IMPLEMENTASI *DIGITAL SIGNATURE* PADA LAPORAN TUGAS AKHIR

Aprianti Nanda Sari[1], Didik Suwito Pribadi[2], Trisna Gelar[3]
Athiyya Rahmawati [4], Nandhifa Azzahra [5], Hilmy Oktoharitsa [6]

[1,2,3,4,5,6] Jurusan Teknik Komputer dan Informatika, Politeknik Negeri Bandung
[1] aprianti.nanda@polban.ac.id , [2] didik.suwito@polban.ac.id , [3] trisna.gelar@polban.ac.id
[4] athiyya.rahmawati.tif19@polban.ac.id , [5] nandhifa.azzahra.tif19@polban.ac.id,
[6] hilmy.oktoharitsa.tif18@polban.ac.id

Abstrak

Salah satu implementasi algoritma kriptografi nirsimetri/asimetri adalah *digital signature*. Tujuan dari skema *digital signature* adalah untuk menggantikan tanda tangan manual dengan cara mengenkripsi nilai hash dari dokumen yang ditandatangani menggunakan kunci privat pengirim. Akibatnya, integritas dari dokumen menjadi terjamin karena perubahan satu bit saja oleh pihak yang tidak berwenang dapat terdeteksi. Pada dokumen laporan Tugas Akhir di Jurusan Teknik Komputer dan Informatika Politeknik Negeri Bandung (JTK POLBAN), terdapat Lembar Pengesahan yang perlu ditandatangani oleh berbagai pihak. Pada sistem yang sedang berjalan, proses tanda tangan dokumen secara digital dilakukan dengan cara menyisipkan citra tanda tangan. Tentunya, cara tersebut tidak aman dan rawan disalahgunakan. Misalnya, perubahan isi dokumen laporan TA oleh pihak yang tidak bertanggung jawab setelah dokumen tersebut ditandatangani. Selain itu, proses pengiriman dokumen digital melalui internet sangat rentan terhadap kemungkinan modifikasi sehingga sulit untuk membuktikan keaslian dokumen. Untuk mengatasi masalah tersebut, penelitian ini mengajukan skema *digital signature* dengan menggunakan algoritma kriptografi asimetri RSA dan fungsi hash MD5. Kompleksitas pada penelitian ini adalah bagaimana menerapkan metode *digital signature* konvensional yang terdiri dari dua pihak yaitu penandatangan dan penerima sedemikian hingga dapat diterapkan pada banyak pihak yang menandatangani dokumen yang sama. Dari hasil percobaan, metode yang diusulkan dapat menyelesaikan semua skenario pengujian dengan baik sehingga manipulasi dokumen dan penyalahgunaan tanda tangan pihak-pihak yang terlibat dapat dihindari.

Kata kunci : *digital signature*, RSA, MD5, laporan tugas akhir

1. Pendahuluan

Menurut buku Panduan Tugas Akhir Program Diploma Tiga Politeknik Negeri Bandung, Tugas Akhir (TA) adalah suatu kegiatan dalam bentuk proyek yang dilaksanakan pada semester akhir perkuliahan program Diploma Tiga dengan beban empat SKS. TA dilaksanakan oleh satu mahasiswa dan dibimbing oleh dosen yang memiliki kompetensi dan kualifikasi yang sesuai. Salah satu hasil karya TA adalah Laporan TA. Salah satu bagian pada Laporan TA adalah Lembar Pengesahan yang berisi judul TA, identitas mahasiswa, nama dan tanda tangan dosen pembimbing, dosen penguji, dan Ketua Jurusan.

Saat ini, proses tanda tangan pada Lembar Pengesahan dilakukan dengan cara menyisipkan citra tandatangan pada dokumen Laporan TA. Tentunya, teknik ini tidak aman dan rawan disalahgunakan oleh pihak yang tidak bertanggung jawab. Selain itu, proses pengiriman dokumen digital melalui internet sangat rentan terhadap kemungkinan modifikasi sehingga sulit membuktikan integritas dokumen. Oleh karena itu, dibutuhkan sebuah sistem untuk membuktikan keaslian identitas pihak yang menandatangani dan integritas dokumen yang dikirim dengan menggunakan metode *digital signature*.

Pada skema *digital signature* konvensional, pihak yang menandatangani dokumen hanya satu entitas. Namun pada kasus nyata penandatanganan laporan TA, ada banyak pihak yang menandatangani dokumen yang sama. Misalnya, para dosen penguji, para dosen pembimbing, dan Ketua Jurusan. Oleh karena itu, perlu strategi khusus untuk mengimplementasikan skema *digital signature* pada laporan TA.

