Aplikasi Digital Signature dengan RSA, Fungsi *Hash* Keccak dan Steganografi pada Lagu di Aplikasi Soundcloud

Pavita Andrea - 18220014 (*Author*)
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 18220014@std.stei.itb.ac.id

***Abstract*—Pada era digital ini, kreativitas manusia sangan didukung oleh hadirnya teknologi termasuk kreasi dalam bidang musik. Platform yang menyediakan layanan gratis untuk mengunggah hasil karya musik pun semakin banyak, dan salah satunya adalah SoundCloud. Namun dikarenakan platform bisa diakses bebas oleh siapapun maka integritas dari hak cipta sebuah lagu menjadi rentan akan plagiarisme. Oleh karena itu, solusi dari masalah ini adalah menggunakan tanda tangan digital dengan RSA, fungsi hash keccak dan steganografi untuk mencegah hal tersebut. Implementasi dari solusi ini menggunakan *local environment* dikarenakan penulis tidak memiliki akses pada keamanan di aplikasi SoundCloud. Pengujian yang dilakukan penulis semuanya berhasil sehingga dapat dinyatakan bahwa algoritma ini dapat berjalan dan bisa menyelesaikan masalah. Untuk kedepannya penulis berharap jika aplikasi SoundCloud dapat mengimplementasikan solusi ini pada aplikasinya.**

Keywords—SoundCloud; tanda tangan digital, RSA, Keccak, Steganografi, LSB, hak cipta musik

I. PENDAHULUAN

Pada era digital ini, kreativitas manusia semakin meningkat dan teknologi menjadi salah satu faktor pendukung hal tersebut. Kemajuan teknologi yang terus berlanjut tanpa henti saat ini memberikan dampak positif bagi berbagai industri, termasuk industri musik. Sebelum adanya teknologi yang canggih seperti saat ini, industri musik terbatas pada strategi pemasaran konvensional, termasuk bagi para musisi. Mereka harus mengandalkan label musik, mengirimkan demo, dan melakukan berbagai langkah lainnya, namun semuanya itu sudah tidak relevan lagi saat ini. Dengan munculnya berbagai platform musik yang mudah digunakan, dapat diakses oleh siapa saja, dan menjadi wadah promosi bagi musisi dari amatir hingga kelas internasional, ini merupakan perkembangan yang sangat menguntungkan.

Salah satu platform musik terbesar di dunia yang menawarkan akses gratis untuk siapa saja adalah SoundCloud. SoundCloud, didirikan pada tahun 2007, merupakan sebuah platform berbagi dan streaming musik. Sebagai salah satu platform streaming musik, SoundCloud memungkinkan pengguna untuk mengunggah, mempromosikan, dan berbagi lagu-lagu yang mereka miliki di profil mereka. Dengan demikian, SoundCloud menjadi platform penting bagi semua kalangan musisi, baik yang berada di tingkat amatir maupun profesional, untuk mempromosikan karya musik mereka.

Pada paragraf diatas telah disebutkan bahwa SoundCLoud menyediakan layanan gratis bagi seluruh pengguna untuk mengunggah karyanya, karena kebijakan ini maka SoundCloud harus lebih ketat dalam menjaga keamanan hak cipta dari musisi yang menggunakan aplikasi ini. Saat ini SoundCloud melakukan pemeriksaan dengan mengecek lagu yang akan diunggah dengan seluruh lagu yang ada di database SoundCloud. Lalu SoundCloud juga akan mengecek laporan plagiarisme lagu dari user. Namun untuk pengecekan dilakukan dengan menyamakan melodi dari lagu secara satu persatu yang membuat pengecekan lebih lama.

Oleh karena itu, untuk memudahkan pengecekan dan meningkatkan keamanan sebuah karya lagu dari plagiarisme maka bisa menambahkan digital signature pada sebuah lagu dengan menggunakan steganografi. Dengan demikian plagiarisme bisa diatasi di dalam aplikasi bahkan bisa diluar aplikasi dengan menambahkan fitur verificator pada aplikasi untuk pengecekan. Pada makalah ini akan diusulkan aplikasi dari tanda tangan digital dengan menggunakan RSA, fungsi hash keccak dan steganografi. Diharapkan implementasi ini dapat mencegah plagiarisme terhadap karya - karya pada SoundCloud dan melindungi hak cipta dari musisi - musisi di seluruh dunia.

II. DASAR TEORI

A. Tanda Tangan Digital

Tanda tangan digital merupakan suatu nilai kriptografis yang selalu unik antara satu dokumen dengan yang lainnya karena bergantung pada isi pesan dan kunci yang digunakan. Ada dua metode yang digunakan untuk menghasilkan tanda tangan digital, yaitu dengan mengenkripsi pesan dan menggunakan kombinasi fungsi hash dan kriptografi kunci-publik.

