E-ISSN : 2407 – 3911
P-ISSN : 2686 - 0333

PENANDA TANGANAN DOKUMEN DIGITAL PADA SISTEM PENYIMPANAN FILE MENGGUNAKAN KOMBINASI ALGORITMA SHA3-512 DAN RSA UNTUK MEMPERTAHANKAN KEASLIAN DATA DOKUMEN

Asep Rizal Nurjaman
Sistem Informasi
Institut Teknologi Nasional
Jl. PHH Mustofa No. 34, Bandung, Jawa barat, Indonesia
aseprizal@itenas.ac.id

Abstrak

Tujuan dari penelitian ini untuk menganalisis keamanan pada skema tanda tangan digital, sehingga dokumen yang di tanda tangani lebih terjaga integritas datanya dan diyakini oleh penerima bersumber dari pengirim yang sah. Pesatnya perkembangan teknologi saat ini membuat semua dokumen fisik yang ditanda tangani beralih menjadi dokumen yang berbentuk *softfile* dengan tanda tangan berbentuk digital. Proses pembuatan tanda tangan digital dimulai dengan pembuatan kunci publik dan kunci pribadi. Kunci publik dibuat dan dipublikasikan untuk memverifikasi tanda tangan dan menghitung nilai hash dari dokumen yang diterima. Saat ini. Beberapa penelitian sudah menggunakan konsep algoritma pada kriptografi yaitu algritma kriptografi RSA, namun masih memiliki kekurangan dimana belum dapat dibuktikan apakah dokumen yang diterima penerima merupakan dokumen dari pengirim yang sah dan tidak ada perubahan pada dokumennya. Pada penelitian ini penulis mencoba untuk menyempurnakan penelitian sebelumnya dimana user bisa memvalidasi keaslian dokumen dan meyakini bahwa pengirim dokumen merupakan pengirim yang sah dengan kombinasi algoritma algoritma RSA dan SHA3-512. Dokumen yang digunakan pada penelitian ini berkestensi .pdf, Pengujian Mitm *attack* menghasilkan kesimpulan bahwa kekuatan kunci rahasia menjadi tumpuan dalam skema yang dibangun. Skema tanda tangan digital yang dibangun bisa memvalidasi keaslian dokumen yang diterima oleh penerima dan membuktikan bahwa dokumen dikirim oleh pengirim yang sah. Waktu untuk validasi dan tanda tangan dokumen bergantung pada ukuran file pdf yang diunggah.

Kata kunci: Tanda tangan digital, SHA3-512, Algoritma RSA.

Abstract

The aim of this research is to analyze the security of digital signature schemes, so that the integrity of the data in the signature document is better maintained and the recipient is trusted to have come from a legitimate sender. The rapid development of technology today means that all signed physical documents have turned into softfile documents with digital signatures. The process of creating a digital signature begins with creating a public key and a private key. A public key is generated and published to verify the signature and calculate the hash value of the received document. Several studies have used the concept of algorithms in cryptography, namely the RSA cryptographic algorithm, but it still has shortcomings in that it cannot be proven whether the document received by the recipient is a document from a legitimate sender and there have been no changes to the document. In this research the author tries to perfect previous research where users can validate the authenticity of documents and believe that the sender of the document is a legitimate sender with a combination of the RSA and SHA3-512 algorithms. The document used in this research has .pdf extension. Mitm attack testing resulted in the conclusion that the strength of the secret key was the basis for the scheme being built. The digital signature scheme that is built can validate the authenticity of

documents received by the recipient and prove that the document was sent by a legitimate sender. Time for document validation and signature depends on the size of the uploaded pdf file.

Keywords: Digital signature, SHA3-512, RSA algorithm

I. PENDAHULUAN

Perkembangan teknologi yang pesat mengubah kebiasaan manusia dalam berkegiatan, transformasi digital mendorong perubahan dari yang awalnya konvensional menjadi otomatis, kemudahan dan kecepatan proses menjadi sebuah alasan untuk digitalisasi dokumen. Saat ini dokumen yang awalnya berupa fisik telah ditransformasi menjadi dokumen digital dengan tanda tangan fisik/basah yang telah bertransformasi menjadi tanda tangan digital seshingga tidak ada alasan untuk jarak dan waktu. Namun keamanan dari tanda tangan digital menjadi tantangan baru untuk menjaga integritas pesan dan meyakini bahwa tanda tangan yang dibubuhkan merupakan tanda tangan asli dari pengirim. Tahun 2022 Pemprov Kaltim menyampaikan bahwa ada dokumen yang keluar dari perangkat daerah dengan menggunakan fasilitas TTE (Tanda Tangan Elektronik) yang dipalsukan oleh pihak-pihak yang tidak bertanggung jawab. Pada 2024 PT Artha Bumi Mining mengalami kerugian yang sangat besar disebabkan oleh pemalsuan dokumen tambang di Sulteng (Tim regional). Solusi yang ditawarkan untuk masalah tersebut adalah algoritma kriptografi dengan skema tanda tangan digital sudah diuji untuk autentikasi pengguna, menjaga keamanan dan integritas datanya.