Pada dasarnya, *digital signature* merupakan implementasi dari algoritma kriptografi nirsimetri. Dokumen yang akan ditandatangani akan diambil nilai hash-nya untuk dienkripsi dengan menggunakan kunci privat milik pengirim untuk menghasilkan *digital signature*. Untuk dapat membuktikan integritas dokumen yang dikirim, nilai hash dokumen akan dibandingkan dengan hasil dekripsi *digital signature* dengan menggunakan kunci publik pengirim. Jika nilai hash dan hasil dekripsi sama,

maka dapat dipastikan bahwa dokumen tidak dimodifikasi oleh pihak tidak bertanggung jawab.

Pada penelitian ini, fungsi hash MD5 yang diciptakan oleh Ronald Rivest (R. Rivest, 1992) digunakan untuk mengekstraksi nilai hash dari dokumen Laporan TA. Pemilihan fungsi hash MD5 ini dilakukan karena memiliki fitur *time stamping* dan banyak digunakan dalam protokol kriptografi (Sobti & Geetha, 2012) (Ghoshal et al., 2020). Sedangkan untuk mengenkripsi nilai hash dokumen Laporan TA, algoritma kriptografi RSA dipilih karena tingkat keamanannya yang baik (R. L. Rivest et al., 1978) (LIVINGSTON, 1956).

2. Landasan Teori

Pada bab ini akan dibahas secara singkat mengenai proses pengesahan laporan TA di JTK POLBAN, fungsi *hash* MD5, *digital signature*, dan algoritma RSA.

2.1 Proses Pengesahan Laporan TA

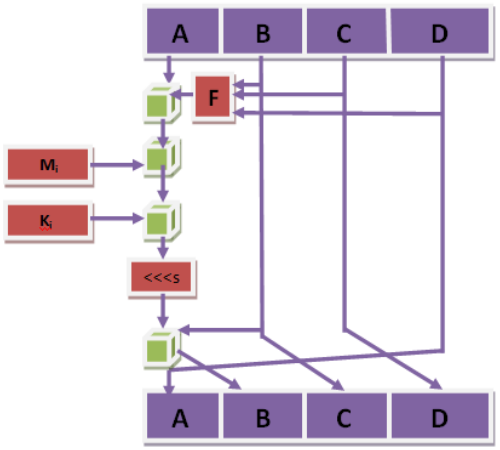
Di JTK POLBAN, setelah mahasiswa melakukan perbaikan terhadap laporan TA dan dipastikan tidak ada perubahan lagi, mahasiswa meminta tanda tangan para dosen penguji, para dosen pembimbing, dan Ketua Jurusan. Urutan pemberian tanda tangan menjadi penting karena wewenang dan tanggung jawab pihak-pihak yang terlibat.

2.2 Fungsi *Hash* MD5

Fungsi hash adalah fungsi yang memetakan bit dengan panjang sembarang menjadi bit dengan panjang yang tetap yang disebut sebagai nilai *hash* (Hofheinz & Kiltz, 2012). Salah satu fungsi *hash* yang sering digunakan adalah MD5 karena memiliki kelebihan yaitu fitur *time stamping* (Sobti & Geetha, 2012) dan waktu komputasi yang relatif cepat (Rachmawati et al., 2018).

Fungsi hash MD5 terdiri dari lima tahapan yaitu penambahan *padding bit*, inisiasi MD *buffer*, memproses pesan dalam blok dengan panjang 16 kata, kemudian menghasilkan *output* sesuai dengan blok kata sebelumnya (R. Rivest, 1992). Ilustrasi fungsi MD5 dapat dilihat pada Gambar 1

Fungsi hash memiliki peranan penting dalam bidang keamanan data. Beberapa penerapan hash yaitu sebagai integritas data (Rasjid et al., 2017), keamanan *password* di *database* (Gauravaram, 2012), keamanan absensi (Sari & Abdillah, 2021), hingga *blockchain* (Wang et al., 2018).



Gambar 1 Ilustrasi fungsi MD5 (Aggarwal et al., 2014)

2.3 RSA

RSA merupakan salah satu algoritma kriptografi asimetris. Artinya kunci yang digunakan untuk enkripsi tidak sama dengan kunci yang digunakan pada proses dekripsi. Sebagai contoh ada dua orang yang ingin berkomunikasi secara rahasia yaitu Alice dan Bob. Mereka sepakat untuk menggunakan algoritma RSA untuk berkomunikasi. Ilustrasi dari cara kerja RSA adalah sebagai berikut (R. L. Rivest et al., 1978) (Boneh, 1999) (LIVINGSTON, 1956).

