ALGORITMA TANDA TANGAN DIGITAL UNTUK MENINGKATKAN KEAMANAN PESAN

Gafrun*[1], Yonal Supit[2],
[1,2]STMIK Catur Sakti Kendari, Program Studi Sistem Informasi
*e-mail: *[1]gafrun@gmail.com, [2]yonalsupit@gmail.com*

Seiring dengan kemajuan teknologi informasi semakin banyajk orang yang mampu memanipulasi data, merubah data yang menyebabkan informasi yang diterima sudah tidak asli. Salah satu kelemahan informasi digital adalah mudahnya dimodifikasi dan dipindahkan oleh siapa saja apalagi informasi tersebut dikirim melalui internet sehingga sulit untuk membuktikan keaslian informasi tersebut [1]. Untuk mengatasi masalah tersebut dibutuhkan tanda tangan digital yang dapat digunakan untuk meningkatkan keamanan serta menjaga data atau informasi yang dapat menghindari pemalsuan informasi [2]. Manfaat dari tanda tangan digital adalah untuk melakukan pembuktian secara matematis bahwa pesan yang dikirim hanya untuk menjaga keaslian pesan dan mencegah adanya nirpenyangkalan. Penelitian ini bertujuan untuk mengetahui proses pembuatan tanda tangan digital menggunakan digital signature algorithm untuk keamanan informasi pesan dan menjaga integritas data secara utuh. Metode penelitian menggunakan algoritma tanda tangan digital yang disebut Digital Signature Algorithm (DSA) dan Fungsi Hash Standard yang disebut Secure Hash Algorithm (SHA). Digital Signature Algorithm (DSA) memiliki fungsi yaitu pembentukan tanda tangan dan pemeriksaan keabsahan tanda tangan (verifikasi). Digital Signature Algorithm (DSA) menggunakan dua buah kunci yaitu kunci publik dan kunci private dan prosedur pembentukan tanda tangan menggunakan kunci private pengirim sedangkan prosedur pemeriksaan tanda tangan menggunakan kunci publik pengirim [3]. Proses pembangkitan kunci sebesar 512 bit sampai 1024 bit dan input teks pesan berupa file yang berekstensi *.txt. Digital Signature Algorithm (DSA) juga menggunakan fungsi hash satu arah SHA-I untuk mengubah pesan menjadi message digest [4][5]. Dengan menggunakan tanda tangan digital dapat memberikan keamanan informasi serta menjaga keaslian data yang berhubungan dengan perubahan data secara tidak sah.

Kata Kunci : *Tanda Tangan Digital, Fungsi Hash, DSA, Metode Blackbox, Modul Signature.*

I. PENDAHULUAN

Informasi merupakan elemen yang sangat penting dalam berbagai bidang kehidupan. Banyak informasi melalui internet baik itu melalu e-mail maupun media sosial.

Informasi yang ditransmisikan melalui internet sangat rentan terhadap kemungkinan modifikasi serta sulitnya pembuktian keaslian informasi tersebut. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang penting dapat diakses oleh orang-orang yang tidak berhak saat melakukan proses pemindahan data melalui media komunikasi bahwa untuk menjamin bahwa informasi berupa pesan tetap terjaga keasliannya dan keutuhannya. Tanda tangan digital merupakan metode yang dapat digunakan untuk memastikan keaslian informasi pesan yang dikirimkan secara elektronik. Dalam membuat tanda tangan digital dalam penelitian ini adalah menggunakan algoritma tanda tangan digital yang disebut Digital Signature Algorithm (DSA). dan Fungsi Hash Standard yang disebut Secure Hash Algorithm (SHA) [4][6]. Digital Signature Algorithm (DSA) memiliki dua fungsi utama yaitu pembentukan tanda tangan dan pemeriksaan keabsahan tanda tangan (verifikasi). Digital Signature Algorithm (DSA) menggunakan dua buah kunci yaitu kunci publik dan kunci private. Prosedur pembentukan tanda tangan menggunakan kunci private pengirim sedangkan prosedur pemeriksaan tanda tangan menggunakan kunci publik pengirim. Digital Signature Algorithm (DSA) juga menggunakan fungsi hash satu arah SHA-I untuk mengubah pesan menjadi message digest [7]. Algortima DSA dapat memberikan keamanan informasi berupa pesan dan menjaga keaslian pesan dari perubahan secara tidak sah. Sistem keamanan yang bias akita kenal saat ini misalnya kriptografi, kriptografi bisa digunakan untuk untuk mengatasi masalah keaslian suatu dokumen [8]. Setiap metode kriptografi atau keamanan data harus dipertimbangkan elemen seperti kekuatan enkripsi RSA, ukuran pesan dan kerentangan terhadap berbagai serangan [9]. Tanda tangan digital atau elektronik dapat menjamin keamanan dokumen yang ditandatanganinya dalam aspek integrity, authentication, serta non repundiation [10][11].

