UNIVERSITAS BUDI LUHUR

SENAFTI
SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI
VOL. 1 NO. 1 SEPTEMBER 2022
E-ISSN: 2962-8628

PROSIDING

SEMINAR NASIONAL MAHASISWA FAKULTAS TEKNOLOGI INFORMASI (SENAFTI)

PERANAN ARTIFICIAL INTELLIGENCE
YANG CERDAS BERBUDI LUHUR
DALAM MENGHADAPI ERA SOCIETY 5.0

CYBER SECURITY

Supported by :
Ngampooz

STEERING COMMITE

Pelindung
Dr. Ir. Wendi Usino, M.Sc., M.M

Penanggung Jawab
Dr. Ir. Deni Mahdiana, S.Kom, M.M., M.Kom

Ketua Pelaksana
Dr. Rusdah, M.Kom

Sekretaris
Retno Wulandari, S.Kom., M.Kom.

Bendahara
Noni Juliasari, S.Kom., M.Kom.

Acara
Ratna Ujian Dari, S.Kom., M.M., M.Kom.

Pengelola Makalah dan Mitra Bestari
1. Atik Ariesta, S.Kom., M.Kom.
2. Samsinar, S.Kom., M.Kom.

Pengelola Editor dan Jurnal
1. Indah Puspasari Handayani, S.Kom., M.Kom.
2. Devit Setiono, S.Kom., M.Kom.
3. Anwar Rifa'i, S.Pd, M.Pd.
4. Reva Ragam Santika, S.Kom., M.Kom.
5. Kukuh Harsanto, S.Kom., M.Kom

Pengelola Teknologi Informasi
1. Sovan Dianarto, S.Kom.
2. Dolly Virgian Shaka Yudha Shakti, S.Kom., M.Kom.

Pengelola Undangan dan Desain
Wasiran

REDAKSI

MITRA BESTARI

1. Dr. Ir. Achmad Solichin, S.Kom., M.T.I (Universitas Budi Luhur)
2. Anita Ratnasari, S.Kom, M.Kom (Universitas Mercu Buana)
3. Prof. Dr. Anton Satria Prabuwono, ST., SSi., M.M (Universitas Budi Luhur)
4. Dr. Ir. Arief Wibowo, S.Kom., M.Kom (Universitas Budi Luhur)
5. Arif Bramantoro, Ph.D (Universitas Budi Luhur)
6. Bima Cahya Putra, S.Kom., M.Kom. (Universitas Budi Luhur)
7. Prof. Ir. Dana Indra Sensuse, Ph.D (Universitas Indonesia)
8. Denni Kurniawan, S.T., M.T.I., Ph.D (Universitas Budi Luhur)
9. Dian Anubhakti, S.Kom., M.Kom. (Universitas Budi Luhur)
10. Dolly Virgian Shaka Yudha Sakti, S.Kom., M.Kom. (Universitas Budi Luhur)
11. Dwi Pebrianti, S.T., M.Eng., Ph.D (Universiti Budi Luhur)
12. Dr. Emy Setyaningsih, S.Si., M.Kom (Institut Sains dan Teknologi AKPRIND Yogyakarta)
13. Dr. Gandung Triyono, M.Kom (Universitas Budi Luhur)
14. Dr. Ir. Goenawan Brotosaputro, S.Kom., M.Sc (Universitas Budi Luhur)
15. Grace Gata, S.Kom., M.Kom. (Universitas Budi Luhur)
16. Dr. Ir. Hari Soetanto, S.Kom., M.Sc (Universitas Budi Luhur)
17. Hendra Cipta, M.Si (Universitas Islam Negeri Sumatera Utara Medan)
18. Hendri Irawan, S.Kom., M.T.I. (Universitas Budi Luhur)
19. Dr. Imelda, M.Kom (Universitas Budi Luhur)
20. Indra Nugraha Abdullah, Ph.D (Universitas Budi Luhur)
21. Dr. Indra, S.Kom., M.T.I (Universitas Budi Luhur)
22. Ita Novita, S.Kom., M.T.I. (Universitas Budi Luhur)
23. Dr. Ir. Iwan Setiawan, MT, MCSA, CRM. (Universitas Nusa Putra)
24. Dr. Ir. Jan Everhard Riwurohi, M.T (Universitas Budi Luhur)
25. Kelik Sussolaikah, S.Kom., M.Kom (Universitas PGRI Madiun)
26. Dr. Krisna Adiyarta M, S.Kom., M.Sc (Universitas Budi Luhur)
27. Luhur Bayuaji, S.T., M.Eng., Ph.D (Universiti Malaysia Pahang)
28. Dr. Ir. Mardi Hardjianto, M.Kom (Universitas Budi Luhur)
29. Mayanda Mega Santoni, S.Komp., M.Kom. (Universitas Pembangunan Nasional Veteran Jakarta)
30. Prof. Dr. Moedjiono, M.Sc (Universitas Budi Luhur)
31. Dr. Mohammad Syafrullah, M.Kom., M.Sc (Universitas Budi Luhur)
32. Dr. Ir. Nazori A. Z., M.T (Universitas Budi Luhur)
33. Noni Juliasari, S.Kom., M.Kom. (Universitas Budi Luhur)
34. Rizky Pradana, S.Kom., M.Kom. (Universitas Budi Luhur)
35. Rohmat Indra Borman, M.Kom. (Universitas Teknokrat Indonesia)
36. Safitri Juanita, S.Kom., M.T.I. (Universitas Budi Luhur)
37. Dr. Samidi, S.Kom., M.M., M.Kom (Universitas Budi Luhur)
38. Setyawan Widyarto, M.Sc., Ph.D (Universiti Selangor, Malaysia)
39. Dr. Sofian Lusa, S.E., M.Kom (Universitas Budi Luhur)
40. Dr. Tenia Wahyuningrum, S.Kom., M.T (Institut Teknologi Telkom Purwokerto)
41. Titin Fatimah, S.Kom., M.Kom. (Universitas Budi Luhur)
42. Dr. Ir. Utomo Budiyanto, M.Kom., M.Sc (Universitas Budi Luhur)
43. Windarto, S.Kom., M.Kom. (Universitas Budi Luhur)
44. Dr. Yan Rianto, M.Eng (Badan Riset dan Inovasi Nasional/BRIN)