Pada tahun 2019 penelitian dengan judul "Implementasi Algoritma Kriptografi Ri*vest Shamir Adleman (RSA)* pada Tanda Tangan Digital" menghasilkan sebuah kesimpulan bahwa konsep algoritma *RSA* untuk tanda tangan digital diimplementasikan di sebuah sistem, namun penerima tidak bisa meyakini bahwa tidak ada perubahan dokumen karena kunci publik, dokumen dan pesan autentikasi dikirim secara bersamaan (Anshori). Pada tahun 2020 penelitian dengan judul "Implementasi *Digital Signature* menggunakan Algortima Kriptografi *RSA* untuk Pengamanan Data di SMK Wirakaraya1 Ciparay" menghasilkan sebuah kesimpulan konsep tanda tangan digital di implementasikan namun dalam sistem yang dibangun, namun proses yang dibangun hanya sampai dokumen di tandatangani oleh pemilik dokumen dan di kirimkan (Suharya). Pada tahun 2022 penelitian dengan judul "Keeping file authenticity with digital signature technique using a combination of *MD5* and elgamal algorithm" menghasilkan sebuah kesimpulan bahwa algoritma Elgamal dengan *MD5* untuk tanda tangan digital diimplementasikan pada file gambar dengan security analysis dari algoritma *MD5* dan elgamal secara umum dengan konsep dokoumen bisa dibuka siapa saja selama memiliki kunci public (Dandi Herman Dinata). Pada tahun 2023 penelitian dengan judul "Digital signature security analysis by applying the elgamal algorithm and the ide method" menghasilkan sebuah kesimpulan bahwa algoritma elgamal diimplementasikan secara statis datanya dan di perlihatkan setiap prosesnya, namun tidak ada pengujian skema pada penelitian ini (R. K. Lubis).

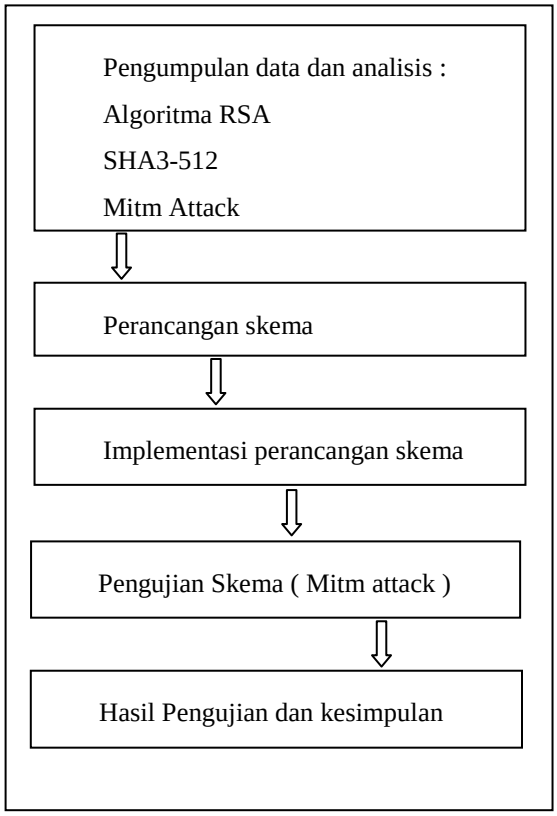
Konsep algoritma kriptografi di terapkan pada tanda tangan digital, konsep tanda tangan digital ini membuat penerima dokumen harus meyakini bahwa dokumen berasal dari pemilik yang sah dan tidak ada perubahan dokumen pada dokumen yang diterima.

Pada penelitian dengan judul "Implementasi *Digital Signature* menggunakan Algortima Kriptografi *RSA* untuk Pengamanan Data di SMK Wirakaraya1 Ciparay" di tahun 2020 dan "Implementasi Algoritma Kriptografi Ri*vest Shamir Adleman (RSA)* pada Tanda Tangan Digital" di tahun 2019, keduanya tidak bisa menunjukkan adanya proses verifikasi dari penerima terhadap dokumen yang diterima sehingga bisa terjadi perubahan dokumen yang dilakukan oleh penyerang dan penerima tidak bisa membuktikan pengirim yang sah dan pesan yang diterima terjaga integritas datanya.

Pada penelitian yang akan diajukan, penulis akan mengembangkan proses tanda tangan digital antara pengirim dan penerima sehingga penerima bisa meyakini integritas pesan dan pengirim yang sah dari dokumen yang diterima. Pengujian sistem yang dikembangkan menggunakan skema pengujian Mitm *attack.*

II. METODE PENELITIAN

Metodologi pada penelitian ini dapat diihat pada gambar 2.1



Gambar 2.1. Gambar metodologi penelitian

Berdasarkan gambar 2.1, metodologi penelitian yang diterapkan pada peneliatian ini adalah sebagai berikut :

1. Pengumpulan data dan analisis

   Pada tahap ini, penulis memilih algoritma yang akan digunakan pada tanda tangan digital dan juga metode pengujian yang akan dilakukan pada penelitina ini. Algoritma yang digunakan :

   a. Algoritma RSA

   Sandi RSA merupakan algoritma kriptografi kunci publik (asimetris). RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (sehingga disebut dengan kunci publik), namun kunci untuk dekripsi bersifat rahasia (kunci privat). Untuk menemukan kunci dekripsi, dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya.