II. METODE PENELITIAN

Pelaksanaan hasil penelitian yang telah dicapai pada tahun 2024 langkah pertama yang dilakukan adalah dengan melakukan pengumpulan bahan dan alat yang akan digunakan dalam proses implementasi algoritma

tanda tangan. Dalam Permasalahan yang terjadi adalah dengan kemajuan teknologi informasi semakin banyak orang yang dapat melakukan manipulasi data, perubahan data yang menyebabkan informasi yang diterima tidak sah karena salah satu kelemahan informasi digital adalah mudahnya dimodifikasi oleh siapa saja apalagi informasi tersebut dikirim melalui internet sehingga sangat sulit untuk memastikan keaslian informasi tersebut. Melihat permasalan yang ada maka dilakukan proses pengumpulan bahan dan alat yang akan digunakan untuk pembuatan algoritma tanda tangan digital. Bahan dan alat yang digunakan berupa suatu teks pesan yang berekstensi .txt dan proses pembangkitan kunci sebesar 512 bit sampai 1024 bit. Bahan dan alat yang digunakan adalah perangkat keras komputer (laptop) dan perangkat lunak sistem operasi windows.Adapun teknik pen pengumplan data dengan cara teknik kepustakaan dengan beberapa studi literatur yang dapat digunakan sebagai acuan dalam perancangan sistem yang akan dibuat.

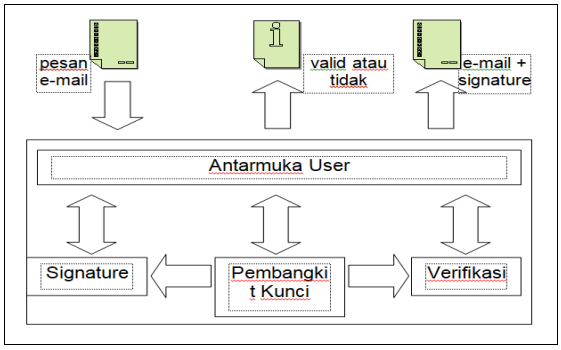
A. Gambaran Perancagan Sistem

Perangkat lunak tanda tangan digital dibuat berdasarkan metode *Digital Signature Algorithm* (DSA) yang selanjutnya akan disebut sebagai Digital Signature for Messages (DSM). Sistem DSM memiliki input berupa pesan dan output berupa pesan yang terenkripsi yang akan dikirim dan notifikasi apakah pesan yang diterima benar atau tidak. Sistem ini akan terdiri dari empat modul: modul Antarmuka User, modul Pembangkit Kunci, modul Signature, dan modul Verifikasi.

Digital Signature Algorithm (DSA) ini akan memiliki properti berupa parameter sebagai berikut:

a. p, adalah bilangan prima dengan panjang 1024 bit. Parameter p bersifat publik dan dapat digunakan bersama-sama oleh orang di dalam kelompok.
b. q, bilangan prima 160 bit, merupakan faktor dari $p - 1$. Dengan kata lain, $(p - 1) \bmod q = 0$. Parameter q bersifat publik.
c. $g = h^{(p-1)/q} \bmod p$, dimana $h < p - 1$ sedemikian sehingga $h^{(p-1)/q} \bmod p > 1$. Parameter g bersifat publik.
d. x, adalah bilangan bulat kurang dari q. Parameter x adalah kunci pribadi.
e. $y = g^x \bmod p$, adalah kunci publik.
f. m, pesan yang akan diberi tanda tangan.

1. Perancangan Antamuka User

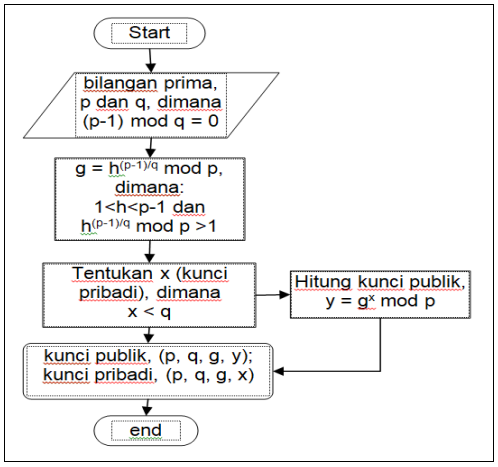


Gambar 1. Perancangan Antarmuka User

Gambar 1. Menggambarkan antarmuka sistem dengan user. Antarmuka user menampilkan menu berisi fungsi-fungsi yang terdapat di dalam perangkat lunak DSM. Terkait dengan fungsionalitas sistem, ada beberapa tugas utama yang ditangani oleh antarmuka user, yaitu:

a. Antarmuka untuk menangani pembangkitan serta pemilihan kunci pribadi dan kunci publik yang dilakukan oleh user.
b. Antarmuka untuk menerima pesan yang menjadi input dari perangkat lunak DSM, sekaligus menampilkan hasil tanda tangan digital sesuai dengan inputan.
c. Antarmuka untuk menampilkan hasil dari verifikasi antara pesan dengan tanda tangan digital yang ada.