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT dan hanya karena rahmat dan karunia-Nya, Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) 2022 telah terselesaikan dengan baik. Prosiding seminar ini merupakan kumpulan makalah hasil penelitian para akademisi dan peneliti yang sebelumnya telah dipresentasikan pada SENAFTI tahun 2022 yang dilaksanakan secara daring (online) pada tanggal 6 September 2022. Tema SENAFTI Tahun 2022 adalah "Peranan Artificial Intelligence yang Cerdas Berbudi Luhur Dalam Menghadapi Era Society 5.0"

Penyusunan prosiding ini dimaksudkan untuk penyebarluasan hasil-hasil penelitian dan kajian dalam bidang teknologi informasi. Selain itu, penyusunan prosiding ini juga dimaksudkan agar masyarakat luas dapat mengetahui berbagai informasi terkait dengan penyelenggaraan SENAFTI. Penyusunan prosiding ini dibagi menjadi 4 (empat) buku yaitu:

1. Buku 1 - Cyber Security
2. Buku 2 – Artificial Intelligence
3. Buku 3 – Programming
4. Buku 4 – Information System

Pada kesempatan ini kami menyampaikan terima kasih yang sebesar-besarnya kepada para akademisi dan peneliti atas hasil karya dan sumbangan pemikiran yang dipresentasikan dalam bentuk makalah dan presentasi ilmiah. Juga kami sampaikan terima kasih kepada para mitra bestari yang telah mereview semua makalah sehingga kualitas isi dari makalah dapat terjaga dan dipertanggungjawabkan. Tak lupa kepada semua pihak yang telah memberikan dukungan bagi terselenggaranya SENAFTI dan atas tersusunnya prosiding ini. Harapan kita bersama, semoga prosiding ini dapat menambah khasanah pengembangan ilmu pengetahuan dan teknologi informasi di Indonesia.

Jakarta, September 2022

Tim Penyusun

IMPLEMENTASI TANDA TANGAN DIGITAL (DIGITAL SIGNATURE) MENGGUNAKAN ALGORITME ELGAMAL PADA DOKUMEN DI BALAI PENDIDIKAN DAN PELATIHAN PENERBANGAN (BP3) CURUG BERBASIS WEB

Vicky Hernando Zulian[1*], Purwanto Purwanto[2]

[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: [1*]vickyhernando0@gmail.com, [2]purwanto@budiluhur.ac.id
(* : corresponding author)

Abstrak- Dengan semakin majunya perkembangan teknologi dibidang internet, dokumen tidak hanya diterbitkan dalam bentuk cetak saja tetapi dokumen kini bisa juga dibuat dalam bentuk sebuah digital. Dokumen dalam bentuk digital rentan akan kemungkinan modifikasi, dan sulit akan membuktikan keasliannya. Tanda tangan digital bisa digunakan untuk mengatasi masalah keaslian dokumen. Dengan memanfaatkan *digital signature* menggunakan metode kriptografi akan memungkinkan dapat mengatasi keabsahan suatu data dokumen. Tanda tangan digital menggabungkan dua algoritma kriptografi sekaligus dalam implementasinya. Algoritma pertama adalah algoritma menggunakan fungsi *hash* untuk membentuk *message digest* dari sebuah dokumen (teks). Algoritma Elgamal dan SHA-256 dapat digabungkan dengan baik dalam membuat sebuah *digital signature.* Untuk membuat *digital signature* yaitu dengan menggunakan fungsi *hash*. Algoritma yang digunakan yaitu *Secure Hash Algorithm* (SHA-256) yang memberikan hasil *message digest*, hasil dari fungsi *hash* tersebut kemudian dienkripsi dengan menggunakan algoritme ElGamal. Penelitian ini menunjukan bahwa *digital signature* menggunakan SHA-256 dan algoritme ElGamal dapat memberikan keamanan dokumen. Penelitian ini menghasilkan file yang disisipkan tanda tangan digital tidak berubah. Ukuran dokumen asli dengan ukuran dokumen setelah disisipkan adalah sama. Pada penyisipan tanda tangan digital dan verifikasi *file* relatif cepat, sehingga dapat mencegah pemalsuan dokumen dari orang yang tidak bertanggung jawab dan dapat menjamin keabsahan atau keaslian suatu dokumen tersebut.