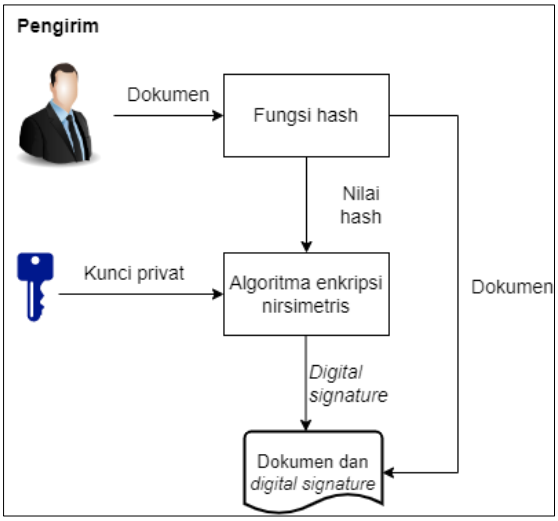
1. Alice dan Bob menentukan nilai N yang merupakan hasil perkalian dua buah bilangan prima p dan q atau dapat ditulis sebagai $N = pq$
2. Tentukan nilai e dan d yang memenuhi persamaan $ed = 1\ mod\ \varphi(N)$, dimana $\varphi(N) = (p-1)(q-1)$.
3. Pasangan berurut $\langle N, e\rangle$ kemudian dijadikan kunci publik dan pasangan berurut $\langle N, d\rangle$ adalah kunci privat.
4. Misal, Alice ingin mengirim pesan M kepada Bob, maka Alice mengenkripsi pesan M menjadi *ciphertext* C berdasarkan persamaan $C = M^d\ mod\ N$.
5. Untuk mendekripsi pesan dari Alice, Bob mengubah *ciphertext* C menjadi pesan M berdasarkan persamaan $M = C^d\ mod\ N$.

2.4 *Digital Signature*

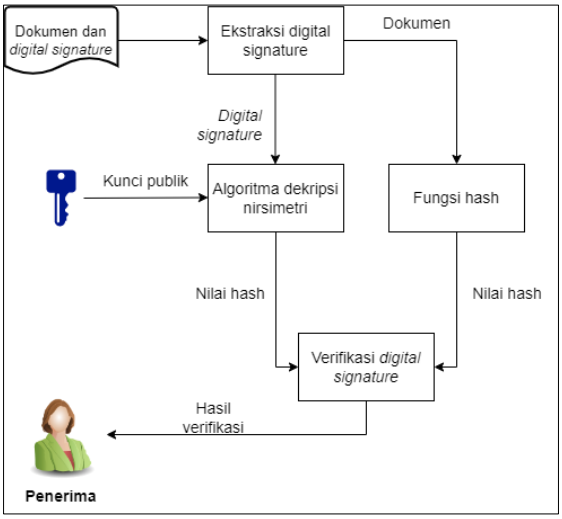
Cara kerja dari *digital signature* mirip dengan tanda tangan pada dunia nyata yaitu memberikan kepastian, autentikasi, dan verifikasi terhadap pengirim atau pemilik dokumen serta keabsahan isi dokumen (Sihombing, 2020).

Secara garis besar, skema *digital signature* memiliki dua proses utama yaitu penandatanganan dokumen dan verifikasi dokumen (Stallings, 2017). Pada proses penandatanganan, dokumen atau pesan yang akan ditandatangani dipetakan oleh fungsi hash menjadi nilai hash. Nilai hash dokumen akan

dienkripsi berdasarkan kunci privat milik pengirim sehingga menghasilkan sebuah blok pendek yang disebut sebagai *digital signature*. Setelah itu, Pengirim kemudian mengirimkan dokumen asli berikut *digital signature* (Kaur & Kaur, 2012). Ilustrasi dari proses penandatanganan dokumen ini dapat dilihat pada Gambar *2*.