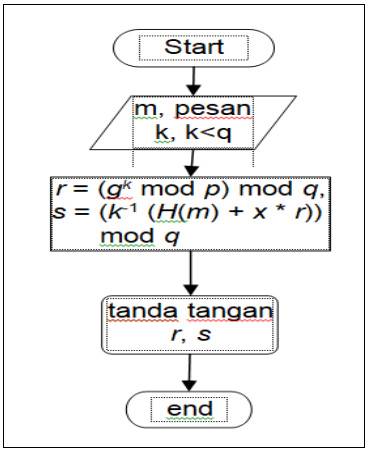
2. Diagram Alir Pembangkitan Kunci



Gambar 2. Diagram Alir Pembangkitan Kunci

Berdasarkan gambar 2. Diagram alir pembangkitan kunci menggambarkan fungsionalitas pembangkitan kunci pribadi dan kunci publik sesuai dengan mekanisme algoritma DSA [12]. menghitung pasangan kunci pribadi dan kunci publik yang diperoleh melalui fungsi matematis, yang memiliki input dua bilangan prima, p dan q.

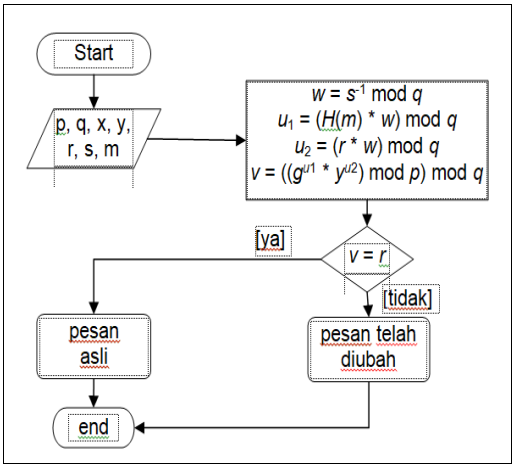
3. Digram Alir Pembangkitan TandaTangan (*Signature*)



Gambar 3. Diagram Alir Tanda Tangan (*Signature*)

Gambar 3. Diagram Alir Pembangkitan TandaTangan (*Signature*) berperan membuat tanda tangan digital dengan mengimplementasikan fungsi hash dan kunci pribadi yang telah dibangkitkan pada modul pembangkit kunci [13]. Tanda tangan digital dalam algoritma DSA disimbolkan dengan r dan s. Nilai r, diperoleh dari persamaan $r = (g^k \bmod p) \bmod q$, sedangkan nilai s dari $s = (k^{-1} (H(m) + x * r)) \bmod q$.

4. Diagram Alir Verifikasi Keabsahan Tanda Tangan



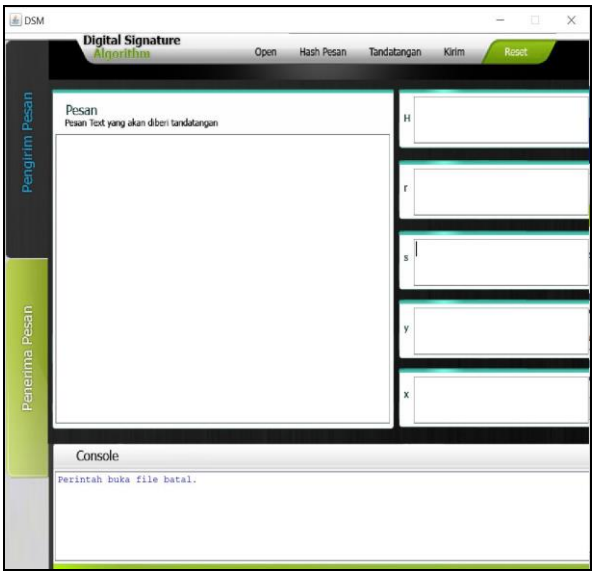
Gambar 4. Diagram Alir Verifikasi Keabsahan Tanda Tangan

Verifikasi Keabsahan Tanda Tan berfungsi untuk mengecek (membandingkan) antara input pesan dan input tanda tangan digital (output dari modul signature), apakah valid atau tidak [14][15].

