

Document berhasil ditanda tangan!
Penandatangan: Luthfi Amaludin
Signature: MEQCICCrFjX6Io/JSJqC22Pg4k
Public Key: -----BEGIN PUBLIC KEY----
MFYwEAYHKoZIzj0CAQYFK4E...
Timestamp: 2024-10-13 15:06:18
Signed document saved as: /content/1-
Proses tanda tangan: 0.18 seconds
```

Gambar 6 Digital Signature pada File DOCX

Penandatanganan yang dilakukan terhadap file DOCX berhasil dilakukan seperti ditunjukkan pada Gambar 4. Signature dan *Public key* berhasil diterapan file DOCX.

```
Digital Signature System
1. Tanda Tangan
2. Verifikasi
3. Keluar
Masukkan pilihan (1-3): 2
Enter the path to the signed docume
Attempting to verify document: /con
Detected MIME type: application/oct
Deteksi tipe file: None
Tipe file tidak didukung: None. Gun

Digital Signature System
1. Tanda Tangan
2. Verifikasi
3. Keluar
```

Gambar 7 *Digital Signature* pada File DOCX

Namun pada saat dilakukan verifikasi file DOCX tidak terbaca oleh sistem yang sudah dibuat ini mungkin disebabkan karena fungsi *hash* yang terlalu panjang, sementara file DOCX membatasi hanya hingga 255 bit, untuk panjang dair BLAKE2b sendiri adalah 512bit. Sehingga fungsi *hash* tersebut tidak cocok diterapkan pada file DOCX.

B. Pengujian Kinerja Proses Tanda Tangan dan Verifikasi

Proses pengujian dilakukan pada 7 sample file PDF dengan ukuran yang beragam dengan tujuan untuk mengukur kinerja waktu proses tanda tangan dan verifikasi. Tabel 1 menunjukan kinerja proses tanda tangan dan Tabel 2 menujukkan kinerja proses verifikasi.

TABEL 1
KINERJA PROSES TANDA TANGAN

No	Nama	Kecepatan
1	10.53608-estudambilisim.1086400-2304059.p	0.62
2	151_Merkurius-arteii_vol2_no4_jul2024_h102-109.pdf	0.65
3	20.06.305_jurnal_eproc.pdf	4.69
4	2787-6200-2-PB.pdf	0.86
5	44_457_Naskah_Publikasi_386-393.pdf	0.64
6	53-Article Text-129-1-10-20210219.pdf	0.95
7	679-Article Text-2625-1-10-20230317.pdf	0.82

TABEL 2
KINERJA PROSES VERIFIKASI

No	Nama	Kecepatan
1	10.53608-estudambilisim.1086400-2304059_signed.pdf	0.52
2	151_Merkurius-arteii_vol2_no4_jul2024_h102-109_signed.pdf	0.62
3	20.06.305_jurnal_eproc_signed.pdf	5.59
4	2787-6200-2-PB_signed.pdf	0.64
5	44_457_Naskah_Publikasi_386-393_signed.pdf	0.57
6	53-Article Text-129-1-10-20210219_signed.pd	0.62
7	679-Article Text-2625-1-10-20230317_signed.pdf	0.80

Kinerja proses verifikasi dari segi kecepatan lebih cepat dibandingkan dengan proses tanda tangan, ini disebabkan verifikasi tanda tangan menggunakan kunci publik melibatkan operasi yang lebih sederhana dibandingkan proses tanda tangan, karena hanya membandingkan hasil hash yang sudah ada dan mengecek validitas tanda tangan dengan kunci publik. Sedangkan proses tanda tangan melibatkan operasi kriptografi kompleks, termasuk kalkulasi titik pada kurva eliptik, yang memerlukan lebih banyak sumber daya.Fungsi *hash* pada proses tanda tangan, dokumen harus di-*hash* terlebih dahulu sebelum ditandatangani, sedangkan dalam verifikasi, hash ulang dilakukan dan dibandingkan dengan hash yang telah disimpan. Pada proses verifikasi, karena hash sudah dihasilkan pada saat tanda tangan, tugas utama adalah memvalidasi tanda tangan terhadap hash yang sudah ada, yang lebih cepat daripada membuat hash baru dan menghasilkan tanda tangan.

V. KESIMPULAN

Penerapan kombinasi algoritma ECDSA dan fungsi *hash* BLAKE2b dalam proses tanda tangan digital dan verifikasi dokumen menunjukkan hasil yang signifikan. Hal ini disebabkan oleh sifat operasional yang berbeda antara kedua proses tersebut. Proses verifikasi hanya melibatkan validasi hasil hash dan tanda tangan yang telah ada, yang merupakan operasi yang lebih sederhana dibandingkan dengan proses penandatanganan. Kecepatan yang ditawarkan oleh fungsi hash BLAKE2b, yang diakui lebih cepat dari SHA-3, berkontribusi pada efisiensi keseluruhan sistem. Selain itu, algoritma ECDSA memberikan tingkat keamanan yang tinggi dalam memastikan keaslian dan integritas dokumen.