   Memfaktorkan bilangan bulat menjadi faktor primanya bukanlah pekerjaan yang mudah. Karena belum ditemukan algoritma yang efisien untuk melakukan pemfaktoran. Cara yang bisa digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor. Jika semakin besar bilangan yang akan difaktorkan, maka semakin lama waktu yang dibutuhkan. Besaran-besaran yang digunakan pada algoritma RSA:

   1. p dan q bilangan prima (rahasia)
   2. r = p . q (tidak rahasia)
   3. $\Phi(r) = (p - 1)(q - 1)$ (rahasia)
   4. PK (kunci enkripsi) (tidak rahasia)
   5. SK (kunci dekripsi) (rahasia)
   6. X (plainteks) (rahasia)
   7. Y (cipherteks) (tidak rahasia)

   Sebagai algoritma Asimetris Kriptografi, algoritma RSA membutuhkan dua kunci yang berbeda untuk enkripsi dan dekripsi. Bilangan yang dipilih sebagai kunci adalah bilangan prima yang besar, dengan alasan pemfaktoran sebuah bilangan hasil perkalian dari dua bilangan prima yang besar menjadi dua bilangan prima yang sesuai akan sangat sulit. Sehingga keamanan dari kode RSA dapat terjamin. Berikut langkah-langkah proses pembangkitan pasangan kunci pada RSA:

   1. Pilih dua buah bilangan prima sembarang, p dan q.
   2. Hitung $r = p*q$. . . . . [1]

   dimana p! = q, sebab jika p = q maka

   $r = p^2$. . . . . [2]

   sehingga p dapat diperoleh dengan menarik akar pangkat dua dari r.

   3. Hitung $\Phi(r) = (p - 1)(q - 1)$ . . . . . [3]
   4. Pilih kunci publik, PK, yang relatif prima terhadap $\Phi(r)$.

5. Bangkitkan kunci rahasia dengan menggunakan SK . PK ≡ 1 (mod Φ(r)).

Perhatikan bahwa SK*PK ≡ 1 (mod Φ(r)) ekivalen dengan SK*PK = 1 + mΦ (r), sehingga SK dapat dihitung dengan persamaan 4

SK = (1 + mΦ (r)) / PK . . . . . [4]

Langkah-langkah pada proses enkripsi adalah sebagai berikut:

1. Plaintext diubah ke dalam bentuk bilangan. Untuk mengubah plaintext yang berupa huruf menjadi bilangan dapat digunakan kode ASCII dalam sistem bilangan desimal.

2. Plaintext m dinyatakan menjadi blok-blok x1, x2, x3, ..., sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0, n-1], sehingga transformasinya menjadi satu ke satu.

3. Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus.

$y_i = x_i^{PK} \bmod r$. . . . . [5]

Langkah-langkah pada proses dekripsi adalah sebagai berikut:

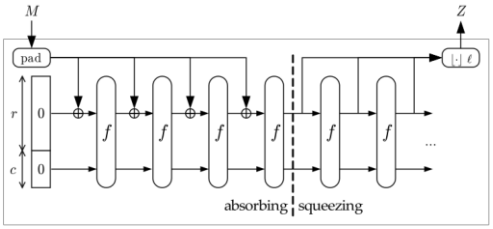
1. Setiap blok ciphertext y_i didekripsi kembali menjadi blok x_i dengan rumus

$x_i = y_i^{SK} \bmod r$

2. Kemudian blok-blok m1, m2, m3, ..., diubah kembali ke bentuk huruf dengan melihat kode ASCII hasil dekripsi.

b. SHA3-512

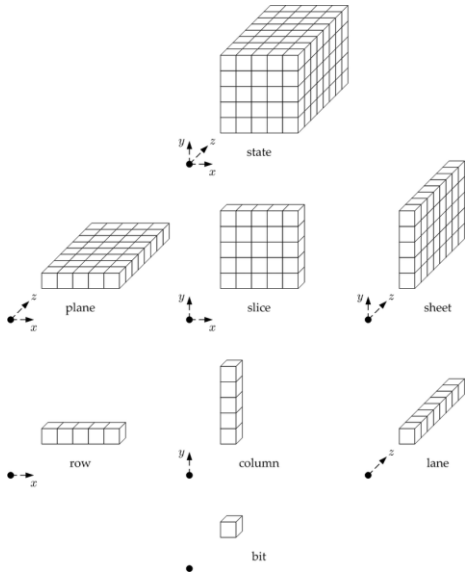
SHA3-512 merupakan salah satu jenis algoritma dari fungsi *hash keccak* yang digunakan untuk membuat integritas pesan terjaga. Fungsi *hash keccak* merupakan salah satu fungsi hash kriptografi yang mempunyai masuukan dan panjang luaran yang berubah-ubah. *Keccak* menggunakan konstruksi spons (*sponge construction*) sebagai dasar desainnya. Konstruksi spons memiliki dua fase yaitu menyerap (*absorbing*) dan memeras (*sequeezing*) (Kelsey) (Dworkin), fungsi *hash keccak* ditunjukan pada Gambar 2.2.



Gambar 2.2. Fungsi hash keccak (J. Kelsey) (M.J. Dworkin)

Absorbing (Kelsey) (Dworkin) adalah suatu proses dimana input akan di-*xor* kan dengan *bitrate* (*r)* dan diteruskan ke fungsi. 5 tahapan operasi pada fungsi *f* yaitu: *diffusion (θ), inter-slice dispersion (ρ), disturbing the horizontal / vertical alignment (π), non-linierity (X),* dan *break symetric (i). Sequeezing* (J. Kelsey) (M.J. Dworkin) merupakan fase untuk mendapatkan output dimana penggabungan digunakan untuk menghasilkan nilai *hash* dengan panjang sama dengan total bit dari *capacity (c).*

State pada *keccak* adalah bit-bit yang dapat dilihat sebagai bit *array* dengan bentuk tiga dimensi (J. Kelsey) (M.J. Dworkin). Setiap sumbu dari *array* di representasikan dengan sumbu x, y dan z. x*y merupakan potongan dari *state* dan z adalah sumbu dari *lane state* Jumlah dari bit-bit untuk setiap *slice* dari state pasti 5*5 atau 25 bit. Sementara ukuran dari tiap *lane* untuk *state* adalah 1, 2, 4, 8, 16, 32 atau 64. *State* dari keccak ditunjukkan pada Gambar 2.3.



