Pengecekan Keaslian *File* PDF Dengan Teknik *Digital Signature* Menggunakan Algoritma BLAKE2s dan AES

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 pada
Jurusan Teknik Informatika

Oleh:
Muhammad Naufal Kateni
NIM: 09021281924062

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2023

LEMBAR PENGESAHAN SKRIPSI

PENGECEKAN KEASLIAN *FILE* PDF DENGAN TEKNIK *DIGITAL SIGNATURE* MENGGUNAKAN ALGORITMA BLAKE2S DAN AES

Oleh:

Muhammad Naufal Kateni

09021281924062

Palembang, 18 Juli 2023

Pembimbing I	Pembimbing II,
Osvari Arsalan, S.Kom., M.T.	Junia Kurniati, M.Kom.
NIP. 198806282018031001	NIP. 1671046606890018

Mengetahui,

Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.

NIP. 197812222006042003

Scanned with CamScanner

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari Senin tanggal 17 Juli 2023 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

Nama : Muhammad Naufal Kateni
NIM : 09021281924062
Judul : Pengecekan Keaslian *File* PDF dengan Teknik *Digital Signature* Menggunakan Algoritma BLAKE2s dan AES

dan dinyatakan **LULUS.**

1. Ketua Penguji

   Kanda Januar Miraswan, M.T. .....
   NIP. 199001092019031012

2. Pembimbing I

   Osvari Arsalan, S.Kom., M.T. .....
   NIP. 198806282018031001

3. Pembimbing II

   Junia Kurniati, M.Kom. .....
   NIP. 1671046606890018

4. Penguji

   Mastura Diana Marieska, M.T. .....
   NIP.198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

Scanned with CamScanner

iii

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Muhammad Naufal Kateni

NIM : 09021281924062

Program Studi: Teknik Informatika

Judul Skripsi : Pengecekan Keaslian File PDF Dengan Teknik Digital Signature Menggunakan Algoritma BLAKE2s dan AES

Hasil Pengecekan *Software iThenticate/Turnitin* : 17%

Menyatakan bahwa laporan penelitian saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan penelitian ini, maka saya bersedia menerima sanksi akademik Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 27 Juli 2023

Muhammad Naufal Kateni,

NIM. 09021281924062

Scanned with CamScanner

iv

Motto:

- "Jangan Lupa Titik Koma!" – Sandhika Galih
- "Don't change so people will like you. Be yourself and the right people will like the real you" – Houtarou Oreki

Kupersembahkan karya tulis ini kepada:

- Kedua Orang Tua dan Saudaraku
- Teman-Teman Seperjuangan
- Fakultas Ilmu Komputer
- Universitas Sriwijaya

CHECKING THE PDF FILE AUTHENTICITY WITH DIGITAL SIGNATURE USING BLAKE2S AND AES ALGORITHM

By :

Muhammad Naufal Kateni
09021281924062

ABSTRACT

Digital signature is a cryptographic technique to maintain and check the authenticity of data or information. In this research, the algorithms used are the BLAKE2s algorithm as a hash algorithm and the AES algorithm as a decryption encryption algorithm. In this research, the data or information to be checked is in the form of PDF files that have varying file sizes. In the BLAKE2s algorithm, the public key is used as a hash randomizer and in the AES algorithm, AES 128 is used with a private key as an identifier of the data to be encrypted or decrypted. In testing, the Avalanche Effect method is used, which is a check for changes in the results of the input text that is changed slightly in cryptographic operations will change drastically or not. Based on the results of research on the overall file size, the results obtained are above 87% which is considered very good.