Gambar 2 Proses penandatanganan



Gambar 3 Proses verifikasi

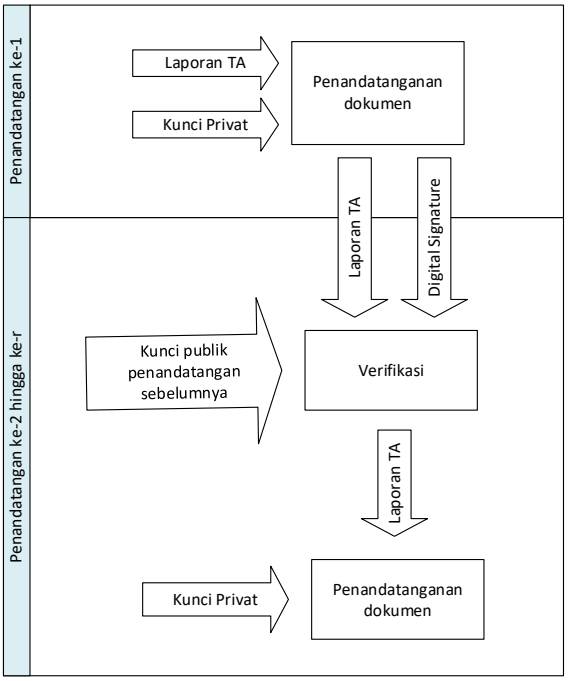
Untuk memastikan bahwa dokumen yang diterima belum mengalami perubahan dan dikirim oleh pengirim yang sah, maka proses verifikasi dilakukan. Pertama-tama, *digital signature* dipisahkan dari dokumen. Setelah itu, *digital signature* didekripsi dengan menggunakan kunci publik. Pada saat yang bersamaan, dokumen yang diterima juga dipetakan oleh fungsi hash menjadi nilai hash. Jika hasil dekripsi dan nilai hash dokumen sama, maka dapat dipastikan bahwa dokumen tidak mengalami perubahan dan dikirim oleh pengirim yang autentik [6]. Proses verifikasi *digital signature* dapat dilihat pada Gambar *3*.

3. Metode yang Diajukan

Pada dasarnya, *digital signature* konvensional hanya terdiri dari dua pihak yaitu pengirim dan penerima. Namun pada studi kasus ini penandatanganan laporan TA melibatkan banyak pihak. Oleh karena itu, perlu strategi khusus untuk menyelesaikan permasalahan tersebut.

Secara singkat, pihak yang menandatangani pertama kali hanya melakukan proses tanda tangan. Sedangkan pihak ke dua dan selanjutnya melakukan verifikasi terlebih dahulu sebelum menandatangani dokumen. Hal ini dilakukan karena pada prosedur pengesahan laporan TA di JTK POLBAN masih mengharuskan adanya citra tanda tangan penguji, pembimbing, dan ketua jurusan. Akibatnya, setelah satu pihak membubuhkan citra tanda tangan pada laporan TA, maka nilai hash dokumen laporan TA akan berubah. Sehingga untuk setiap proses tanda tangan oleh penandatangan ke dua dan seterusnya perlu diverifikasi untuk menjaga integritas dokumen.

Ilustrasi dari proses penandatanganan pada metode yang diajukan dapat dlihat pada Gambar 4.



Gambar 4 Ilustrasi metode penandatanganan yang diajukan

Beberapa notasi yang digunakan pada tulisan ini dijelaskan pada Tabel 1.

Tabel 1 Notasi yang digunakan

Notasi	Keterangan
$md5(a)$	Mengekstraksi nilai hash dokumen a dengan algoritma MD5
$E(h,p)$	Mengenkripsi nilai hash h dengan kunci privat p

Notasi	Keterangan
$D(s,q)$	Mendekripsi *digital signature* s dengan kunci publik q

Sebagai contoh, himpunan dosen penguji $U = \{u_1, u_2, \ldots, u_n\}$, himpunan dosen pembimbing $B = \{b_1, b_2, \ldots, b_m\}$, dan Ketua Jurusan (k) yang hanya ada satu orang. Maka himpunan pihak yang menandatangani (T) adalah

$$|T| = r = |U| + |B| + 1 = m + n + 1$$

Dengan urutan penandatanganan adalah $T = \langle u_n, u_{n-1}, \ldots, u_1, b_m, b_{m-1}, \ldots, b_1, k\rangle = \langle t_1, t_2, \ldots, t_r\rangle =$. Untuk itu, proses penandatanganan dan verifikasi dokumen laporan TA dibagi menjadi lima tahapan yang akan dijelaskan sebagai berikut.