Gambar 2.3. State pada keccak (Kelsey) (Dworkin)

c. Mitm Attack

Serangan Man-in-the-Middle adalah taktik yang digunakan oleh penyerang untuk mengintersepsi dan memanipulasi komunikasi antara dua pihak tanpa sepengetahuan mereka. Dalam skenario ini, penyerang secara rahasia menyusup ke dalam aliran komunikasi, kemudian mencuri atau mengubah informasi yang ditransmisikan. Konsep dasar serangan ini melibatkan tiga entitas: pengirim, penerima, dan penyerang yang berada di tengah-tengah keduanya. Dalam dunia digital, serangan ini dapat menyusup ke segala bentuk komunikasi online, mulai dari pesan email hingga transaksi finansial. Skema *Mitm attack* pada penelitian ini, penyrang akan menyadap komunikasi antara kueduanya lalu akan coba menebak kunci rahasia milik pengirim yang digunakan untuk memanipulasi data

2. Perancangan skema

Pada tahap ini, akan dibuat skema untuk melakukan proses penanda tanganan secara digital dan proses validasi bagi penerima sehingga integritas data dokumen bisa tetap terjaga dan penerima meyakini jika pesan berasal dari pengirim yang sah.

3. Implementasi perancangan skema

Pada tahap ini, hasil dari perancangan skema akan di implementasikan pada sebuah sistem berbentuk prototype berbasis web dimana flow dari proses penanda tanganan dan validasi dokumen bisa divalidasi.

Prototyping merupakan metode pengembangan perangat lunak yang berupa model fisik kerja sistem dan berfungsi sebagai versi awal dari sistem. Metode prototyping ini akan menghasilkan prototype sistem sebagai perantara pengembang dan pengguna agar dapat berinteraksi dalam proses kegiatan pengembangan sistem informasi (Purnomo, D). Model prototyping bisa dilihat pada Gambar 2.4, dimana model prototype setidaknya mempunyai 6 tahapan sebagai berikut:

Tahap 1: Requirements Gathering and Analysis (Analisis Kebutuhan)

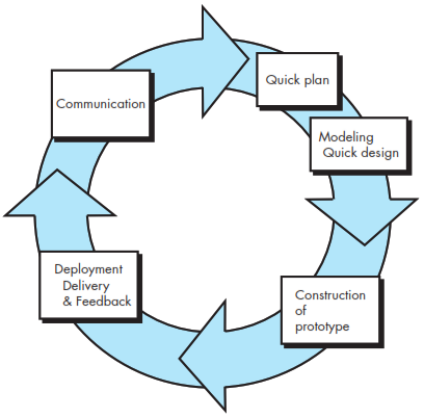
Tahap 2: Quick Design (Desain cepat)

Tahap 3: Build Prototype (Bangun Prototipe)

Tahap 4: User Evaluation (Evaluasi Pengguna Awal)

Tahap 5: Refining Prototype (Memperbaiki Prototipe)

Tahap 6: Implement Product and Maintain (Implentasi dan Pemeliharaan



Gambar 2.4. Metode Prototyping

E-ISSN : 2407 – 3911
P-ISSN : 2686 - 0333

4. Pengujian Skema Mitm attack

   Pada tahap ini skema yang dibangun akan diujikan dengan penyerangan *Mitm*, dimana akan dilihat probabilitas attack dari penyerang yang akan berada di antara pengirim dan penerima dengan tujuan untuk mencari tahu kunci rahasia dari pengirim yang nantinya akan digunakan untuk memanipulasi data dokumen nya.

5. Hasil pengujian dan kesimpulan

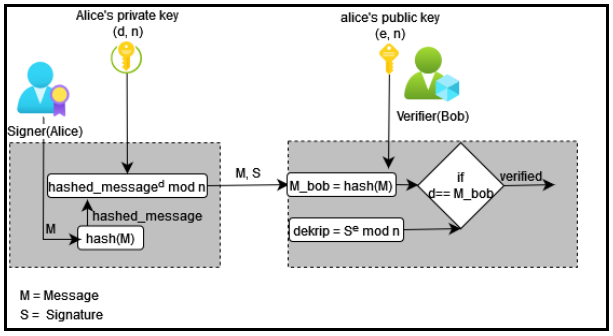
   Pada tahap ini akan disampaikan hasil akhir dari penelitian ini.

III. ANALISIS DAN PERANCANGAN

Pada bab ini disampaikan perancangan skema, implementasi skema pada tanda tangan digital dan validasi dokumen serta hasil pengujian

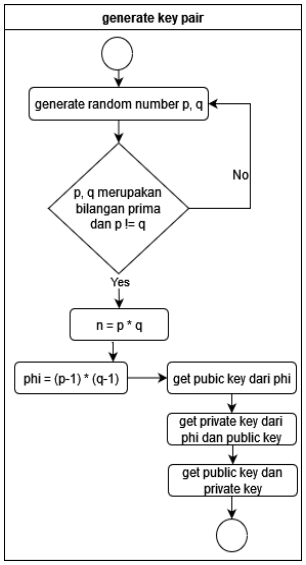
III.1 Skema tanda tangan digital dan validasi

Secara umum, skema dari penelitian ini terdiri dari pengirim dan penerima. Gambar 3.1. merupakan proses penanda tangan dan validasi dokumen.



Gambar 3.1. Skema tanda tangan digital

Pada skema yang akan dibangun pengguna harus memiliki *generate public key* dan *private key* terutama untuk penanda tangan dokumen, proses untuk *generate public key* dan *private key* pada algoritma RSA yang dapat dilihat pada Gambar 3.2. dimana penerima akan menggunakan *public key* pengirim untuk memvalidasi integritas dokumen.