Kata Kunci: *digital signature*, elgamal, fungsi *hash, tanda tangan digital.*

IMPLEMENTATION OF DIGITAL SIGNATURE USING THE ELGAMAL ALGORITHM ON DOCUMENTS AT THE FLIGHT EDUCATION AND TRAINING CENTER (BP3) CURUG WEB-BASED

Abstract- *With the advancement of technological developments in the internet, documents are not only published in print but now documents can also be made in digital form. Documents in digital form are vulnerable to possible modification, and it is difficult to prove their authenticity. Digital signatures can be used to resolve document authenticity issues. By utilizing digital signatures using cryptographic methods, it will be possible to overcome the validity of a document data. Digital signatures combine two cryptographic algorithms at once in their implementation. The first algorithm is an algorithm that uses a hash function to form a message digest from a document (text). Elgamal algorithm and SHA-256 can be combined well in creating a digital signature. To create a digital signature is to use a hash function. The algorithm used is Secure Hash Algorithm (SHA-256) which provides message digest results, the results of the hash function are then encrypted using the ElGamal algorithm. This study shows that digital signatures using SHA-256 and the ElGamal algorithm can provide document security. This research resulted in a file inserted with a digital signature that did not change. The size of the original document and the size of the document after it is inserted are the same. The insertion of digital signatures and levers is relatively fast, so it can prevent falsification of documents from irresponsible people and can guarantee the validity or authenticity of the document.*

Keywords*: digital signature, elgamal, hash funtion.*

1. PENDAHULUAN

Dengan berkembangnya sebuah teknologi internet, dokumen kini bisa dibuat dalam bentuk digital. Sebuah dokumen digital bila di kirim melalui internet, akan rentan terhadap kemungkinan perubahan isi data, dan sulit

membuktikan keaslian dokumen tersebut. Dengan mudahnya pengirim menampik bahwa dia yang telah membuat atau mengirim dokumen tersebut [1].

Balai Pendidikan dan Pelatihan Penerbangan (BP3) adalah salah satu instansi pemerintahan yang memiliki banyak data yang bersifat rahasia dan sensitif, sehingga harus dijaga keasliannya. Mengingat banyak data seperti surat kerjasama, surat tugas dan dokumen laporan keuangan sehingga harus diamankan agar tetap terjaga keaslian data tersebut. Sudah tidak asing lagi perusahaan atau instansi pasti mempunyai dokumen penting untuk menjalankan sebuah perusahaan.

Sistem kriptografi bisa digunakan untuk mengatasi masalah keaslian suatu dokumen. Salah satu cara untuk mengatasi masalah keaslian suatu dokumen yaitu sistem kriptografi tanda tangan digital. Tanda tangan digital berfungsi untuk memastikan bahwa dokumen tersebut adalah asli dan tidak pernah termodifikasi[2]. Tanda tangan digital dapat digunakan dalam memanfaatkan sebuah teknik kriptografi. Tanda tangan basah dipindai lalu dicantumkan kedalam sebuah dokumen[3]. Tanda tangan diperoleh dari suatu nilai kriptografi yang ditentukan dari sebuah pesan dan pemilik pesan. Bila sebuah dokumen tersebut disimpan ulang, tanda tangan digital yang telah dibuat akan hilang. Hal ini mengakibatkan dokumen menjadi tidak asli lagi.

Egi dan Irawan telah melakukan penelitian menggunakan metode *Secure Hash Algorithm* (SHA-256) dan Riverst Shamir Adleman (RSA) dalam membentuk *digital signature* dan kriptografi lalu menghasilkan aplikasi tanda tangan digital untuk otentikasi sertifikat tanah digital. Algoritma RSA adalah algoritma yang tidak terlalu sederhana dan tidak juga terlalu rumit. RSA merupakan algoritma asimetri, yang berarti memiliki dua kunci, yaitu kunci publik dan kunci privat[7]. Proses pembangkitan kunci menggunakan algoritme RSA dimana akan menghasilkan *p, q, n, ø (n), e, d, Kpublik, dan Kprivat*[6]. *Digital signature* memberikan sebuah keamanan otentikasi dokumen yang digunakan pada dokumen digital tersebut.

Dalam implementasi tanda tangan yaitu dengan mencampurkan dua algoritma kriptografi. Pertama algoritma fungsi hash yang digunakan untuk pembentukan *messeage digest*. Kedua algoritme yang dipakai adalah algoritme kunci *public* ElGamal diperlukan untuk enkripsi *message digest* tersebut. Algoritme ElGamal mempunyai dua kunci rahasia berupa tiga pasang bilangan dan kunci rahasia berupa dua bilangan. Kerugian dari algoritme ini adalah ciphertext nya yang mempunyai panjang dua kali lipat dari plaintext nya[4]. Terdapat dua proses utama pada *digital ginature* tersebut, yaitu *digital signature* dan verifikasi. Proses digital signature yaitu dengan mengubah sebuah pesan atau dokumen menjadi *message digest*, dan mengenkripsinya menggunakan algoritme kunci publik ElGamal(9). Sementara, verifikasi dilakukan dengan membandingkan hasil dekripsi pesan yang diterima oleh *message digest* sebelumnya.