Keywords: Cryptography, Digital Signature, BLAKE2s, AES, PDF File

PENGECEKAN KEASLIAN *FILE* PDF DENGAN TEKNIK *DIGITAL SIGNATURE* MENGGUNAKAN ALGORITMA BLAKE2S DAN AES

Oleh :

Muhammad Naufal Kateni
09021281924062

ABSTRAK

Tanda tangan digital adalah teknik kriptografi untuk menjaga dan mengecek keaslian suatu data atau informasi. Pada penelitian ini algoritma yang digunakan adalah algoritma BLAKE2s sebagai algoritma *hash* dan algoritma AES sebagai algoritma enkripsi dekripsi. Pada penelitian ini, data atau informasi yang akan di cek keasliannya berupa *file* PDF yang memiliki ukuran *file* yang bervariasi. Pada algoritma BLAKE2s digunakan kunci publik sebagai pengacak *hash* dan pada algoritma AES digunakan AES 128 dengan kunci pribadi sebagai pengidentifikasi dari data yang ingin dienkripsi maupun dekripsi. Pada pengujian digunakan metode *Avalanche Effect* yang merupakan pengecekan akan perubahan hasil dari teks masukan yang diubah sedikit pada operasi kriptografi akan berubah drastis atau tidak. Berdasarkan hasil penelitian terhadap ukuran *file* secara keseluruhan hasil yang didapat adalah diatas 87% yang terbilang sangat baik.

Kata Kunci: Kriptografi, Tanda Tangan Digital, BLAKE2s, AES, *File* PDF

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala limpahan rahmat, karunia, dan hidayah-Nya, sehingga penulis dapat menyelesaikan penulisan tugas akhir ini dengan judul "Pengecekan Keaslian *File* PDF dengan Teknik *Digital Signature* Menggunakan Algoritma BLAKE2s dan AES" sebagai salah satu syarat untuk meraih gelar Sarjana S1 Teknik Informatika di Universitas Sriwijaya.

Dalam menyelesaikan penulisan tugas akhir ini, terdapat banyak pihak yang terlibat baik dalam bentuk bantuan, bimbingan, dan dukungan kepada penulis baik secara langsung maupun tidak. Maka dari itu, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tua dan saudara yang telah memberikan dukungan dan dorongan selama pengerjaan tugas akhir.
2. Alm. Bapak Jaidan Jauhari, S.Pd. M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
3. Ibu Alvi Syahrini Utami, M.Kom., selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya
4. Bapak Osvari Arsalan, S.Kom., M.T. selaku pembimbing I dan Ibu Junia Kurniati, M.Kom. selaku pembimbing II, yang telah membimbing penulis selama pengerjaan tugas akhir.
5. Bapak Kanda Januar Miraswan, M.T. selaku ketua penguji dan Ibu Mastura Diana Marieska, M.T. selaku penguji tugas akhir.
6. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Aditiya Ramadhan dan Rizky Azizi, teman terdekat yang telah menjadi teman sejak semester awal hingga akhir dan selalu bersama mulai dari belajar, tugas kelompok, proyek, main, hingga bolos ketika ada kuis pada mata kuliah kalkulus.

8. Hardian Theja, Irvan Arvandi, Kurniawan Cristianto, Muqsith Giga, Ricky Alturino, dan Vinito Zummizola selaku teman seperjuangan tugas akhir yang selalu nongkrong baik di basecamp atau di kampus untuk bermain, bercerita, dan saling membantu perihal tugas akhir.
9. Rekan-rekan seperjuangan skripsi yaitu Andri, Ajai, Nanda, Dimas, Indra, Totok, Friska, Debo, Wafi, Caca, Rachel, dan Yuyun yang telah membantu penulis dalam hal apa pun.
10. Pihak-pihak lainnya yang telah membantu penulis yang tidak bisa disebutkan satu persatu.