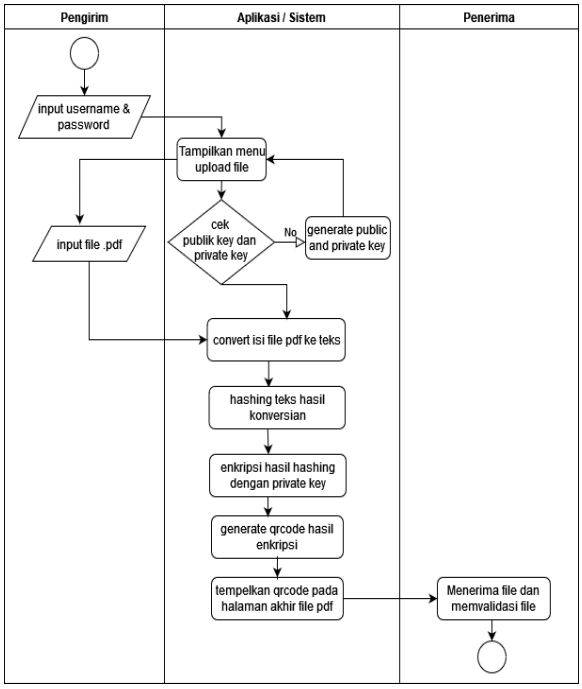
Gambar 3.2. Proses generate key pair RSA

Skema yang dibangun pada penelitian ini terdiri dari skema penanda tangan digital dan skema validasi dokumen. Detail dari kedua skema tersebut dijelaskan pada:

A. Skema penanda tangan digital pada dokumen

   Pada skema penanda tanganan digital, proses yang dilakukan oleh pengguna hanya mengupload file dengan ekstensi hanya .pdf. Pada sistem akan di cek terkait *public key* dan *private key* pengguna, proses ekstraksi isi dokumen dokumen, dan juga proses hashing isi dokumen dengan algoritma SHA3-512 yang di enkripsi dengan algoritma RSA sebagai penjaga integritas dokumen menggunakan *private key* pengirim. Pada penelitian ini bentuk tanda tangan digital dibuat dalam bentuk qrcode yang di sisipkan pada halaman akhir dokumen sehingga saat isi dokumen berubah maka seharusnya isi qrcode juga ikut berubah untuk memastikan integritas dokumen terjaga. Gambar 3.3. menampilkan proses penanda tanganan digital.

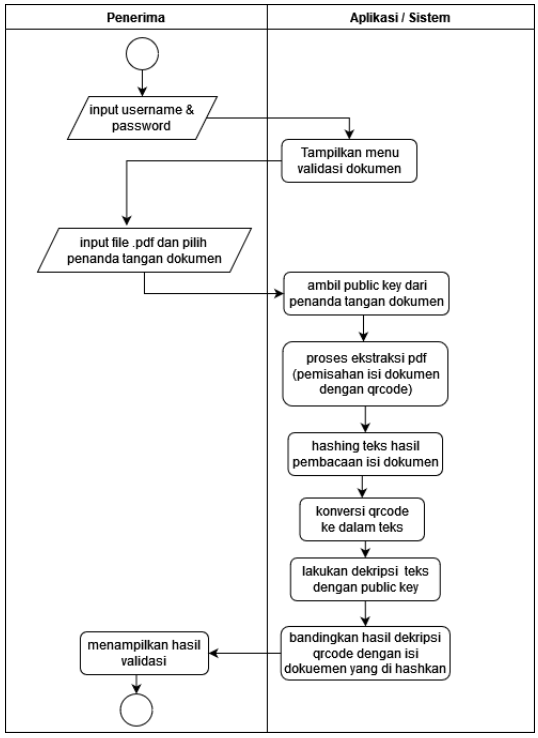
E-ISSN : 2407 – 3911
P-ISSN : 2686 - 0333



Gambar 3.3. Proses penanda tanganan digital dokumen

B. Skema validasi pada dokumen

Pada skema validasi dokumen digital, penerima mengupload dokumen yang sudah di tanda tangani ke dalam sistem lalu pilih penanda tangan dokumen. Sistem akan mengambil *public key* penanda tangan dokumen lalu akan dilakukan proses ekstraksi dokumen pdf untuk mengambil isi dokumen dan qrcode sebagai tanda tangan digital. Isi dokumen pdf akan dikonversi ke teks dan di hashing kan dengan menggunakan algoritma SHA3-512, selanjutnya qrcode pada dokumen akan dikonversi ke dalam teks yang selanjutnya akan dilakukan proses dekripsi dengan menggunakan algoritma RSA dengan *public key* dari penanda tangan. Validasi dokumen pada sistem dilakukan dari hasil hash isi dokumen yang akan di bandingkan dengan hasil deksipsi qrcode yang sudah diubah menjadi teks. Proses validasi dokumen oleh penerima dapat dilihat pada Gambar 3.3.