Menerapkan fungsi hash adalah salah satu cara unntuk membuat tanda tangan digital pada dokumen. Penelitian ini menerpakan Algoritme *Secure Hash Algorithm-256* (SHA-256) untuk mendapatkan hasil message digest [10]. Dan untuk pembentukan enkripsi tanda tangan digital menggunakan algoritme kunci publik ElGamal.

2. METODE PENELITIAN

2.1 Metode Pengumpulan Data

Tahap ini merupakan tahap dalam pengumpulan data menurut masalah yang ditentukan dari tahap sebelumnya. Beberapa tahap yang dilakukan adalah:

a. Studi Literatur

   Melalui studi literatur ini peneliti memperoleh data atau informasi dengan mengumpulkan, mempelajari dan membaca referensi baik dari buku, jurnal, makalah, internet dan berbagai sumber lainnya yang berkaitan dengan masalah yang akan dibahas yaitu implementasi digital signature khususnya menggunakan metode algoritma Elgamal dan SHA-256

b. Observasi

   Melihat langsung alur proses dokumen serta mempelajari dokumen yang digunakan untuk mengumpulkan data perancangan sistem.

2.2 Penerapan Fungsi Hash SHA-256

Proses awal digital signature adalah merubah dokumen menjadi *message digest* dengan memakai fungsi hash. SHA-256 adalah fungsi hash yang diterapkan untuk mencapai message digest dengan panjang 256 bit[5]. Berikut proses pembentukan message digest:

a. *Message padding*

   Masukan pesan pada SHA-256 dibuat menjadi sebuah blok- blok yang sama-sama memiliki panjang 512 bit. Pembagian ini menghasilkan jumlah blok terakhir menjadi lebih kecil sama dengan 512 bit. Blok yang terakhir mengalami *message padding*.

b. Tambahan Panjang Bit

Total bit dilihat di blok terakhir adalah 448 bit pada proses message padding. Untuk memperoleh 64 bit terakhir agar total panjang blok terakhir 512 bit dengan merepresentasikan M ke bilangan biner.

c. Inisialisasi Nilai Hash

Untuk menyimpan nilai inisialisasi awal dan nilai output sementara pada SHA-256 menggunakan buffer H_0, H_1, H_2, H_3, H_4, H_5, H_6, H_7. Nilai buffer untuk inisialisasi awal dalam notasi heksadesimal.

Tabel 1. *Initial Hash Value*

H_0	6a09e667
H_1	bb67ae85
H_2	3c6ef372
H_3	a54ff53a
H_4	510e527f
H_5	9b0588c
H_6	1f83d9ab
H_7	5be0cd19

2.3 Tahapan Penerapan Metode ElGamal

Algoritme ElGamal adalah algoritme kriptografi asimetris yang didasarkan pada sulitnya menyelsaikan permasalahan logaritma diskrit. Algoritme ElGamal terdiri dari tiga proses yaitu, pembentukan kunci, algoritme enkripsi, dan algoritme dekripsi [8]. Langkah-langkahnya sebagai berikut.

a. Pembentukan Kunci

Pembentukan kunci terdiri dari dua kunci yaitu kunci publik dan kunci pribadi. Proses ini memerlukan bilangan prima p dan dua bilangan acak g dan x. Untuk (p, g, dan y) adalah pasangan kunci publik dan nilai (x dan p) adalah pasangan kunci pribadi. Algoritme Elgamal menetapkan bilangan bulat pada perhitungannya. Lalu pesan yang dikirim harus diubah kedalam sebuah bilangan bulat. Pengkonversiannya menggunakan ASCII. ASCII merupakan representasi bilangan numerik dari sebuah karakter yang biasa digunakan dikomputer yang 0 adalah nilai minimalnya dan 255 adalah nilai maksimalnya. Menurut sistem elgamal, bilangan prima yang digunakan harus lebih besar 255. Berikut proses pembentukan kunci:

1. Bilangan prima p > 255.
2. Pilih bilangan acak g dan x, lebih besar dari p.
3. Hitung persamaan y :

$$y = g^x \bmod p \quad (1)$$

4. Menghasilkan kunci publik (p, g, y) dan kunci pribadi (x, p).

b. Algoritme Enkripsi

Untuk mengenkripsi membutuhkan kunci publik (p, g, y). Berikut proses enkripsi:

1. Memotong plaintext menjadi blok-blok m1, m2, m3, ..., nilai dalam setiap blok didalam selang (0, p-1).
2. Mengubah hasil blok *message* kedalam nilai ASCII.
3. Memilih bilangan acak k, dengan syarat $1 \leq k \leq p-2$.
4. Setiap blok m dienkripsi dengan persamaan:

$$a = g^k \bmod p \quad (2)$$
$$b = y^k m \bmod p \quad (3)$$

5. Menyusun ciphertext menjadi berurutan a1, b1, a2, b2, ..., an, bn.
6. a, b merupakan hasil ciphertext untuk blok *message* m yang didapatkan.

c. Algoritme Dekripsi

Untuk mendekripsikan dibutuhkan kunci private (x dan p). Berikut proses dekripsi:

1. Menghitung kunci pribadi x dengan persamaan :

$$(ax)\text{-}1 = a\ p\text{-}1\text{-}x \bmod p \quad (4)$$

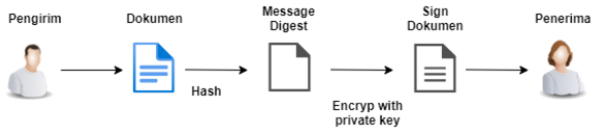
2. Medekripsikan a dan b menjadi plaintext m dengan persamaan :

$$m = b * a \text{ x mod } p \quad (5)$$

3. Mengubah nilai m yang didapat kedalam nilai ASCII.
4. Menyusun plaintext dengan urutan m1, m2, m3, ..., mn.

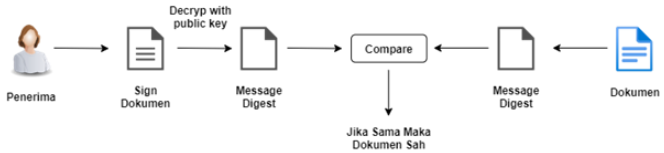
2.4 Tahapan Perancangan

a. Tahapan Tanda Tangan
Pada tahap ini dilakukan perancangan sistem yang mempresentasikan sebuah proses tahapan tanda tangan.



Gambar 1. Tahapan Tanda Tangan

b. Tahapan Verifikasi File
Pada tahap ini adalah perancangan sistem yang mempresentasikan sebuah proses tahap verifikasi file.



Gambar 2. Tahapan Verifikasi File

3. HASIL DAN PEMBAHASAN

Implementasi metode yang dijalankan untuk membuat digital signature. Meliputi proses penyisipan tanda tangan digital sampai dengan proses verifikasi dokumen yang telah disisipkan tanda tangan digital dengan menerapkan metode algoritme ElGamal.

3.1 Tahapan Pembuatan Kunci

Pada tahap pembentukan kunci bertujuan untuk membangkitkan *private key* dan *public key*. *Private key* digunakan dalam pembentukan digital signature, sedengkan kunci publik digunakan untuk verifikasi. Pada proses ini menggunakan metode ElGamal. Proses ini membutuhkan pasangan kunci, selanjutnya diwujudkan dengan memilih bilangan prima p dan dua buah bilangan acak g dan x dengan syarat g dan x lebih kecil dari p yang memenuhi persamaan $y = g^x \text{ mod } p$.

3.2 Tahapan Proses Digital Signature

Setelah proses pembentukan kunci yaitu proses pembentukan digital signature terhadap file yang akan disisipkan tanda tangan digital.

a. Proses Hashing
Proses awal pembentukan digital signature yaitu merubah file menjadi message digest dengan menggunakan algoritme SHA-256. Hasil message digest dari pesan atau file.

Tabel 2. Message Digest Dokumen

Input Dokumen	Message Digest
ST.152 spt.pdf	4cd511f6cf1e18a364e3ac7c757579e9f29c33 6d6a099b4d86e396cf61efe85a

b. Enkripsi
Pada proses ini, message digest akan dienkripsi menggunakan kunci pribadi ElGamal yang sebelumnya sudah dibangkitkan, sehingga message digest yang dienkripsi akan menghasilkan digital signature. Sebelum

memecahkan message digest menjadi blok-blok kecil. Message digest diubah terlebih dahulu kedalam kode ASCCI.

Tabel 3. Message Digest ke Kode ASCII

Message Digest	4cd511f6cf1e18a364e3ac7c757579e9f29c336d6a099b4d86e396cf61efe85a
Message Digest (Dalam kode ASCCI)	52 99 100 53 49 49 102 54 99 102 49 101 49 56 97 51 54 52 101 51 97 99 55 99 55 53 55 53 55 57 101 57 102 50 57 99 51 51 54 100 54 97 48 57 57 98 52 100 56 54 101 51 57 54 99 102 54 49 101 102 101 56 53 97

Proses enkripsi ini menggunakan algoritme ElGamal yang membutuhkan p = 257, g = 11, dan y = 22.

Tabel 4. Proses Enkripsi

Kunci Publik	p = 257	
	g = 11	
	y = 22	
Rumus Enkripsi	a = g^k mod p	(2)
	b = $y^k m$ mod p.	(3)

Berikutnya hasil enkripsi diubah ke dalam heksadesimal untuk memperoleh digital signature akhir.

Tabel 5. Hasil Digital Signature

Hasil Enkripsi	30 185 137 25 73 196 17 161 190 141 184 89 223 251 234 107 8 79 4 106 30 31 137 93 73 168 17 238 190 148 184 229 223 148 234 84 8 78 4 53 30 182 137 25 73 5 17 228 190 174 180 112 223 27 234 224 8 101 4 29 20 216 137 139 73 56 17 84 190 185 184 248 223 254 234 201 8 230 4 114 30 202 137 214 73 38 17 178 190 185 184 178 223 133 234 122 8 229 4 41 30 216 137 192 73 201 17 101 190 159 184 201 223 148 234 178 8 115 4 206 30 216 137 105 73 145 17 91
Digital Signature (Konverensi ke heksadeimal)	1E B9 89 19 49 C4 11 A1 BE 8D B8 59 DF FB EA 6B 8 4F 4 6A 1E 1F 89 5D 49 A8 11 EE BE 94 B8 E5 DF 94 EA 54 8 4E 4 35 1E B6 89 19 49 5 11 E4 BE AE B4 70 DF 1B EA E0 8 654 1D 14 D8 89 8B 49 38 11 54 BE B9 B8 F8 DF FE EA C9 8 E6 4 72 1E CA 89 D6 49 26 11 B2 BE B9 B8 B2 DF 85 EA 7A 8 E5 4 29 1E D8 89 C0 49 C9 11 65 BE 9F B8 C9 DF 94 EA B2 8 73 4 CE 1E D8 89 69 49 91 11 5B