Penulis menyadari bahwa dalam penulisan tugas akhir ini masih banyak kekurangan dikarenakan adanya keterbatasan baik dalam pengetahuan maupun pengalaman, maka dari itu penulis menerima masukan berupa kritik dan saran yang dapat mengembangkan penelitian ini. Akhir kata semoga tugas akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, 21 Juli 2023

Muhammad Naufal Kateni

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR ISTILAH, SINGKATAN, DAN LAMBANG

Algoritma	:	Sebuah tata cara untuk menyelesaikan masalah matematis dengan langkah-langkah yang telah ditentukan
AES (*Advanced Encryption Standard)*	:	Algoritma cipher blok kunci simetris pengembangan dari algoritma *Data Encryption Standard* yang dikembangkan oleh Joan Daemen dan Vincent Rijment
AddRoundKey	:	Ronde pada proses enkripsi dan dekripsi algoritma AES dimana pada ronde ini terjadi proses XOR antara matriks kunci pribadi dengan matriks *cipher* blok (*plaintext* pada enkripsi dan *ciphertext* pada dekripsi)
Array	:	Sekumpulan data yang tersusun secara linear dapat berjenis sama maupun berbeda
Avalanche Effect	:	Pengecekan rasio perubahan hasil dari teks masukan yang diubah sedikit pada operasi kriptografi akan berubah drastis atau tidak
Bernstein's ChaCha	:	Algoritma *cipher* alir yang dikembangkan oleh Daniel J. Bernstein
Bit	:	Satuan kecepatan transfer data terkecil dalam sistem informasi
BLAKE	:	Fungsi *hash* yang dibuat berdasarkan Bernstein's ChaCha cipher alir
BLAKE2	:	Fungsi *hash* yang dibuat berdasarkan fungsi *hash* BLAKE yang dikembangkan oleh Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, dan Christian Winnerlein
BLAKE2b	:	Fungsi *hash* varian dari BLAKE2 yang memiliki panjang 64 *bytes*
BLAKE2s	:	Fungsi *hash* varian dari BLAKE2 yang memiliki panjang 32 *bytes*
Blok	:	Kumpulan *byte* pada matriks
Blowfish	:	Algoritma *cipher* blok kunci simetris

		yang dikembangkan oleh Bruce Scheiner
Byte	:	Kumpulan beberapa bit dimana 1 *byte* terdiri atas 8 bit
Cipher	:	Algoritma untuk melakukan proses enkripsi dan dekripsi
Cipherkey	:	Kunci rahasia yang digunakan untuk melakukan proses enkripsi dan dekripsi
Ciphertext	:	Data hasil proses enkripsi
Cipher alir	:	Algoritma yang melakukan konversi teks per 1 *byte* pada suatu waktu
Cipher blok	:	Data per baris pada matriks
Compress	:	Proses utama yang digunakan untuk mengubah nilai kondisi *hash* selama proses *hash* sedang berlangsung
Counter	:	Nilai yang bersifat dinamis bertujuan untuk membantu operasi matematis yang sedang dilakukan
Dekripsi	:	Metode dekode data agar komputer dapat membaca kembali data yang telah dienkripsi
DES (*Data Encryption Standard*)	:	Algoritma kunci simetris yang digunakan untuk melakukan proses enkripsi data
Digital Signature	:	Teknik kriptografi untuk menjaga dan mengecek keaslian suatu data atau informasi
DOCX (*Office Open XML Document*)	:	Jenis yang digunakan untuk membuat dan membuka Microsoft Word versi 2007 keatas
Enkripsi	:	Metode pengkodean data agar komputer tidak dapat membaca data
Exhaustive key search	:	Jenis serangan kriptografi dimana penyerang akan mencoba untuk menebak kunci kriptografi dengan cara menebak secara acak
Flag	:	Aturan opsional yang diberikan pada fungsi *hash* untuk mengubah cara kerja dari fungsi *hash* itu sendiri