Gambar 3.4. Proses validasi dokumen

III.2 Implementasi skema tanda tangan digital

Hasil implementasi skema penanda tanganan digital dan validasi dokumen dapat dilihat pada:

1. Halaman Login pengguna

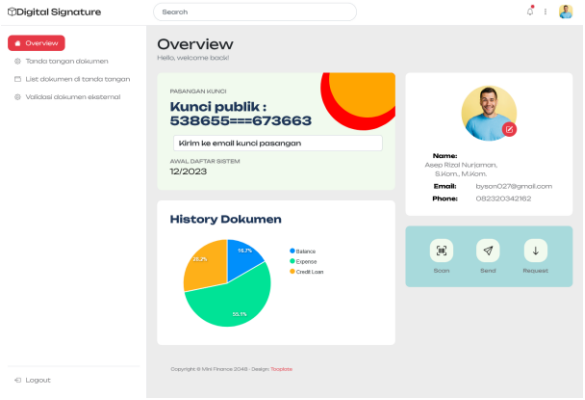
Halaman awal agar bisa melakukan penanda tanganan digital atau validasi dokumen yaitu halaman login pengguna dimana pengguna akan memasukkan username dan password. Halaman login pengguna bisa dilihat pada Gambar 3.5.

Gambar 3.5. Halaman login pengguna

E-ISSN : 2407 – 3911
P-ISSN : 2686 - 0333

2. Halaman dashboard

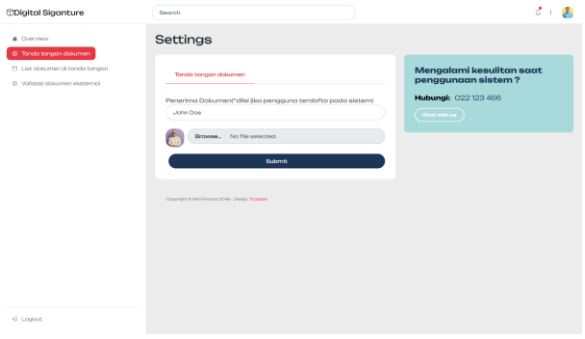
Halaman dashboard menampilkan kunci publik, history dokumen, menu tanda tanagn digital, list dokumen masuk dan verifikasi dokumen digital. Gambar 3.6 menampilkan halaman dashboard sistem.



Gambar 3.6. Dashboard sistem

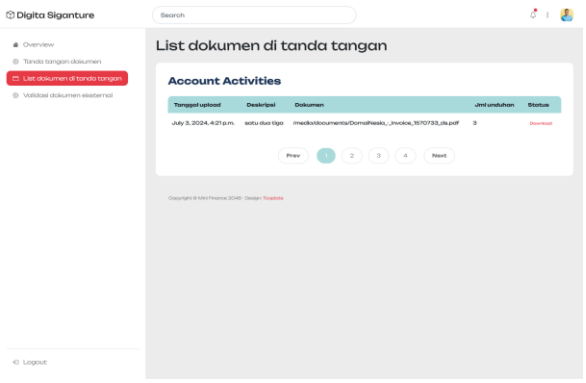
3. Halaman penanda tanganan dokumen

Halaman penanda tanganan dokumen menampilkan form untuk unggah dokumen pdf dan juga penerima dokumen saat penerima terdaftar terdaftar dalam sistem, jika tida terdaftar maka form penerima dokumen bisa dikosongkan. Saat pengguna sistem submit dokumen maka proses validasi pada sistem akan berjalan dari mulai pembacaan konten dokumen pdf sampai proses pembubuhan qrcode sebagai tanda tangan digital pada dokumen pdf. Gambar 3.7 menampilkan halaman penanda tanganan dokumen.



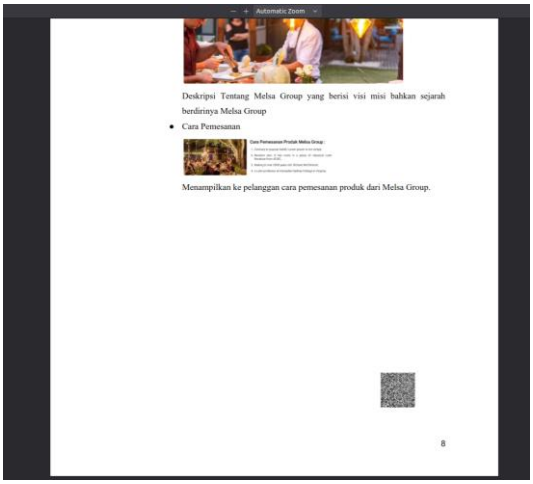
Gambar 3.7. Halaman Tanda tangan digital

Setelah submit / upload dokumen selesai, pengguna bisa melihat dokumen yang sudah di tanda tangan pada menu list dokumen di tanda tangan. Di menu ini memuat semua dokumen yang di tanda tangani oleh pengguna yang masuk pada sistem. Dokumen yang sudah di tanda tangani bisa di unduh dengan menekan tombol *download*. Menu list dokumen ditanda tangan bisa dilihat pada Gambar 3.8.



Gambar 3.8. Halaman list dokumen di tanda tangan

Gambar 3.9 menampilkan potongan tanda tangan digital pada dokumen pdf dalam bentuk qrcode yang dibubuhkan pada halaman akhir dokumen.



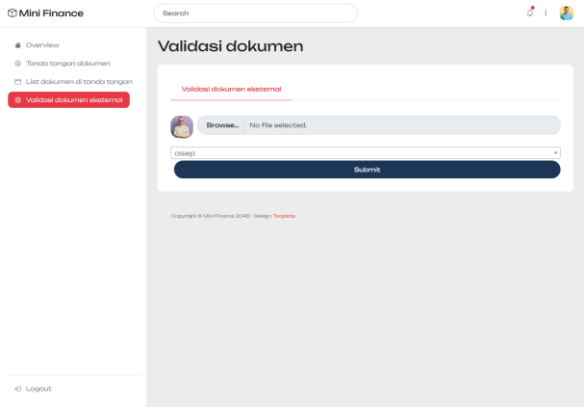
Gambar 3.9. Qrcode sebagai tanda tangan digital