3.1 Penandatanganan Oleh t_1

Sebelum proses penandatanganan dokumen, sistem akan membuat kunci privat $P = \langle p_1, p_2, \ldots, p_r \rangle$ dan kunci publik $Q = \langle q_1, q_2, \ldots, q_r \rangle$ untuk setiap pihak-pihak yang akan menandatangani. Pada studi kasus ini, penguji terakhir menjadi pihak pihak pertama yang menandatangani dokumen laporan TA dengan rincian langkah sebagai berikut.

1. Dokumen laporan TA (a) yang diberikan mahasiswa disisipi citra tandatangan dosen penguji dengan urutan terakhir (u_n). Setelah itu, diekstrak nilai hashnya dengan menggunakan fungsi MD5
$$h_1 = md5(a)$$
2. Nilai hash h_1 kemudian dienkripsi dengan menggunakan kunci privat penandatangan pertama (p_1) untuk menghasilkan *digital signature* pertama (s_1)
$$s_1 = E(h_1, p_1)$$
3. Sisipkan s_1 pada metadata dokumen laporan TA yang sudah disisipi citra tanda tangan $a_1$dan kirim ke penguji selanjutnya.

3.2 Penandatanganan Oleh $\langle t_2, .., t_r\rangle$

Sebelum menandatangani dokumen, penandatangan yang terdiri dari penguji u_{n-1} hingga penguji u_1 serta pembimbing b_m hingga pembimbing b_1 melakukan verifikasi terlebih dahulu.

Untuk setiap penandatangan selanjutnya t_i dengan $2 \leq i \leq r$ lakukan langkah-langkah berikut.

1. Dokumen yang diterima dipisahkan antara dokumen dan *digital signature*-nya
2. *Digital signature* didekripsi dengan menggunakan kunci publik miliki penandatangan sebelumnya.
$$h_{i-1}' = D(s_{i-1}, q_{i-1})$$
3. Ekstrak nilai hash dokumen yang diterima
$$h_{i-1} = md5(a_{i-1})$$
4. Bandingkan apakah $h_{i-1}' = h_{i-1}$. Jika sama maka proses dilanjutkan ke langkah selanjutnya. Jika tidak sama, maka proses berhenti.
5. Sisipi citra tanda tangan pada dokumen laporan TA dan ekstraksi nilai hashnya
$$h_i = md5(a_i)$$
6. Enkripsi nilai hash dengan kunci publik penandatangan
$$s_i = E(h_i, p_i)$$
7. Sisipkan s_i pada metadata dokumen laporan TA yang sudah disisipi citra tanda tangan a_i dan kirim ke penandatangan selanjutnya. Jika penandatangan adalah Ketua Jurusan, maka proses berhenti dan dokumen laporan TA dapat diverfikasi.

3.3 Verifikasi oleh Pihak Lain

Pihak lain yang menerima laporan TA seperti pihak perpustakaan, mahasiswa, atau pengunjung perpustakaan yang ingin menggunakan laporan TA sebagai referensi. Untuk memastikan integritas dokumen tersebut, maka proses verifikasi dilakukan. Langkah-langkah untuk verifikasi adalah sebagai berikut.

1. Dokumen laporan TA (a) yang diterima pihak lain dipisahkan antara dokumen dan *digital signature* (s_r) penandatangan terakhir yaitu Ketua Jurusan.
2. Ekstrak nilai hash dokumen laporan TA dengan menggunakan fungsi MD5
$$h_r = md5(a_r)$$
3. Dekripsi *digital signature* dengan menggunakan kunci publik penandatangan terakhir (q_r)
$$h_r' = D(s_r, q_r)$$
4. Bandingkan apakah h_r identik dengan h_r'. Jika iya, maka dapat dipastikan dokumen laporan TA tidak mengalami modifikasi.

3.4 Ilustrasi Metode yang Diajukan

Sebagai contoh, sebuah dokumen laporan TA akan ditandatangani oleh pihak-pihak dengan jabatan dan urutan tanda tangan seperti pada Tabel 2.

Tabel 2 Jabatan dan urutan penandatangan

Nama	Jabatan	Urutan Tanda Tangan
A	Penguji 3	1
B	Penguji 2	2
C	Penguji 1	3
D	Pembimbing 2	4
E	Pembimbing 1	5
F	Ketua Jurusan	6

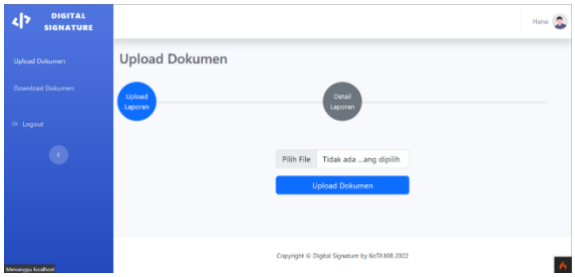
Misal nilai hash dari laporan TA tersebut adalah 876D271405F2AC6AF99994B708720206. Ilustrasi proses pada metode yang diajukan adalah sebagai berikut.