File	:	Kumpulan data dan informasi yang saling berhubungan
Galois Field Matrix	:	Matriks yang memiliki nitai tetap yang telah ditentukan oleh pengembang algoritma AES
Generic attack	:	Suatu aksi dimana seseorang berusaha untuk mengeksploitasi kelemahan dari algoritma kriptografi untuk mendapatkan akses terhadap informasi yang bersifat sensitif
Hash	:	Sebuah operasi yang menerima masukkan berupa teks sepanjang berapapun dan mengubahnya menjadi teks terkompresi dengan panjang tetap
Hash pohon	:	Salah satu turunan dari operasi *hash* yang memiliki konsep struktur data
Heksadesimal	:	Sistem angka berbasis 16 yang terdiri dari angka 0-9 dan huruf A sampai F
Herding	:	Jenis serangan rekayasa sosial dimana penyerang akan mengumpulkan beberapa orang sebagai target dan memengaruhi mereka untuk melakukan suatu aksi dengan memberikan kesan jika sudah banyak orang yang telah melakukan aksi tersebut
Initialization Vector	:	Data acak maupun setengah acak yang membantu proses enkripsi agar hasil enkripsi terlihat unik
Input	:	Data yang di masukkan pada suatu sistem
Inverse S-Box (*Inverse Substitution Box*)	:	Nilai tetap yang telah ditentukan dan digunakan untuk proses *InvSubBytes* pada proses dekripsi algoritma AES
InvMixColumns	:	Ronde proses dekripsi algoritma AES dimana pada ronde ini terjadi perkalian matriks antara *galois field matrix InvMixColumns* dengan matriks *cipher* blok
InvShiftRows	:	Ronde proses dekripsi algoritma AES dimana pada ronde ini terjadi pergeseran *byte* pada matriks *ciphertext* sebanyak n

		kali (sesuai letak blok) ke kanan
InvSubBytes	:	Ronde proses dekripsi algoritma AES dimana pada ronde ini terjadi pergantian *bytes* antara nilai matriks *ciphertext* dengan tabel *Inverse* S-Box
Kriptografi	:	Teknik untuk mengamankan data atau informasi
Length extension	:	Jenis serangan kriptografi dimana penyerang mengeksploitasi kelemahan dari suatu fungsi *hash*
Long-message second preimages	:	Jenis serangan kriptografi fungsi *hash* dimana penyerang mencoba untuk menebak teks masukkan yang memiliki hasil *message digest* yang sama dengan teks masukan yang dimasukkan oleh penyerang
MD5 (*Message Digest* 5)		Fungsi *hash* yang menghasilkan data sepanjang 128 bit
Message digest	:	Kumpulan angka dan huruf acak hasil dari fungsi *hash* yang digunakan untuk mengecek kesalahan data
MixColumns	:	Ronde proses enkripsi algoritma AES dimana pada ronde ini terjadi perkalian matriks antara *galois field matrix MixColumns* dengan matriks *cipher* blok
Output	:	Data yang dihasilkan dari suatu sistem
Padding	:	Penambahan kata seperti (spasi, garis bawah, dll) pada suatu teks baik di awal maupun diakhir teks tersebut hingga panjang teks mencapai angka yang ditentukan
PDF (*Portable Document Format*)	:	Jenis *file* yang bertujuan untuk membuka *file* berjenis dokumen dengan cara mempertahankan tata letak dan format aslinya
Penguncian MAC	:	Proses pembangkitan kunci rahasia yang digunakan pada autentikasi data
Perkalian dot	:	Perkalian skalar antara dua buah blok