4. Halaman validasi dokumen

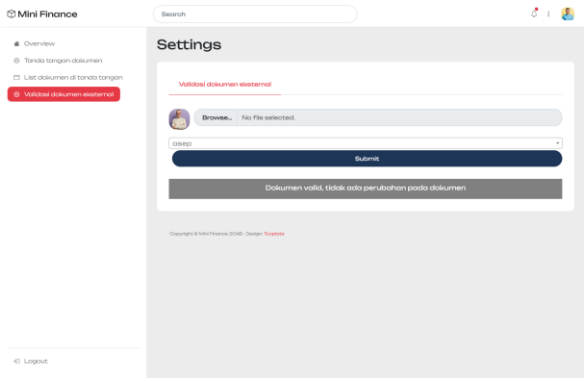
Pengguna dapat memvalidasi keaslian dokumen dengan cara masuk ke menu validasi dokumen eksternal lalu unggah

E-ISSN : 2407 – 3911
P-ISSN : 2686 - 0333

dokumen pdf dan juga pilih penanda tangan dokumen nya. Lalu tekan tombol submit untuk memvalidasi dokumen. Proses yang terjadi pada sistem adalah pembacaan isi dokumen dan pengambilan public key penanda tangan dokumen dan proses validasi dokumen. Gambar 3.10 merupakan tampilan untuk halaman validasi dokumen. Dan hasil validasi dapat dilihat pada Gambar 3.11.



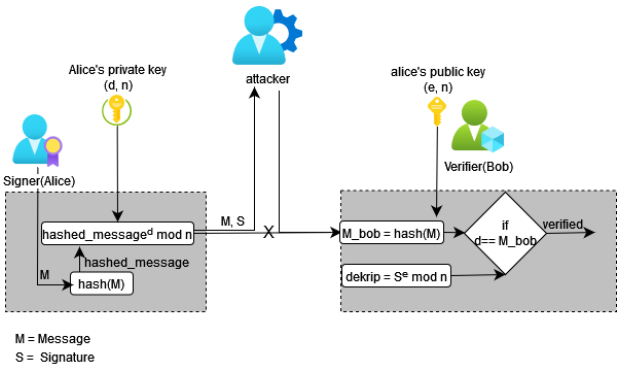
Gambar 3.10. Halaman validasi dokumen



Gambar 3.10. Halaman hasil validasi dokumen

III.3 Pengujian skema tanda tangan digital

Skema *Mitm attack* dilakukan untuk melihat seberapa besar celah penyrang untuk bisa mendapatkan kunci rahasia pengirim dimana penyrang berada di antara penanda tangan dan yang memvalidasi dokumen. Skema *Mitm attack* dapat dilihat pada Gambar 3.11.



Gambar 3.11. Skema Mitm attack

Peluang penyerang untuk mendapatkan kunci dengan brute force adalah $1/2^l$ dimana l merupakan panjang kunci rahasia. Proses untuk menebak kunci rahasia penanda tangan bisa dilihat pada persamaan 6.

M,S
hm = h(M)
tmp = 0
l = 1
while S != tmp {
  tmp = hm^l mod n
  l = l + 1
} . . . . . [6]

Pengujian sistem juga dilakukan untuk menghitung waktu proses penanda tanganan dan valdasi dokumen. Tabel 1 menunjukan waktu penanda tanganan dan waktu validasi dokumen dalam satuan detik.

Tabel 1. Waktu tanda tangan dan validasi dokumen

No	Dokumen pdf	Ukuran pdf	Waktu sign	Waktu validasi
1	Dokumen1	10.1 MB	36.04 sec	89.58 sec
2	Dokumen2	1.3 MB	0.4 sec	0.59 sec
3	Dokumen3	613.8 kB	0.49 sec	1.67 sec
4	Dokumen4	4.3 MB	3.19 sec	4.92 sec
5	Dokumen5	12.9 MB	4.55 sec	12.57 sec
6	Dokumen6	18.0 MB	1.96 sec	0 sec
7	Dokumen7	9.4 MB	5.08 sec	13.68 sec
8	Dokumen8	11.9 MB	2.41 sec	4.05 sec
9	Dokumen9	6.4 MB	1.69 sec	3.63 sec

Dari percobaan pada Tabel 1 dapat dilihat bahwa proses waktu penanda tanganan bergantung pada ukuran file, konten pdf dan kualitas gambar pada dokumen pdf. Pada Dokumen6 ukuran file pdf 18 MB karena pada file tersebut memiliki banyak gambar dengan kualitas tinggi namun pada dokumen6 hanya memiliki 9 halaman sehingga waktu penanda tanganan relatif cepat di bandingkan pada dokumen1

karena pada dokumen1 isi dokumen lebih banyak dalam bentuk teks sehingga ukuran file lebih kecil di banding dokumen6 namun proses waktu penandatanganan lebih lama dari dokumen6 karena dokumen1 memiliki 135 halaman. Jumlah halaman pada penelitian ini bisa dilihat pda Tabel 2.

Tabel 2. Jumlah halaman dokumen

No	Dokumen pdf	Jumlah halaman pdf
1	Dokumen1	135 halaman
2	Dokumen2	8 halaman
3	Dokumen3	8 halaman
4	Dokumen4	260 halaman
5	Dokumen5	233 halaman
6	Dokumen6	9 halaman
7	Dokumen7	315 halaman
8	Dokumen8	158 halaman
9	Dokumen9	40 halaman

Ukuran file setelah proses penanda tanganan bisa dilihat pada Tabel 3. Pada tabel tersebut, file yang sudah di tanda tangani mengalami perubahan ukuran file dengan rata-rata perubahan ukuran file dari 0.1% s/d 15% bergantung pada konten dokumen yang dijadikan bagian dari tanda tangan digital.