1. A menyisipkan citra tanda tangannya pada laporan TA sehingga nilai hash-nya tidak lagi sama dan berubah menjadi 5631F050295B46C7 03215BB5E70EC6C9.
2. A mengenkripsi nilai hash pada langkah 1 dengan menggunakan kunci privatnya. Hasil enkripsi disebut *digital signature* pertama atau s_1. Misal nilai s_1 adalah 7F7F3C8A445CC3 FEFB4470CAD8716522.
3. Sebelum menyisipkan citra tangannya, B akan mengecek integritas dokumen dengan mendekripsi s_1 dengan menggunakan kunci privat milik A. Sebagai contoh, dokumen laporan TA tidak dimodifikasi oleh pihak lain sehingga hasil dekripsi identik dengan nilai hash pada langkah 1. Jika ada indikasi dokumen dimodifikasi, maka proses berhenti.
4. B menyisipkan citra tanda tangannya sehingga nilai hash laporan TA tidak lagi sama seperti pada langkah 1 dan berubah, misalnya menjadi FF392DC6ABEF02CCDD93BB137A327C0B.
5. B mengenkripsi nilai hash pada langkah 4 dengan menggunakan kunci privatnya. Hasil enkripsi disebut *digital signature* ke dua atau s_2. Misal nilai s_2 adalah B9AA0EFBA715CE 41B53F1DE639C5B705.
6. Untuk C, D, E, dan F melakukan verifikasi dan menandatangani laporan TA seperti pada langkah 3, 4, dan 5.
7. Misal, nilai hash laporan TA yang sudah ditandatangani oleh ketua jurusan F adalah 16C9E2506CED86DC4DF564FC77AF7548 dan *digital signature* ke enam (s_6) adalah 50898011291E5A2CA524C7D8D6F52CC6. Agar pihak lain dapat mengecek integrasi dokumen, ia dapat mendekripsi s_6 dengan menggunakan kunci publik milik F dan membandingkannya dengan nilai hash laporan TA yang sudah ditandatangani oleh F.

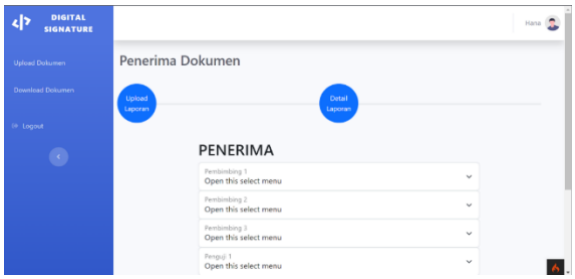
4. Implementasi

Berdasarkan metode yang diajukan, kemudian dibuat purwarupa aplikasi penandatanganan laporan TA di JTK POLBAN. Berikut adalah tangkapan layar dari purwarupa yang dibuat.

Setelah berhasil *login*, mahasiswa dapat mengunggah laporan TA yang akan ditandatangani pada halaman *Upload* Dokumen seperti pada Gambar 5. Setelah diunggah, mahasiswa dapat memilih siapa saja penerima dokumen yang dapat menandatangani dokumen pada halaman Penerima Dokumen seperti pada Gambar 6.