Permutasi	:	Operasi untuk melakukan proses pengaturan angka dalam urutan tertentu
Personalization	:	Teknik kriptografi dengan menambahkan data acak pada teks masukan yang bertujuan untuk membuat teks bersifat unik
Plaintext	:	Teks yang ingin dilakukan proses enkripsi terhadap algoritma enkripsi
Round constant	:	Data tetap yang digunakan untuk membantu proses enkripsi dan dekripsi
RSA (Rivest Shamir Adleman)	:	Algoritma kunci publik yang biasanya digunakan untuk melakukan proses transmisi data yang aman
S-Box (*Substitution Box*)		Nilai tetap yang telah ditentukan dan digunakan untuk proses *SubBytes* pada proses enkripsi algoritma AES
Salting	:	Teknik kriptografi dengan menambahkan data acak pada teks masukan yang bertujuan untuk meningkatkan keamanan
Search engine	:	Program yang bertujuan untuk mencari suatu informasi menggunakan kata kunci yang diberikan oleh pengguna
Serpent	:	Algoritma *cipher* blok yang dikembangkan oleh Ross Anderson, Eli Biham, dan Lars Knudsen
SHA-1 (*Secure Hash Algorithm* 1)	:	Fungsi *hash* yang menerima masukkan dan menghasilkan data sepanjang 160 bit
SHA-256 (*Secure Hash Algorithm* 256)	:	Fungsi *hash* yang menerima masukkan dan menghasilkan data sepanjang 256 bit
ShiftRows	:	Ronde proses enkripsi algoritma AES dimana pada ronde ini terjadi pergeseran *byte* pada matriks *cipher* blok sebanyak n kali (sesuai letak blok) ke kiri
State	:	Kondisi data yang sedang diproses pada suatu waktu
SubBytes	:	Ronde proses enkripsi algoritma AES dimana pada ronde ini terjadi pergantian *bytes* antara nilai matriks *cipher* blok

		dengan tabel S-Box
XOR (*Exclusive* OR)	:	Operasi perbandingan terhadap dua angka biner dimana hasilnya akan menjadi 1 jika kedua angka biner berbeda dan 0 jika angka biner sama

DAFTAR LAMPIRAAN

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab I pendahuluan ini akan membahas tentang latar belakang diambilnya topik "Pengecekan Keaslian *File* PDF Dengan Teknik *Digital Signature* Menggunakan Algoritma BLAKE2s dan AES". Bab ini juga membahas tentang rumusan masalah yang dihadapi selama penelitian berlangsung, tujuan dari penelitian, manfaat dari penelitian, batasan masalah untuk memperkecil ruang lingkup penelitian, sistematika penulisan, dan kesimpulan dari topik yang sedang diteliti.

1.2 Latar Belakang Masalah

Secara umum untuk mengamankan data atau informasi selama penyimpanan atau pengiriman, digunakan teknik enkripsi dan dekripsi dari algoritma kriptografi (Sinaga et al., 2022). Keamanan data yaitu langkah untuk menjaga atau melindungi data dari hal-hal yang tidak diinginkan seperti penyalahgunaan yang dibuat oleh pihak yang tidak berwenang baik pihak asing atau pihak di dalam lembaga tersebut. Pada zaman digital, komunikasi dengan jaringan menjadi penting dimana komunikasi dengan media jaringan membuat proses yang terjadi menjadi lebih efektif dan efisien. Dalam merancang sebuah keamanan sistem komputer, pastilah dibutuhkan pula metode pengamanan untuk data atau *file* di dalamnya. Apabila informasi diletakkan di dalam perangkat komputer yang digunakan untuk umum dan bersama, maka data tersebut sangat rawan untuk

dimanipulasi (Risna et al., 2022). Tindak pidana manipulasi informasi elektronik merupakan kejahatan penipuan, pemalsuan, atau rekayasa yang dilakukan menggunakan komputer atau jaringan internet. Berkembangnya teknologi di era globalisasi membuat banyak celah seseorang melakukan tindak pidana/kejahatan termasuk di dalamnya tindak pidana manipulasi informasi elektronik (Marpaung, 2020).

Salah satu langkah keamanan adalah dengan menerapkan tanda tangan digital (*digital signature*) pada dokumen digital. Tanda tangan digital terdiri dari informasi elektronik yang berkaitan dengan informasi elektronik lainnya sebagai sistem verifikasi atau otentikasi (Budiarti et al., 2020). Tanda tangan digital dengan menggunakan kriptografi untuk menandatangani *file* secara digital. Tanda tangan digital juga merupakan hasil penerapan teknik kriptografi pada konten *file* asli. Kriptografi dimaksudkan untuk memastikan bahwa informasi rahasia yang dikirim melalui internet tidak dapat diketahui dan digunakan oleh orang lain atau pihak yang seharusnya tidak memiliki akses. Tanda tangan digital harus memiliki fungsi yang sama dengan tanda tangan pada umumnya (Anshori et al., 2019).