III. HASIL DAN PEMBAHASAN

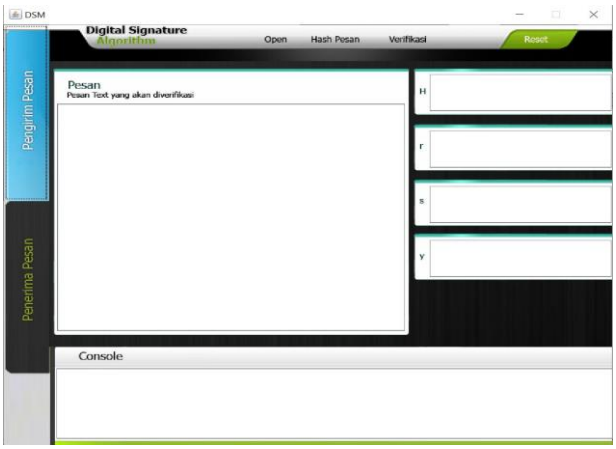
Hasil Pengujian Algoritma Tanda Tangan Digital Untuk Meningkatkan Keamanan Pesan

A. Halaman Utama Aplikasi Pengirim Pesan



Gambar 5. Halaman Utama Aplikasi Pengirim Pesan

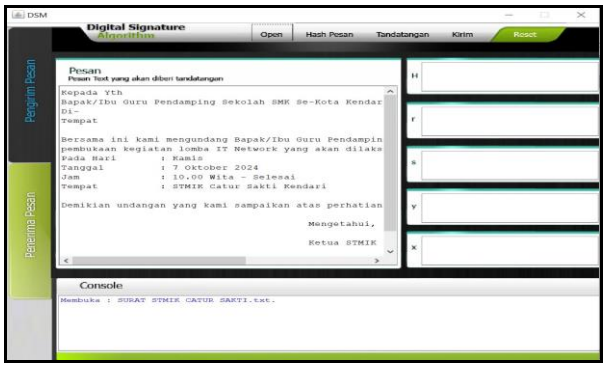
B. Halaman Utama Aplikasi Penerima Pesan



Gambar 6. Halaman Utama Aplikasi Penerima Pesan

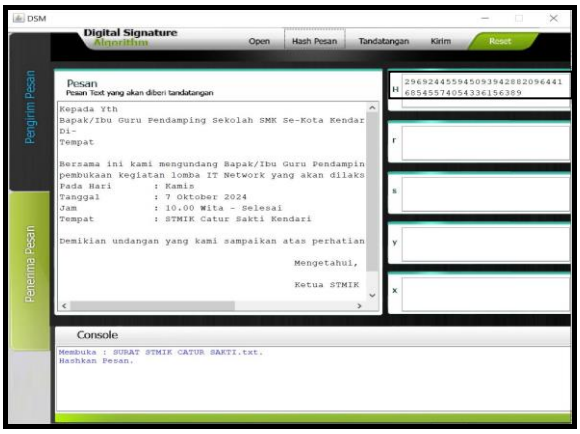
1. 1 Transformasi Pesan Menggunakan Fungsi Hash

Mula-mula pesan ditulis, atau di buka melalui file Open untuk menampilkan pesan yang akan dikirim sebagai berikut.



Gambar 7. Tampilan Pesan Asli

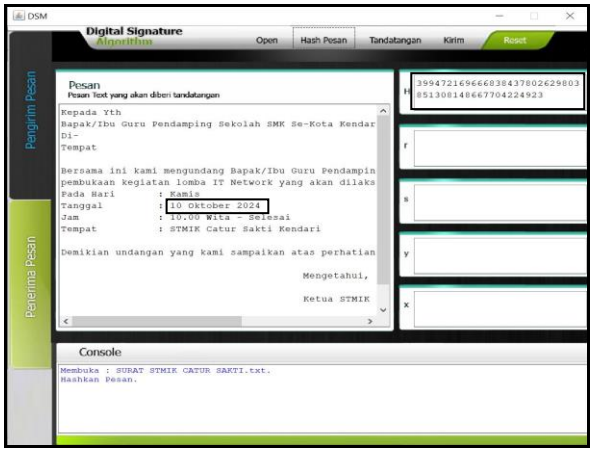
Untuk mengubah pesan menjadi message digest dilakukan dengan menekan tombol “Hash pesan”. Sehingga akan diperoleh suatu bilangan integer 160 bit yang dihasilkan dari transformasi pesan menggunakan fungsi hash SHA-1. Gambar 8 menunjukkan hasil transformasi pesan pada Gambar 7.



Gambar 8. Tampilan Hasil Transformasi Pesan

Apabila pesan berubah, maka hasil transformasi juga akan berubah. Yang akan berakibat pada berubahnya tandatangan dan kunci publik yang dihasilkan. Hasil

transformasi untuk pesan yang telah diubah ditunjukkan pada Gambar 9.