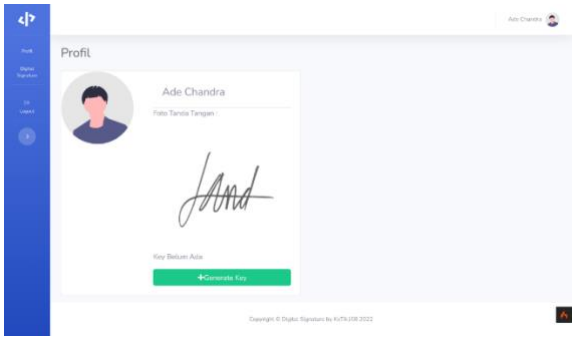
Gambar 5 Halaman Upload Dokumen



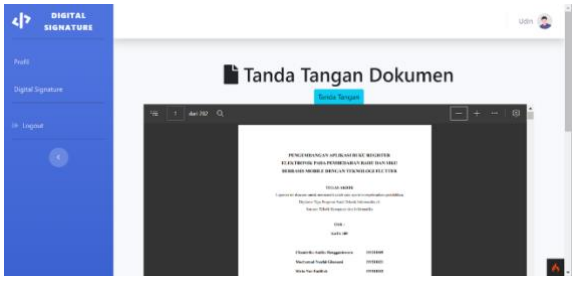
Gambar 6 Halaman Penerima Dokumen

Penerima dokumen, dalam hal ini adalah para dosen penguji, para dosen pembimbing, dan Ketua Jurusan dapat melihat daftar dokumen yang perlu ditandatangani pada halaman Daftar Dokumen seperti pada Gambar 7. Kemudian pilih dokumen yang akan ditandatangani dan unggah citra tanda tangan seperti pada Gambar 8. Citra tanda tangan tersebut akan disisipkan pada Lembar Pengesahan dokumen laporan TA seperti pada Gambar 9. Secara otomatis, aplikasi akan melakukan proses pembuatan *digital signature* seperti yang dibahas pada bab 3.2 dan 3.3.

Gambar 7 Halaman Daftar Dokumen

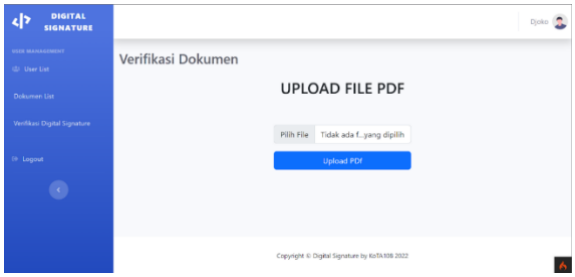


Gambar 8 Unggah citra tanda tangan

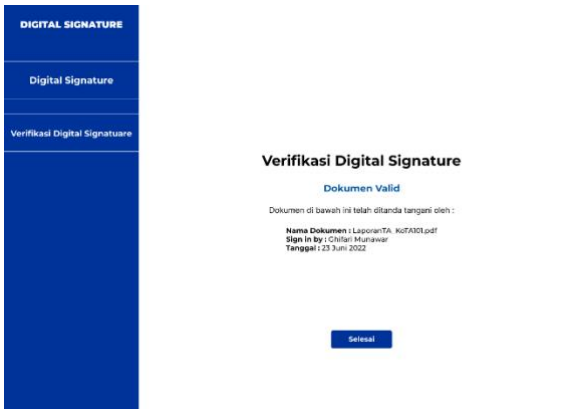


Gambar 9 Citra tanda tangan yang disisipkan pada Lebar Pengesahan

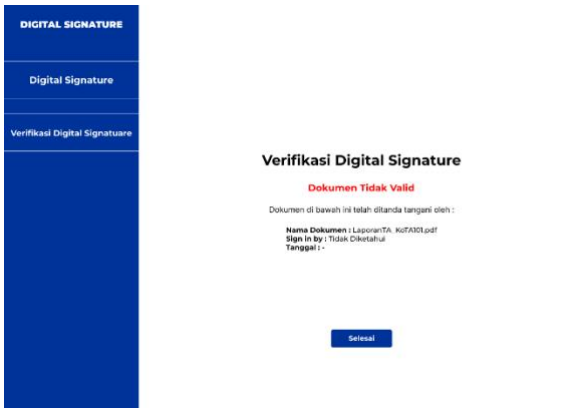
Untuk mengecek integritas dokumen, pengguna tidak perlu login dan hanya mengunggah dokumen laporan TA seperti pada Gambar 10. Setelah itu akan muncul hasil verifikasi dokumen tersebut seperti pada Gambar 11. Jika terjadi manipulasi pada dokumen, maka akan muncul tampilan bahwa dokumen tidak valid seperti pada Gambar 12.



Gambar 10 Halaman Verifikasi Dokumen



Gambar 11 Hasil verifikasi dokumen yang valid



Gambar 12 Hasil verifikasi dokumen yang tidak valid

5. Pengujian

Aplikasi purwarupa yang telah dibuat kemudian diuji untuk mengetahui fungsionalitasnya dengan pendekatan *black-box*. Hasil pengujian dapat dilihat pada Tabel 3.