File yang hendak dikirim terlebih dahulu akan dilakukan fungsi *hash* sehingga menjadi bentuk yang ringkas yang disebut dengan *message digest*. Kemudian, *message digest* tersebut dienkripsi menggunakan algoritma kriptografi kunci publik, lalu kunci privat milik penandatangan atau pengirim *file* akan digunakan untuk melakukan enkripsi pada *message digest*. Hasil dari enkripsi inilah yang disebut sebagai tanda tangan digital (*digital signature*) (Anshori et al., 2019).

Penelitian-penelitian sebelumnya yang telah menggunakan algoritma AES dan BLAKE2s sudah banyak dilakukan begitu juga untuk membuat tanda tangan digital tetapi belum ada penelitian tanda tangan digital yang menggunakan algoritma AES dan BLAKE2s secara bersamaan. Beberapa kasus dan algoritma yang telah digunakan pada penelitian sebelumnya antara lain kasus citra digital menggunakan algoritma AES (Haris et al., 2023), kasus *caching key* menggunakan algoritma BLAKE2s (Wibowo & Nurwasito, 2022), kasus tanda tangan digital menggunakan algoritma MD5 dan *Paillier Cryptosystem* (Sinaga et al., 2022), dan kasus tanda tangan digital menggunakan algoritma RSA (Anshori et al., 2019).

Semakin banyaknya manipulasi dan pencurian data, maka dilakukan penelitian terhadap topik tanda tangan digital. Implementasi yang digunakan pada penelitian ini adalah algoritma *hashing* dengan menggunakan BLAKE2s karena masih jarang digunakan dan dapat bertahan terhadap serangan *generic attack* seperti *herding*, *long-message second preimages*, dan *length extension* (Satria et al., 2018). Untuk algoritma enkripsi dan dekripsi yang digunakan adalah algoritma AES, dikarenakan algoritma AES dapat bertahan terhadap serangan *exhaustive key search* (Asriyanik, 2017) dan kecepatan enkripsi dan dekripsi AES selalu lebih unggul dari algoritma lainnya (Priambudi & Mufti, 2023).

1.3 Rumusan Masalah

Berdasarkan latar belakang di atas, dapat disimpulkan bahwa penelitian ini akan melakukan fungsi *hash* pada *file* PDF dan hasil *hash* akan dienkripsi atau

didekripsi sehingga dapat di bandingkan dengan hasil *hash file* PDF yang asli. Oleh karena itu, rumusan masalah dapat diuraikan sebagai berikut:

1. Bagaimana cara membuat perangkat lunak yang dapat mengecek keaslian suatu *file* PDF menggunakan algoritma BLAKE2s dan AES?
2. Bagaimana tingkat kebauran nilai kriptografi dari hasil enkripsi dan *hash* yang dilakukan menggunakan algoritma BLAKE2s dan AES?
3. Bagaimana pengaruh ukuran *file* PDF terhadap hasil Avalanche Effect?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini dapat diuraikan sebagai berikut:

1. Membuat perangkat lunak yang dapat mengecek keaslian suatu *file* PDF menggunakan algoritma BLAKE2s dan AES.
2. Mengetahui tingkat kebauran nilai kriptografi dari hasil enkripsi dan *hash* yang dilakukan menggunakan algoritma BLAKE2s dan AES dengan menggunakan metode *Avalanche Effect.*
3. Mengetahui seberapa besar pengaruh ukuran *file* PDF terhadap hasil *Avalanche Effect*.