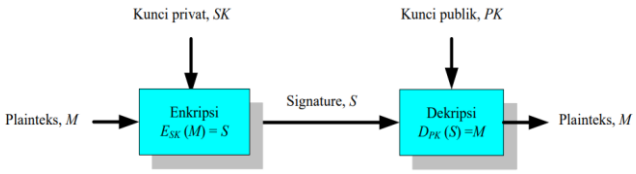
Metode mengenkripsi pesan dapat dilakukan dengan 2 cara yaitu bisa menggunakan kriptografi simetri ataupun kriptografi kunci publik.

Jika metode kriptografi simetri digunakan, enkripsi pesan menggunakan algoritma simetri dapat memberikan solusi otentikasi pengirim karena hanya pengirim dan penerima yang

mengetahui kunci simetri. Namun, metode ini tidak memiliki fitur yang dapat mencegah pihak yang terlibat untuk menyangkal atau menolak keterlibatan mereka (*non-repudiation*). Untuk mengatasi masalah ini maka dibutuhkan pihak ketiga atau penengah. Berikut adalah diagram alur dari metode kriptografi simetri dengan A adalah kunci simetri pengirim, B adalah kunci simetri penerima, E adalah fungsi enkripsi, M adalah pesan, dan S adalah tanda tangan digital.

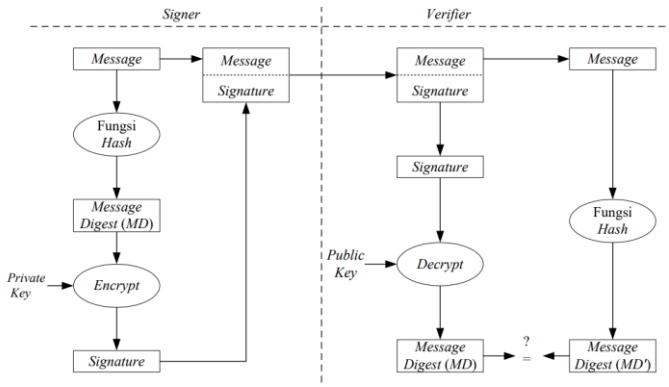
Gambar 2.1 Diagram alur tanda tangan digital menggunakan kriptografi simetri

Dalam penggunaan kriptografi kunci publik, pesan akan dienkripsi dengan menggunakan kunci privat pengirim. Kemudian, penerima akan mendekripsi pesan tersebut menggunakan kunci publik pengirim. Berikut adalah diagram alur dari metode kriptografi kunci publik.



Gambar 2.2 Diagram alur tanda tangan digital menggunakan kriptografi kunci publik. Sumber https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/21%20-%20Tanda-tangan-digital-2021.pdf

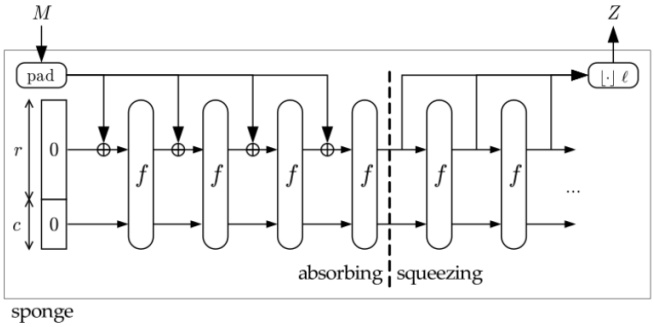
Dalam beberapa kasus, seringkali tidak perlu menjaga kerahasiaan pesan, tetapi penting untuk memastikan keaslian pesan dan memiliki mekanisme anti-penyangkalan. Untuk tujuan ini, kombinasi kriptografi kunci publik dan fungsi hash dapat digunakan. Tanda tangan digital dibuat dengan menghitung nilai hash dari pesan dan mengenkripsinya menggunakan kunci privat pengirim. Pengirim kemudian mengirimkan pesan beserta tanda tangan digital kepada penerima. Penerima akan mendekripsi tanda tangan digital dan membandingkan hasil hash dengan hash pesan yang dihasilkan oleh penerima sendiri. Jika nilai hash sama, berarti pesan yang diterima sesuai dengan yang dikirimkan. Sebaliknya, jika nilai hash berbeda, pesan telah mengalami perubahan. Berikut adalah diagram alur dari metode ini.