3.3 Tahapan Proses Verifikasi

Proses verifikasi dilakukan untuk pengujian keaslian data. Berikut ini adalah tahapan verifikaksi digotal signature.

a. Hashing file yang diterima
   File yang diterima kembali di Hash untuk menghasilkan message digest.
b. Dekripsi
   Pada proses ini dilakukan dekripsi pada digital signature menggunakan kunci publik ElGamal. Digital signature didekripsi untuk menghasilkan message digest yang kemudian dibandingkan dengan message digest file awal. Digital signature yang diterima diubah ke dalam desimal, lalu didekripsi menggunakan kunci publik x = 13 dan p = 257, selanjutnya tiap-tiap blok chipertext dideskripsikan seperti tabel 6.

Tabel 6. Proses dekripsi

Kunci Privat	x =13	
	p = 257	
Rumus Dekripsi	s = a x mod p	(6)
	m = b*S p^{-2} mod p	(7)

Selanjutnya hasil dekripsi dikonverensi ke dalam kode ASCCI.

Tabel 7. Konversi Hasil Dekripsi Ke Kode ASCII

Hasil Dekripsi	52 99 100 53 49 49 102 54 99 102 49 101 49 56 97 51 54 52 101 51 97 99 55 99 55 53 55 53 55 57 101 57 102 50 57 99 51 51 54 100 54 97 48 57 57 98 52 100 56 54 101 51 57 54 99 102 54 49 101 102 101 56 53 97
Konverensi Dalam kode ASCII	52 99 100 53 49 49 102 54 99 102 49 101 49 56 97 51 54 52 101 51 97 99 55 99 55 53 55 53 55 57 101 57 102 50 57 99 51 51 54 100 54 97 48 57 57 98 52 100 56 54 101 51 57 54 99 102 54 49 101 102 101 56 53 97

c. Perbandingan message digest

Ini adalah tahapan terakhir pengujian keaslian dokumen, dimana pada tahap ini telah medapatkan dua buah message digest, yaitu message digest hasil proses hashing dari file dokumen yang diterima dan message digest hasil hashing yang diterima.

Tabel 3.7 Hasil Verifikasi

***Message digest* file**	4cd511f6cf1e18a364e3ac7c757579e9f29c33 6d6a099b4d86e396cf61efe85a
***Message digest* Hasil Dekripsi**	4cd511f6cf1e18a364e3ac7c757579e9f29c33 6d6a099b4d86e396cf61efe85a

Dan dapat disimpulkan dokumen yang diterima terbukti keabsahnnya. Karena hasil message digest saat didekripsi sama dengan hasil message digest dari dokumen aslinya.

3.4 Pengujian Sistem Digital Signature

Hasil pengujian sistem yang bertujuan untuk memastikan agar aplikasi berjalan dengan baik.

a. Proses penyisipan digital signature pada file *.pdf

Berikut adalah tampilan file *.pdf asli sebelum disisipkan tanda tangan digital pada gambar 3.