1.5 Manfaat Penelitian

Manfaat yang didapat dari penelitian dapat diuraikan sebagai berikut:

1. Menghasilkan perangkat lunak yang dapat melakukan pengecekan terdapat keaslian suatu *file* PDF.
2. Memberikan informasi dan ilmu pengetahuan tentang topik tanda tangan digital kepada para pembaca.

3. Menambah referensi penelitian terkait tanda tangan digital karena topik tanda tangan digital sendiri masih sedikit diteliti.

1.6 Batasan Masalah

Batasan masalah dari penelitian ini dapat diuraikan sebagai berikut:

1. *File* yang akan di cek keasliannya hanya *file* PDF.
2. Algoritma yang digunakan algoritma BLAKE2s dan AES.
3. Algoritma AES yang digunakan adalah AES 128 bit yang memiliki panjang kunci pribadi sebesar 32 karakter.
4. Pengamanan *file* hanya sebatas pengecekan keaslian *file* tersebut.

1.7 Sistematika Penulisan

Struktur pembuatan laporan penelitian ini mengikuti sistematika penulisan skripsi dari Fakultas Ilmu Komputer Universitas Sriwijaya yang dapat diuraikan sebagai berikut:

BAB I. PENDAHULUAN

Pada bab I memaparkan tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan dari penelitian ini.

BAB II. KAJIAN LITERATUR

Pada bab II memaparkan tentang landasan teori yang berkaitan dengan penelitian seperti teori mengenai algoritma yang digunakan dan penelitian-penelitian lain yang relevan seperti penelitian sebelumnya.

BAB III. METODOLOGI PENELITIAN

Pada bab III memaparkan tentang tahapan-tahapan yang dilakukan ketika melakukan penelitian. Selain tahapan juga memaparkan tentang metode pengembangan perangkat lunak dan manajemen proyek perangkat lunak.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab IV memaparkan tentang pengembangan perangkat lunak dalam bentuk diagram yang menjelaskan bagaimana cara kerja dari perangkat lunak itu sendiri dan rancangan antarmuka dari perangkat lunak.

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada bab V memaparkan tentang hasil dan analisis dari penelitian yang dilakukan dalam bentuk pengujian menggunakan metode *Avalanche Effect* pada *file* PDF dengan ukuran *file* yang bervariasi.

BAB VI. KESIMPULAN DAN SARAN

Pada bab VI memaparkan tentang kesimpulan yang dapat diambil setelah melakukan penelitian dan saran yang dapat ditambahkan dalam penelitian yang dapat melengkapi kekurangan dari penelitian ini.

1.8 Kesimpulan

Bab ini telah menguraikan latar belakamg dari topik yang ingin diteliti yaitu tanda tangan digital dengan *file* PDF dengan menggunakan algoritma BLAKE2s dan AES. Pada bab ini juga telah dibahas tentang rumusan masalah, tujuan penelitian, manfaat penelitian, dan batasan masalah dari topik yang ingin diteliti.

DAFTAR PUSTAKA

Abdurrachman, T., & Suteja, B. R. (2021). Pengembangan Sistem Informasi Asosiasi Jasa Konstruksi dengan Menerapkan Tanda Tangan Digital. *Jurnal Teknik Informatika Dan Sistem Informasi*, *7*(1).

Adhiwijna, A. (2019). *Hash Function Performance*.

Anshori, Y., Dodu, A. Y. E., & Wedananta, D. M. P. (2019). Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital. *Techno. Com*, *18*(2), 110–121.

Asriyanik, A. (2017). Studi Terhadap Advanced Encryption Standard (Aes) Dan Algoritma Knapsack Dalam Pengamanan Data. *SANTIKA (Jurnal Ilmiah Sains Dan Teknologi)*, *7*(1), 553–561.

Azdy, R. A. (2016). Tanda tangan digital menggunakan algoritme keccak dan RSA. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi*, *5*(3), 184–191.

Budiarti, N., Putra, Y. P., & Nurmandi, A. (2020). *Penerapan Tanda Tangan Digital sebagai Bentuk Baru Penyelenggaraan Smart Governance*.