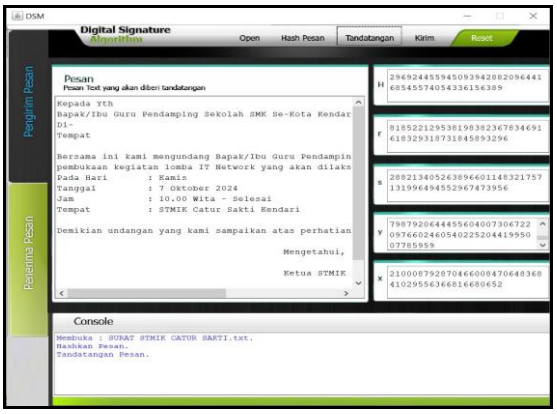


Gambar 9. Tampilan Pesan Yang Sudah Diubah

Tampak bahwa pesan asli dan pesan yang telah diubah menunjukkan hasil transformasi fungsi hash yang berbeda. Hal ini disebabkan karena setiap karakter dalam sebuah pesan akan menghasilkan nilai bit yang berbeda. Sehingga pada saat ditransformasikan dengan fungsi hash, diperoleh hasil yang berbeda pula.

1.2 Penandatanganan Pesan dan Pembangkitan Kunci Publik Y

Untuk menandatangani pesan dan membangkitkan kunci publik y, dilakukan dengan menekan tombol Tandatangan. Hasil tandatangan dan kunci publik ditunjukkan pada Gambar 10 berikut.

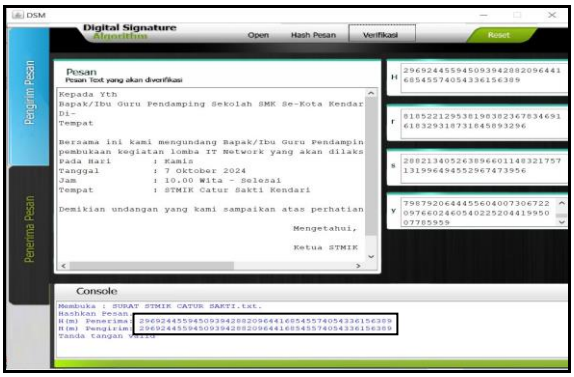


Gambar 10. Hasil Tanda Tangan dan Kunci Publik Y Dari Pesan

Pada gambar 10 dapat dijelaskan mengenai penandataganan pesan dan pembangkitan kunci publik bahwa Pada sistem tandatangan digital yang menggunakan algoritma DSA, Pada penandatanganan pesan, dibutuhkan bilangan p, q, g, k, dan kunci pribadi x. Sedangkan verifikasi pesan membutuhkan bilangan p, q, g, tandatangan r, dan s, serta kunci publik y. Oleh karena itu, jika salah satu atau ketiga bilangan tersebut berubah, maka akan menghasilkan tandatangan yang berbeda.

1.3. Verifikasi

Verifikasi pesan dilakukan dengan memasukkan pesan yang diterima, tandatangan r dan s, serta kunci publik y. Jika pesan belum berubah, maka verifikasi akan menghasilkan notifikasi bahwa tandatangan dan pesan yang diterima adalah valid. Namun, jika pesan tersebut telah diubah, atau dikirim oleh orang yang tidak bersangkutan maka akan menghasilkan notifikasi bahwa pesan dan tandatangan yang diterima tidak valid. Tampilan tahap verifikasi ditunjukkan pada Gambar 11. Begitu juga untuk tampilan tahap verifikasi dengan pesan yang telah diubah ditunjukkan pada Gambar 12.

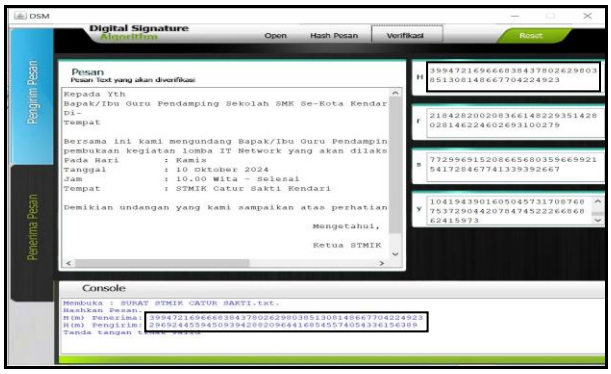


Gambar 11. Tampilan Hasil Verifikasi Pesan

1.4. Pengujian Keamanan Tanda Tangan Digital untuk Integritas Data

Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah, untuk menjaga integritas data sistem harus memiliki kemampuan untuk mendeteksi adanya manipulasi data oleh pihak-pihak yang tidak berhak antara lain perubahan data, penghapusan, dan penambahan pesan kedalam data yang sebenarnya.