Tabel 3. Ukuran file awal dan setah tanda tangan

No	Dokumen pdf	Ukuran file awal	Ukuran file setelah tanda tangan
1	Dokumen1	10.1 MB	10.4 MB
2	Dokumen2	1.3 MB	1.5 MB
3	Dokumen3	613.8 kB	855.3 kB
4	Dokumen4	4.3 MB	4.1 MB
5	Dokumen5	12.9 MB	14.6 MB
6	Dokumen6	18.0 MB	18.2 MB
7	Dokumen7	9.4 MB	11.9 MB
8	Dokumen8	11.9 MB	11.8 MB
9	Dokumen9	6.4 MB	6.8 MB

Berdasarkan Tabel 1, saat validasi dokumen terjadi kegagalan validasi karena dokumen yang di tanda tangani sudah memiliki qrcode sehingga saat proses validasi konten dari qrcode dokumen awal tidak masuk ke proses konversi isi dokumen ke teks dan menghasilkan gagal validasi dokumen.

IV. KESIMPULAN

Berdasarkan penelitiian ini, maka algoritma RSA dan SHA3-512 berhasil diterapkan pada sistem tanda tangan digital dengan batasan hanya dokumen pdf dan dokumen pdf yang akan di tanda tangani belum mimiliki qrcode. Dengan menggunakan algortima RSA dan SHA3-512 penerima dokumen bisa meyakini bahwa penanda tangan dokumen merupakan pengguna yang sah karena divalidasi dengan kunci publik penanda tangan, selain itu keaslian dokumen bisa dipastikan terjaga karena saat pada dokumen telah dibubuhkan tanda tangan digital di halaman akhir dokumen, sehingga saat ada perubahan sedikit pun pada dokumen bisa harusnya qrcode sebagai tanda tangan digital nya berubah. Berdasarkan pengujian skema pada tanda tangan digital, waktu untuk penanda tanganan dan validasi dokumen bergantung pada banyaknya halaman dan kualitas gambar dalam dokumen pdf yang diunggah. Berdasarkan skema dan algoritma yang digunakan probabilitas penyerang untuk bisa merubah dokumen adalah $1/2^{l}$ dimana l merupakan panjang kunci rahasia yang digunakan untuk mengenkripsi hasil hashing.

Pada penelitian sebelumnya diharapkan sistem bisa membedakan tanda tangan yang di buat oleh system dalam bentuk qrcode dan qrcode lainnya yang sudah ada sebelumnya dalam dokumen pdf

REFERENSI

Stallings, W. (2013). "Cryptography and Network Security: Principles and Practice". New Jersey: Prentice Hall Press.

Stallings, William. (2005). "Cryptography and Network Security Principles and Practices (4th ed.)". Prentice Hall.

Dang, Quynh H. (2012). Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.FIPS.180-4

B. Bhushan, G. Sahoo and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking — A review," 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall), 2017, pp. 1-6, doi: 10.1109/ICACCAF.2017.8344724.

W. Diffie, M. Hellman, New directions in cryptography. IEEE Transactions on Information Theory, 22, (1976), pp. 644–654.

Secure Hash Standard (SHS). Federal Information Processing Standards Publication, FIPS PUB 202, 2015

T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31, (1985), pp.469–472.

https://diskominfo.kaltimprov.go.id/berita/hati-hati-mulai-ada-pemalsuan-tanda-tanganelektronik

Dandi Herman Dinata, Nova Mayasari, & Rio Septian Hardinata. (2022). Keeping File Authenticity with Digital Signature Technique using a Combination of MD5 and Elgamal Algorithm. INFOKUM, 10(03), 350-356.

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

A. Saepulrohman, and A. Ismangil, "Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA)," Int. J. Electron. Commun. Syst., vol. 1, no. 1, pp. 1–9, Jun. 2021

R. K. Lubis, A M H Pardede, and Husnul Khair, "Digital Signature Security Analysis by Applying the Elgamal Algorithm And The Idea Method", j. of artif. intell. and eng. appl., vol. 3, no. 1, pp. 373–382, Oct. 2023.

Helfi Nasution, Heri Priyanto, and Nanda Widya, "Penerapan Digital Signature untuk Persuratan menggunakan Metode Algoritma SHA-1 di Sektor Pertanian, Ketahanan Pangan dan Perikanan Kab. Mempawah", Scientica, vol. 2, no. 4, pp. 131–149, Jan. 2024.

Tim regional. (2024, May 21). Kasus Pemalsuan Dokumen Tambang, Polda Sulteng Tetapkan Tersangka. *Https://Www.Liputan6.Com/Regional/Read/5601604/Kasus-Pemalsuan-Dokumen-Tambang-Polda-Sulteng-Tetapkan-Tersangka*.

Kelsey, J., Change, S., & Perlner, R. (2016). *SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash*. https://doi.org/10.6028/NIST.SP.800-185

Dworkin, M. J. (2015). *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. https://doi.org/10.6028/NIST.FIPS.202

Suharya, Y., Kom, S., & Widia, H. (n.d.). *IMPLEMENTASI DIGITAL SIGNATURE MENGGUNAKAN ALGORITMA KRIFTOGRAFI RSA UNTUK PENGAMANAN DATA DI SMK WIRAKARYA 1 CIPARAY*.

Purnomo, D. (2017). Model prototyping pada pengembangan sistem informasi. *JIMP-Jurnal Informatika Merdeka Pasuruan*, *2*(2).