Handoko, L. B., & Umam, C. (2022). Pengamanan File Lampiran Pada Email Berbasis TLS Menggunakan Algoritma AES dan LSB. *Seminar Nasional Inovasi Dan Pembangunan Teknologi Terapan (SENOVTEK)*, *1*, 53–61.

Haris, M., Lydia, M. S., & Sutarman, S. (2023). Pengamanan Pada Citra Digital dengan Menggunakan Modifikasi Blok Data Algoritma AES-Rijndael. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *7*(1), 444–453.

Marpaung, S. A. A. P. (2020). *Tindak Pidana Manipulasi Informasi Elektronik Dalam Usaha Transportasi Yang Menggunakan Aplikasi Berbasis Teknologi Informasi (Analisis Putusan Nomor: 797/Pid. Sus/2018/PN. Mks)*.

Muslih, M., & Handoko, L. B. (2022). PENGUJIAN AVALANCHE EFFECT PADA KRIPTOGRAFI TEKS MENGGUNAKAN AUTOKEY CIPHER. Seminar Nasional Teknologi Dan Multidisiplin Ilmu (SEMNASTEKMU), 2(1), 127–134.

Precilia, D. P., & Izzuddin, A. (2015). Aplikasi Tanda Tangan Digital (Digital Signature) Menggunakan Algoritma Message Digest 5 (MD5). *Energy-Jurnal Ilmiah Ilmu-Ilmu Teknik*, *5*(1), 14–19.

Priambudi, I., & Mufti, M. (2023). Implementasi Kriptografi dengan Metode AES-128 untuk Pengamanan File Berbasis Web pada SMP Yapipa. *SKANIKA*, *6*(1), 22–31.

Rahmawati, R., & Rahardjo, D. (2016). Aplikasi Pengamanan Data Menggunakan Algoritma Steganografi Discrete Cosine Transform dan Kriptografi AES 128 BIT pada SMK PGRI 15 Jakarta. *Jurnal Teknik Informatika Dan Sistem Informasi*, *2*(1).

Risna, R., Amaliah, Y., & Yunita, S. (2022). IMPLEMENTASI KRIPTOGRAFI PADA PENGAMANAN DATA PEMBAYARAN PIUTANG PELANGGAN MENGGUNAKAN VIGENERE CIPHER. *Sebatik*, *26*(2), 525–534.

Satria, B., Kusyanti, A., & Yahya, W. (2018). Implementasi algoritme blake2s pada json web token (jwt) sebagai algoritme hashing untuk mekanisme autentikasi layanan rest-api. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer E-ISSN*, *2548*, 964X.

Sinaga, B., Rohim, M. A., & Bu'ulolo, E. (2022). Implementasi MD5 dan Paillier Cryptosystem Untuk Membuat Tanda Tangan Digital. *Resolusi: Rekayasa Teknik Informatika Dan Informasi*, *2*(5), 187–194.

Suharya, Y. (2020). Implementasi Digital Signature Menggunakan Algoritma Kriftografi RSA Untuk Pengamanan Data Di SMK Wirakarya 1 Ciparay. *COMPUTING| Jurnal Informatika*, *7*(1), 21–29.

Wibowo, R. R., & Nurwasito, H. (2022). Implementasi Algoritma Blake2s untuk Mekanisme Caching Key Value pada REST API. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer E-ISSN*, *2548*, 964X.

Widarma, A. (2016). Kombinasi Algoritma AES, RC4 dan Elgamal Dalam Skema Hybrid Untuk Keamanan Data. *CESS (Journal of Computer Engineering, System and Science)*, *1*(1), 1–8.

Wiguna, B. S. (2018). *Implementasi Algoritme BLAKE2S Pada JSON Web Token Sebagai Algoritme Hashing Untuk Mekanisme Autentikasi Layanan REST API*. Universitas Brawijaya.