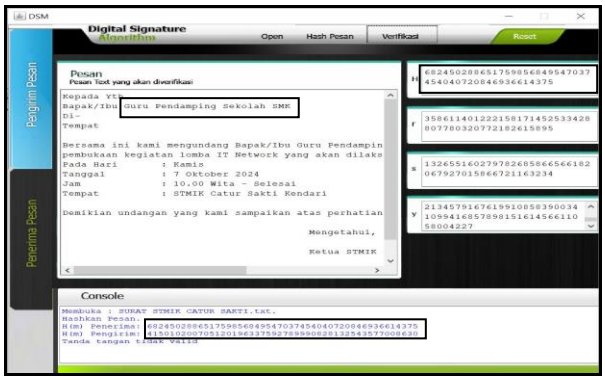
1.4.1. Hasil verifikasi pesan yang telah diubah :



Gambar 12. Tampilan hasil verifikasi pesan yang telah diubah

Berdasarkan hasil verifikasi pesan pada gambar 12. Tampak bahwa pesan asli telah diubah menunjukkan hasil transformasi fungsi hash yang berbeda. Hal ini disebabkan karena setiap karakter dalam sebuah pesan akan menghasilkan nilai bit yang berbeda, sehingga pada saat ditransformasikan dengan fungsi hash, diperoleh hasil yang berbeda pula. dan akan menghasilkan notifikasi bahwa pesan yang diterima tidak valid.

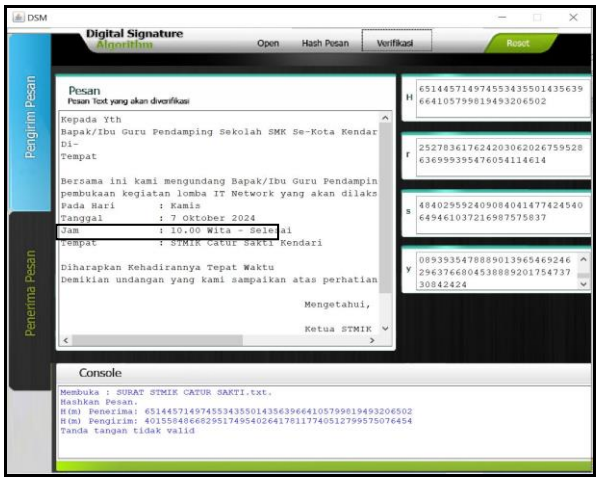
1.4.2. Hasil Verifikasi Pesan Yang Telah Dihapus



Gambar 13. Tampilan hasil verifikasi pesan yang telah di hapus

Berdasarkan hasil verifikasi pesan pada gambar 13. Tampak bahwa pesan asli telah dihapus menunjukkan hasil transformasi fungsi hash yang berbeda. Hal ini disebabkan karena setiap karakter dalam sebuah pesan akan menghasilkan nilai bit yang berbeda, sehingga pada saat ditransformasikan dengan fungsi hash, diperoleh hasil yang berbeda pula. dan akan menghasilkan notifikasi bahwa pesan yang diterima tidak valid.

1.4.3. Hasil Verifikasi Penambahan Pesan

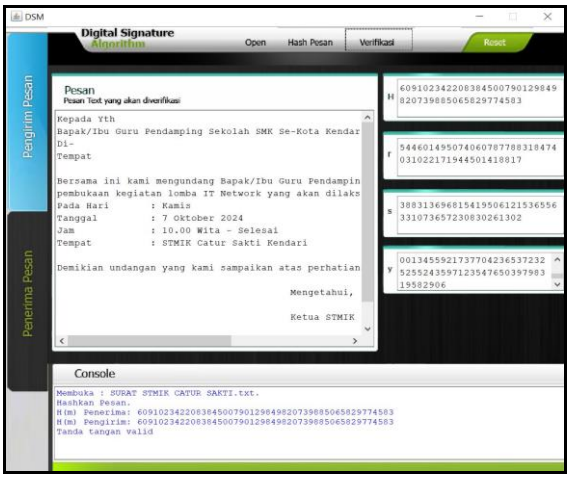


Gambar 14. Hasil Verifikasi Penambahan Pesan

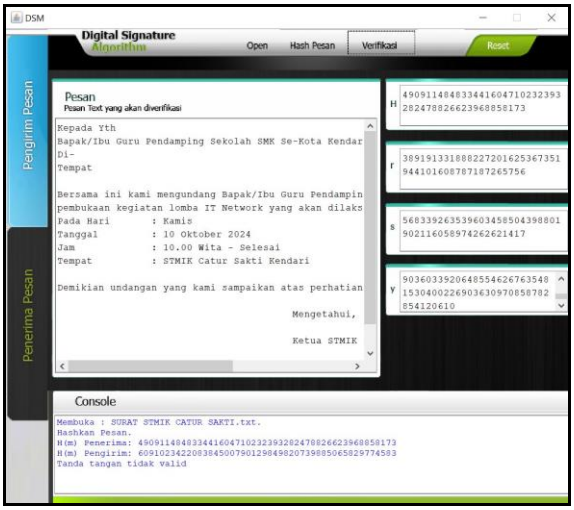
Berdasarkan hasil verifikasi pesan pada gambar 14. Tampak bahwa pesan asli telah ditambah menunjukkan hasil transformasi fungsi hash yang berbeda. Hal ini disebabkan karena setiap karakter dalam sebuah pesan akan menghasilkan nilai bit yang berbeda, sehingga pada saat ditransformasikan dengan fungsi hash, diperoleh hasil yang berbeda pula. dan akan menghasilkan notifikasi bahwa pesan yang diterima tidak valid.