Disarankan untuk mengeksplorasi algoritma digital signature dan hasing yang lebih sesuai untuk jenis dokumen tertentu, seperti file DOCX yang memiliki batasan *hashing* 255 bit.

REFERENSI

[1] A. Lorien and T. Wellem, 'Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature', *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 4, pp. 663–671, 2021, doi: 10.29207/resti.v5i4.3316.

[2] I. Afrianto, A. Heryandi, A. Finandhita, and S. Atin, 'Prototype of E-Document Application Based on Digital Signatures to Support Digital Document Authentication', *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 879, no. 1, 2020, doi: 10.1088/1757-899X/879/1/012042.

[3] Sugiyatno and P. D. Atika, 'Digital Signature Dengan Algoritma Sha-1 Dan Rsa Sebagai Autentikasi', *J. Cendikia*,

pISSN: 2252-486X
eISSN: 2548-4710

vol. 16, no. 2, pp. 74–83, 2018.

[4] L. Juliana Pangaribuan, C. Indra Cahyadi, J. Banjarnahor, B. Barus, and B. N. Siahaan, 'KLIK: Kajian Ilmiah Informatika dan Komputer Strategi Otentikasi Dokumen Pada Email Menggunakan Digital Signature dengan Algoritma Schnorr', *Media Online*, vol. 3, no. 4, pp. 384–392, 2023, [Online]. Available: https://djournals.com/klik

[5] A. Apriliani, N. A. Hasibuan, and D. P. Utomo, 'Implementasi Algoritma SHA-3 Dan ElGamal Untuk Otentikasi Piagam Penghargaan Berbasis Digital Signature', *SNASTIKOM Semin. Nas. Teknol. Inf. Komun.*, vol. 9, no. 1, pp. 157–164, 2022.

[6] M. F. Ramadhan, 'Aplikasi Pengesahan Multi Dokumen Dengan Tanda Tangan Digital Secara Dinamis', *J. Ilm. Sain dan Teknol.*, vol. 2, pp. 301–314, 2024.

[7] E. Wahyudi, M. M. Efendi, M. Subli, A. Subki, and M. R. Alfian, 'Penerapan Digital Signature Scheme Dengan Metode Schnorr Authentication', *Explore*, vol. 10, no. 1, p. 23, 2020, doi: 10.35200/explore.v10i1.360.

[8] A. Ismail, V. A. H. F, and A. T. F, 'Sistem Tanda Tangan Digital Menggunakan SHA-3 dan ECDSA', *Unistek*, vol. 10, no. 2, pp. 84–93, 2023.

[9] N. Arwah, A. Aminuddin, and S. Arifianto, 'Implementasi Tanda Tangan Digital menggunakan ECDSA (Studi Kasus: Jurnal Tipe File pdf)', *J. Repos.*, vol. 3, no. 3, pp. 321–330, 2024, doi: 10.22219/repositor.v3i3.31069.

[10] V. H. Zulian and P. Purwanto, 'Implementasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritme ElGamal Pada Dokumen Di Balai Pendidikan dan Pelatihan Penerbangan BP3 Curug Berbasis Web', *Senafti*, vol. 1, no. 1, pp. 386–393, 2022.

[11] F. Az-Zahra, R. Marwati, and R. Sispiyati, 'Implementasi QR Code dengan Algoritma Secure Hash Algorithm (SHA)-256 dan Rivest Shamir Adleman (RSA) yang Ditingkatkan untuk Autentikasi Dokumen Digital', *J. EurekaMatika*, vol. 12, no. 1, pp. 11–22, 2024, [Online]. Available: https://ejournal.upi.edu/index.php/JEM

[12] I. P. Y. Suantara, I. P. Satwika, and K. Q. Fredlina, 'Perbandingan Kinerja Waktu Algoritma ECDSA, EdDSA, RSA, Dan Implementasinya Pada Sistem Multi-Signature Dokumen Pdf', *J. Tek. Inform. dan Sist. Inf.*, vol. 11, no. 1, pp. 85–98, 2024, [Online]. Available: http://jurnal.mdp.ac.id

[13] N. A. Fitriani, A. Aminuddin, and S. Arifianto, 'Perbandingan Kinerja Algoritma Elliptic Curve Digital Signature Algorithm (ECDSA) Menggunakan Fungsi Hash Secure Hash Algorithm (SHA-1) dan Keccak pada Tanda Tangan Digital', *J. Repos.*, vol. 3, no. 3, pp. 331–342, 2024, doi: 10.22219/repositor.v3i3.31071.

[14] Arnaldy, 'Analisis Integritas Dokumen Digital Pada Aplikasi Digisign UTD PNJ Menggunakan Tanda Tangan Digital', *Repository.Pnj.Ac.Id*, no. Md, 2020, [Online]. Available: https://repository.pnj.ac.id/6650/2/1807422025 - Muhammad Dimas Yudha - Paper Jurnal.pdf

[15] J. P. Aumasson, S. Neves, Z. Wilcox-O'Hearn, and C. Winnerlein, 'BLAKE2: Simpler, smaller, fast as MD5', *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7954 LNCS, pp. 119–135, 2013, doi: 10.1007/978-3-642-38980-1_8.