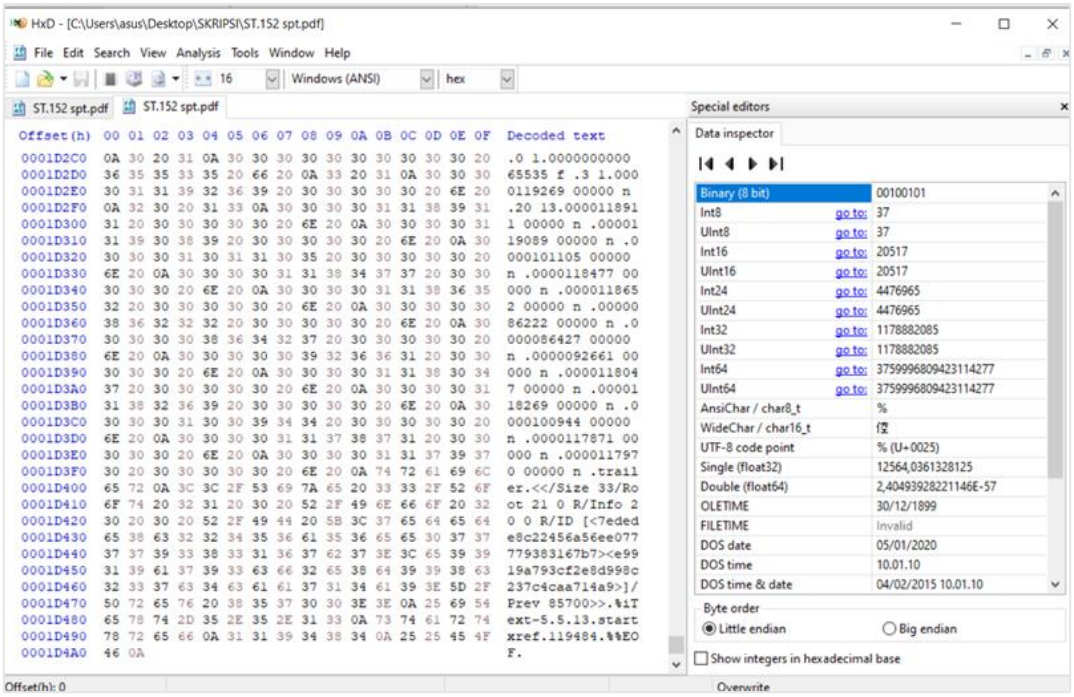

KEMENTERIAN PERHUBUNGAN
BADAN PENGEMBANGAN SUMBER DAYA MANUSIA PERHUBUNGAN
BALAI PENDIDIKAN DAN PELATIHAN PENERBANGAN CURUG

SURAT TUGAS
Nomor : ST.152/BP3C-2022

Gambar 3. Tampilan Layar **pdf*

b. Pengecekan sebelum disisipkan menggunakan aplikasi HxD

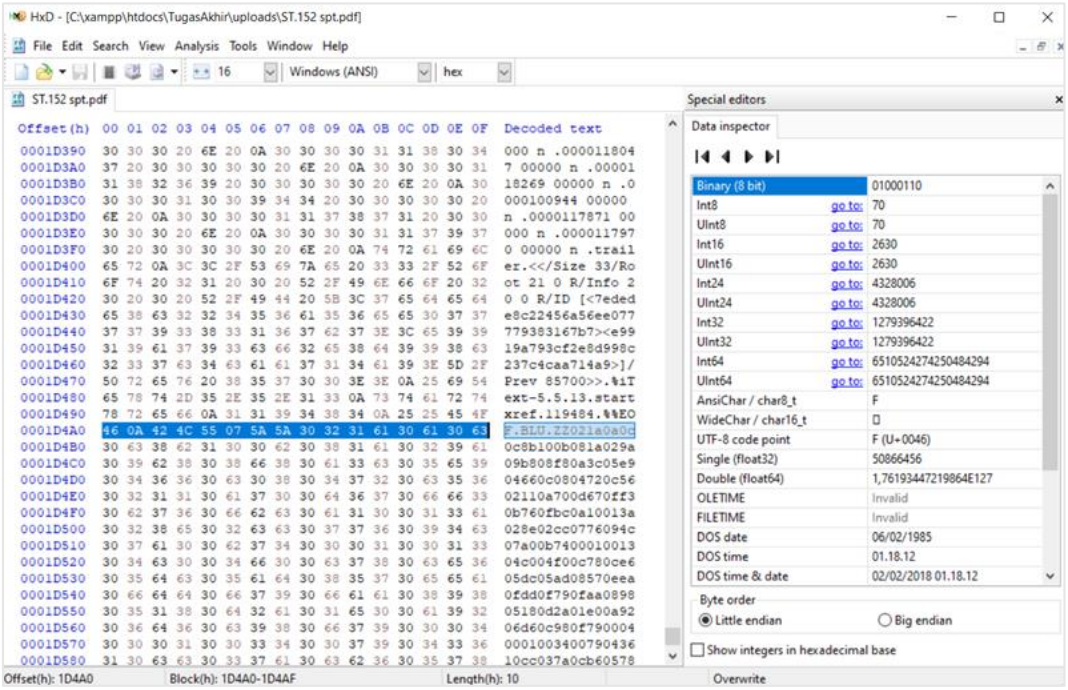
Selanjutnya file *.pdf dibandingkan sebelum dan sesudah disisipkan digital signature menggunakan aplikasi HxD. File dibuka pada aplikasi Hxd, maka akan terlihat perbedaan sebelum dan sesudah disisipkan digital signature. Berikut adalah file *.pdf sebelum disisipkan digital signature yang berada pada gambar 4:



Gambar 4. Tampilan Layar **.pdf* Sebelum Disisipkan DS

c. Pengecekan sesudah disisipkan menggunakan aplikasi HxD

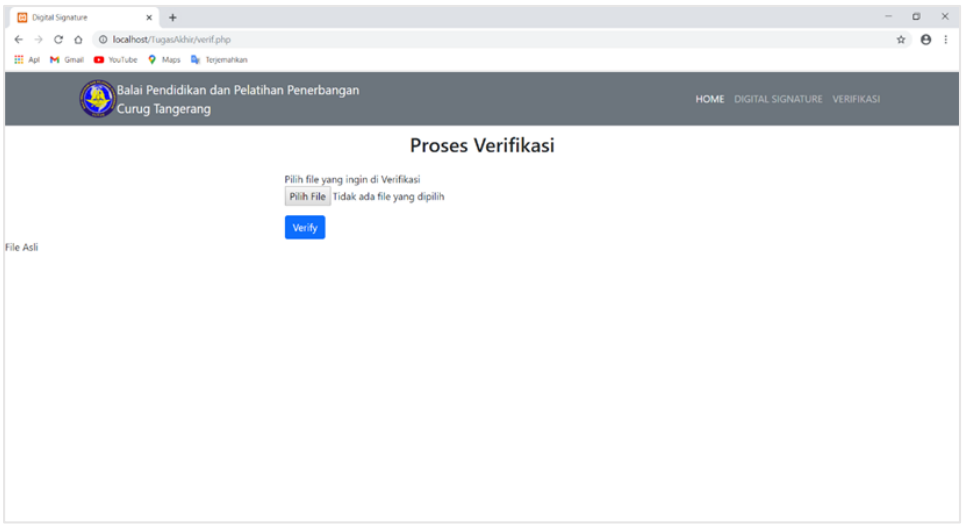
File *.pdf setelah disisipkan digital signature. Akan bertambah decode text yang berarti file sudah diberi sebuah tanda tangan digital. Berikut file yang sudah diberi tanda tangan digital pada gambar 5.



Gambar 5. Tampilan Layar **.pdf* Sesudah Disisipkan DS

d. Proses Verifikasi

Setelah proses penyisipan digital signature kedalam file, selanjutnya dilakukan proses verifikasi untuk membuktikan keaslian file tersebut, terdapat pada gambar 6 dibawah ini.



Gambar 6. Tampilan Layar File Asli

4. KESIMPULAN

Dilihat dari hasil penelitian, pengujian dan analisis sistem, dapat disimpulkan sebagai berikut

a. Algoritma ElGamal dan *Hasing* SHA-256 dapat digabungkan dengan baik dalam membuat sebuah *digital signature*.
b. Aplikasi digital signature dirancang mampu menyelsaikan permasalahan pengujian file yang dapat dilakukan oleh pihak yang tidak bertanggung jawab, sehingga mampu diandalkan dalam otentikasi file dari tindakan pemalsuan dan modifikasi data.
c. Dari pengujian ukuran dokumen asli dengan ukuran dokumen setelah disisipkan *digital signature* adalah sama.

DAFTAR PUSTAKA

[1] O. K. Sulaiman, M, Ikhwani Dan S. F, Rizki. "Model Keamanan Informasi Berbasis Tanda Tangan Digital Dengan Data Encryption Standard (Des) Algorithm", *Infotekjar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, vol. 1, no. 1, pp. 14-19, 2016.

[2] J. H. Lubis. "Analisa Tanda Tangan Digital Menggunakan Hebbian Learning Dan Support Vector Machine*"*. *Jurnal Teknik Informatika Kaputama (Jtik)*, vol. 2, no. 2, pp. 1-8, 2018.

[3] M, Ikhwani "Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma Rsa," *Cess Journal Of Computer Engineering System And Science*, vol. 1, no. 1, pp. 15-20, 2016.

[4] J. S. Tambunan Dan M. I. Sukmana. "Penyandian Pesan Berdasarkan Algoritma Rc5 Dan El-Gamal". *Jurnal & Penelitian Teknik Informatika, vol.* 2, no. 2, pp, 1-5. 2018.

[5] Azhar, Hanifah, "Perbandingan Algoritma Fungsi Hash Md5 Dengan Sha-1", Institut Teknologi Bandung. 2013. Tersedia Dalam Pada : Http://Informatika.Stei.Itb.Ac.Id/~Rinaldi.Munir/ Kriptografi/2012-2013/ Makalah2 2013 /Makalah2 Kripto 2013-045.Pdf

[6] E. C. Prabowo, Dan I. Afrianto. "Penerapan Digital Signature Dan Kriptografi Pada Otentikasi Sertifikat Tanah Digital," *Jurnal Ilmiah Komputer Dan Informatika*, vol. 6, no. 2, pp. 83–90, 2018.

[7] Pratama, Aditya, "Studi Perbandingan Danimplementasi Kombinasi Fungsi Hash Dan Kriptografi Kunci-Publik", Institut Teknologi Bandung. 2011. Tersedia Pada : Http://Informatika.Stei.Itb.Ac.Id/~Rinaldi.Munir/ Kriptografi/2010-2011/Makalah2/Makalah2- If3058-Sem2-2010-2011-016.Pdf

[8] N. Idhawati. Dan A. Prihanto. "Penerapan Algoritma Kriptografi Asimetris Elgamal Dengan Modifikasi Pembangit Kunci Terhadap Enkripsi Dan Dekripsi Gambar Warna. *Journal of Informatics and Computer Science*, vol. 1, no. 2, pp. 97-103. 2019.

[9] N. Zaatsiyah Dan Djuniadi. "Implementing Digital Signature with Rsa and Md5 in Securing E-Invoice Document" *Jurnal Pendidikan Teknologi Informasi*, vol. 5, no. 2, pp. 129-140, 2021.

[10] F.S. Sutopo, M. Riri Dan K. Cece. "Implementasi Digital Signature Algorithm (Dsa) Menggunakan Secure Hash Algorithm-256 (Sha256) Pada Media Gambar". *Jem (Jurnal Eurekamatika)*, vol. 9, no. 2, pp. 94-106, 2021.

ISSN 2962-8628

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR
Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260
https://senafti.budiluhur.ac.id/