1.4.4. Nirpenyangkalan (*Non Repudiation*)

Merupakan usaha untuk mencegah terjadinya penyangkalan, bahwa pengirim pesan tidak dapat mengelak bahwa dialah yang mengirim pesan tersebut. Pada sistem tandatangan digital yang menggunakan algoritma DSA, setiap user (pengirim maupun penerima) menyimpan tiga bilangan yang sama yaitu p, q, dan g. Pada penandatanganan pesan, dibutuhkan bilangan p, q, g, k, dan kunci pribadi x. Sedangkan verifikasi pesan membutuhkan bilangan p, q, g, tandatangan r, dan s, serta kunci publik y. Oleh karena itu, jika salah satu atau ketiga bilangan tersebut berubah, maka akan menghasilkan tandatangan yang berbeda. Dan jika dilakukan verifikasi, maka diperoleh notifikasi bahwa pesan tersebut tidak valid dengan kata lain pesan dikirim oleh pihak lain. Gambar 15 dan 15 menunjukkan perbedaan tandatangan yang dihasilkan apabila nilai p, q, maupun g berubah. Pada Gambar 16. ditunjukkan hasil yang diperoleh jika nilai q berubah.



Gambar 15. Hasil verifikasi dengan bilangan p,q, dan g asli



Gambar 16. Hasil verifikasi dengan tanda tangan r, s dan kunci public y berubah

1.5. Analisis Hasil Algoritma Tanda Tangan Digital Untuk Meningkatkan Keamanan Pesan.

Dari hasil peneltian yang telah ada sebelumnya mengenai tanda tangan digital maka penulis ingin mengembangkan perangkat lunak yang telah ada yaitu algoritma tanda tangan digital untuk keamanan pesan dengan menggunakan algoritma DSA (*Digital signature*

Algorithm). Perangkat lunak ini dibuat dengan pembangkitan sepasang kunci privat dan kunci public, proses tanda tangan (*signature*) dan proses verifikasi. Jadi berdasarkan hasil implementasi dan pengujan sistem yang dibangun perangkat lunak dapat ::

1. Menjaga integritas data dan menjamin keaslian pesan secara utuh dan belum pernah dimanipulasi selama proses pengiriman, dalam menjaga integritas data. Algoritma DSA memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak antara lain pengapusan pesan, penambahan pesan dan perubahan pesan kedalam data yang sebenarnya. Apabila pesan asli telah dihapus, diubah dan tambah akan menunjukkan hasil transformasi fungsi hash yang berbeda, hal ini disebabkan karena setiap karakter dalam sebuah pesan akan menghasilkan nilai bit yang berbeda, sehingga pada saat ditransformasikan dengan fungsi hash, diperoleh hasil yang berbeda pula. dan akan menghasilkan notifikasi bahwa pesan yang diterima tidak valid.
2. Perangkat lunak DSA yang dibuat dapat mencegah terjadinya penyangkalan, bahwa pengirim pesan tidak dapat mengelak bahwa dialah yang mengirim pesan tersebut. bahwa setiap user (pengirim maupun penerima) menyimpan tiga bilangan yang sama yaitu p, q, dan g. Pada penandatanganan pesan, dibutuhkan bilangan p, q, g, k, dan kunci pribadi x. Sedangkan verifikasi pesan membutuhkan bilangan p, q, g, tandatangan r, dan s, serta kunci publik y. Oleh karena itu, jika salah satu atau ketiga bilangan tersebut berubah, maka akan menghasilkan tandatangan yang berbeda. Dan jika dilakukan verifikasi, maka diperoleh notifikasi bahwa pesan tersebut tidak valid dengan kata lain pesan dikirim oleh pihak lain

IV. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Berdasarkan hasil pengujian dapat disimpulan perangkat lunak algoritma tanda tangan digital untuk keamanan pesan adalah :

1. Perangkat lunak Algoritma tanda tangan digital (DSA) dibuat dengan menggunakan tiga tahap yaitu : proses pembangkitan kunci pribadi dan kunci publik, proses *signature* dan proses verifikasi.
2. Perangkat lunak yang dibuat dengan menggunakan Algoritma (DSA) dapat memperlihatkan pengaruh pesan yang telah ubah, dihapus, dan ditambah oleh pihak ketiga. Hal ini membuktikan bahwa DSA dapat menjaga integritas data secara utuh dan dapat mencegah terjadinya Nir penyangkalan (*non repudiation*).
3. Dari pengujian terhadap sistem, diketahui bahwa tingkat keamanan tanda tangan digital sangat baik, karena perubahan 1 karakter saja dari tanda tangan maupun pesan akan memberikan dampak yang signifikan yaitu tanda tangan menjadi tidak valid.