Tabel 3 Hasil pengujian purwarupa

No	Pengujian	Hasil
1	Aplikasi dapat melakukan autentikasi pengguna	Berhasil
2	Aplikasi dapat mengatur otorisasi pengguna berdasarkan *role* pengguna yaitu mahasiswa, dosen pembimbing, dosen penguji, dan Ketua Jurusan	Berhasil
3	Mahasiswa dapat mengunggah laporan TA	Berhasil
4	Aplikasi dapat melakukan proses penandatanganan oleh dosen pembimbing, dosen penguji, dan Ketua Jurusan	Berhasil
5	Aplikasi dapat melakukan verifikasi dokumen	Berhasil

6. Kesimpulan dan Saran

Berdasarkan hasil pengujian, purwarupa dari metode yang diajukan dapat berfungsi secara baik. Selain itu, pada metode yang diajukan juga dapat menjaga integritas laporan TA. Hal ini terbukti karena perubahan satu bit saja pada dokumen laporan TA mengakibatkan nilai hash berubah dan tidak sama dengan hasil dekripsi *digital signature*-nya.

Namun, pada metode yang diajukan ini masih terdapat kelemahan yaitu pihak lain hanya dapat melakukan verifikasi terhadap dokumen laporan TA yang ditandatangani oleh Ketua Jurusan sebagai penandatangan terakhir. Hal ini dikarenakan pada metode ini hanya menerapkan konsep *digital signature* konvensional yang dilakukan secara estafet. Oleh karena itu, penulis menyarankan untuk menerapkan konsep *multisignature* untuk memungkinkan lebih dari satu pihak menandatangani dokumen yang sama.

Daftar Pustaka:

Aggarwal, S., Goyal Astt Professor, N., & Aggarwal Astt Professor MRCE, K. (2014). A review of Comparative Study of MD5 and SHA Security Algorithm. In *International Journal of Computer Applications* (Vol. 104, Issue 14).

Boneh, D. (1999). Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, *46*(2), 203–213.

Gauravaram, P. (2012). Security analysis of salt||password hashes. *Proceedings - 2012*

International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2012, 25–30. https://doi.org/10.1109/ACSAT.2012.49

Ghoshal, S., Bandyopadhyay, P., Roy, S., & Baneree, M. (2020). A journey from md5 to sha-3. *Trends in Communication, Cloud, and Big Data: Proceedings of 3rd National Conference on CCB, 2018*, 107–112.

Hofheinz, D., & Kiltz, E. (2012). Programmable hash functions and their applications. *Journal of Cryptology*, *25*(3), 484–527. https://doi.org/10.1007/s00145-011-9102-5

Kaur, R., & Kaur, A. (2012). Digital signature. *Proceedings: Turing 100 - International Conference on Computing Sciences, ICCS 2012*, 295–301. https://doi.org/10.1109/ICCS.2012.25

LIVINGSTON, S. (1956). Attacks on the RSA Twenty Years of Cryptosystem. *The New England Journal of Medicine*, *254*(26), 1211–1216.

Rachmawati, D., Tarigan, J. T., & Ginting, A. B. C. (2018). A comparative study of Message Digest 5(MD5) and SHA256 algorithm. *Journal of Physics: Conference Series*, *978*(1). https://doi.org/10.1088/1742-6596/978/1/012116

Rasjid, Z. E., Soewito, B., Witjaksono, G., & Abdurachman, E. (2017). A review of collisions in cryptographic hash function used in digital forensic tools. *Procedia Computer Science*, *116*, 381–392. https://doi.org/10.1016/j.procs.2017.10.072

Rivest, R. (1992). *The MD5 message-digest algorithm*.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126.

Sari, A. N., & Abdillah, T. G. (2021). Metode Absensi Mahasiswa berbasis QR Code dan Time-Based One-Time Password. *Jurnal Informatika Polinema*, *7*(2), 29–34. https://doi.org/10.33795/jip.v7i2.492

Sihombing, L. B. (2020). Keabsahan Tanda Tangan Elektronik Dalam Akta Notaris. *Jurnal Education and Development*, *8*,(No. 1), Hal. 134.

Sobti, R., & Geetha, G. (2012). Cryptographic Hash functions - a review. *IJCSI International Journal of Computer Science Issues*, *9*(2), 461–479.

Stallings, W. (2017). *Cryptography and Network Security Principles and Practice 7th Edition Global Edition British Library Cataloguing-in-Publication Data*.

Wang, M., Duan, M., & Zhu, J. (2018). Research on the security criteria of hash functions in the blockchain. *BCC 2018 - Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, Co-Located with ASIA CCS 2018*, 47–55. https://doi.org/10.1145/3205230.3205238