4.2. Saran

Saran dari penulis adalah untuk dapat memberikan perbandingan bahwa algoritma tanda tangan digital mana yang terbaik untuk studi kasus yang sama dan untuk lebih mengoptimalkan penggunaan perangkat lunak, agar fitur dalam perangkat lunak ini dapat ditambah dengan suatu fungsi yang dapat memberikan enkripsi terhadap isi dokumen digital yang ditandatangani.

DAFTAR PUSTAKA

[1] S. F. Sutopo, R. Marwati, and C. Kustiawan, "Implementasi Digital Signature Algorithm (DSA) Menggunakan Secure Hash Algorithm-256 (SHA-256) pada Media Gambar," *J. EurekaMatika*, vol. 9, no. 2, pp. 94–106, 2020.

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

[3] T. Yuniati and M. F. Sidiq, "Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital sebagai Alternatif Pengesahan Dokumen di Masa Pandemi," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 6, 2020, doi: 10.29207/resti.v4i6.2502.

[4] N. Zaatsiyah and D. Djuniadi, "Implementing Digital Signature With Rsa and Md5 in Securing E-Invoice Document," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 5, no. 2, p. 129, 2021, doi: 10.22373/cj.v5i2.10359.

[5] L. B. Handoko, "DIGITAL SIGNATURE PADA CITRA MENGGUNAKAN RSA DAN VIGENERE CIPHER BERBASIS MD5," vol. 10, no. 1, pp. 357–366, 2019.

[6] A. H. HR, M. Khudzaifah, and M. N. Jauhari, "Implementasi Fungsi Hash MD5 dan Kriptografi Algoritma RSA pada Pembuatan Tanda Tangan Digital," *J. Ris. Mhs. Mat.*, vol. 1, no. 2, pp. 51–63, 2021, doi: 10.18860/jrmm.v1i2.13992.

[7] P. Hade and M. Winoto, "Penggunaan Digital Signature Sebagai Keamanan Sistem Informasi," *J. Unikom*, vol. 1, no. 4, 2022, [Online]. Available: https://www.researchgate.net/publication/370098591

[8] 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.

[9] J. Hutagalung, P. S. Ramadhan, and S. J. Sihombing, "Keamanan Data Menggunakan Secure Hashing Algorithm (SHA)-256 dan Rivest Shamir Adleman (RSA) pada Digital Signature," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 6, pp. 1213–1222, 2023, doi: 10.25126/jtiik.1067319.

[10] I. B. G. Sarasvananda and I. B. A. I. Iswara, "Tanda Tangan Elektronik Menggunakan Algoritma Rivest Shamir Adleman (RSA) pada Sistem Informasi Surat Menyurat LPIK INSTIKI," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 11, no. 2, pp. 289–296, 2022, doi: 10.32736/sisfokom.v11i2.1403.

[11] A. A. Santosa and A. A. N. Perwira Redi, "Pemilihan Platform Tanda Tangan Digital Berdasarkan Faktor Keberlanjutan Selama Pandemi COVID-19 Menggunakan Metode AHP," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 12, no. 2, pp. 195–209, 2021, doi: 10.31849/digitalzone.v12i2.8014.

[12] S. Neyman and S. Qisthina, "Pengamanan Internet of Things untuk Tanda Tangan Digital Menggunakan Algoritme Elgamal Signature Scheme," *J. Ilmu Komput.*

dan Agri-Informatika, vol. 8, no. 1, pp. 69–78, 2021, doi: 10.29244/jika.8.1.69-78.

[13] R. A. Perdana, D. R. Anbiya, and A. Grahitandaru, "Penerapan Tanda Tangan Digital pada Gambar Formulir Digital Signature Implementation on C1 .PLANO-KWK di Pilkada Sulawesi Selatan," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 5, pp. 475–484, 2019, doi: 10.25126/jtiik.201961471.

[14] Y. Suharya and H. Widia, "Implementasi Digital Signature Menggunakan Algoritma Kriftografi RSA Untuk Pengamanan Data Di SMK Wirakarya 1 Ciparay," *J. Inform.*, vol. 07, no. 01, pp. 20–29, 2020.

[15] Y. Anshori and A. Y. Erwin Dodu, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital Implementation of Rivest Shamir Adleman (RSA) Cryptography Algorithm On Digital Signatures," 2019.