Gambar 2.3 Diagram alur tanda tangan digital menggunakan kombinasi fungsi hash dan kriptografi kunci publik. Sumber https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/21%20-%20Tanda-tangan-digital-2021.pdf

B. Fungsi Hash Keccak (SHA-3)

Fungsi hash Keccak, juga dikenal sebagai SHA-3, adalah sebuah algoritma kriptografis yang digunakan untuk menghasilkan nilai hash yang unik dari data input. Pada tahun 2015, fungsi hash Keccak (SHA-3) diadopsi sebagai standar oleh Institut Nasional Standar dan Teknologi (NIST). Fungsi hash Keccak (SHA-3) memiliki variasi dengan panjang output yang berbeda, seperti Keccak-224, Keccak-256, Keccak-384, dan Keccak-512. Fungsi hash Keccak (SHA-3) memiliki keunggulan, termasuk tingkat keamanan yang kuat dan kecepatan komputasi yang efisien. Fungsi hash Keccak (SHA-3) digunakan dalam berbagai aplikasi keamanan, seperti verifikasi integritas data, keamanan pesan, dan kriptografi publik. Fungsi hash keccak memanfaatkan konstruksi spons yang dapat dilihat pada diagram dibawah.



Gambar 2.4 Diagram konstruksi spons. Sumber https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/20%20-%20SHA-3-2020

C. Algoritma RSA

RSA adalah sepasang kunci kriptografi yang digunakan untuk proses enkripsi dan dekripsi. Algoritma ini dikembangkan oleh tiga peneliti MIT, yaitu Ronald Rivest, Adi Shamir, dan Len Adleman. Keamanan algoritma ini tergantung pada kesulitan dalam memfaktorkan bilangan prima yang sangat besar. Prosedur RSA dibagi menjadi 3 bagian utama yaitu, pembangkitan kunci, enkripsi dan dekripsi.

Pada bagian pembangkitan kunci akan dipilih 2 bilangan prima, misal p dan q untuk membangkitkan kunci. Lalu dibutuhkan bilangan hasil perkalian p dan q yang akan disebut sebagai n. Setelah menghitung n maka akan dihitung $\phi(n)$ yang memiliki persamaan sebagai berikut.

$$\phi(n) = (p - 1)(q - 1). \quad (1)$$

Setelah menghitung $\phi(n)$ maka akan ditentukan bilangan e sebagai kunci public dan e harus relative prima terhadap $\phi(n)$. Lalu hitung kunci deskripsi yang akan disebut sebagai d dengan persamaan sebagai berikut.

$$ed \equiv 1 \pmod{\phi(n)} \quad (2)$$

Pada tahap enkripsi maka pesan akan dibagi menjadi blok-blok plainteks. Lalu akan dihitung blok cipherteks untuk blok plainteks menggunakan kunci public e dengan persamaan sebagai berikut.

$$c = m^e \bmod(n) \quad (3)$$

Pada tahap dekripsi maka cipherteks akan dibagi menjadi blok-blok cipherteks. Lalu akan dihitung blok plainteks untuk blok cipherteks menggunakan kunci privat d dengan persamaan sebagai berikut.

$$m = c^d \bmod(n) \quad (4)$$

D. Steganografi

Steganografi adalah pengetahuan dan keterampilan dalam menyembunyikan pesan yang rahasia menggunakan metode tertentu, sedemikian rupa sehingga tidak ada yang curiga tentang keberadaan pesan tersebut. Terdapat 4 kriteria untuk menentukan apakah steganografi termasuk berkualitas atau tidak, yaitu sebagai berikut.

- *Imperceptible*
  Pesan rahasia tidak dapat dipersepsi secara visual atau secara audial dengan kata lain pesan sangat tersembunyi sehingga pesan tidak dapat diketahui hanya dengan dilihat atau didengar seperti biasa.
- *Fidelity*
  Penyisipan pesan rahasia tidak teralu mempengaruhi kualitas *cover-object*.
- *Recovery*
  Pesan tersembunyi harus bisa diekstrasi kembali.
- *Capacity*
  Ukuran pesan yang disembunyikan sedapat mungkin besar

Pada makalah ini digunakan metode steganografi digital untuk menyembunyikan kredensial dari sebuah lagu, sehingga metode steganografi yang paling cocok untuk kasus ini adalah LSB (*Least Significant Byte*). Metode ini merupakan metode yang paling popular dan memanfaatkan kelemahan pengamatan indra visual dan indra pendengaran manusia sebagai cara untuk menyembunyikan pesan rahasia. Metode ini mengubah nilai byte satu lebih tinggi atau lebih rendah dari nilai sebelumnya dengan mengacu pada bit pesan sehingga tidak berpengaruh terhadap persepsi visual maupun auditori.

III. Rancangan Solusi dan Implementasi

Berikut adalah rancangan solusi dan rancangan implementasi dari masalah yang telah disebutkan pada pendahuluan.

A. Rancangan Solusi

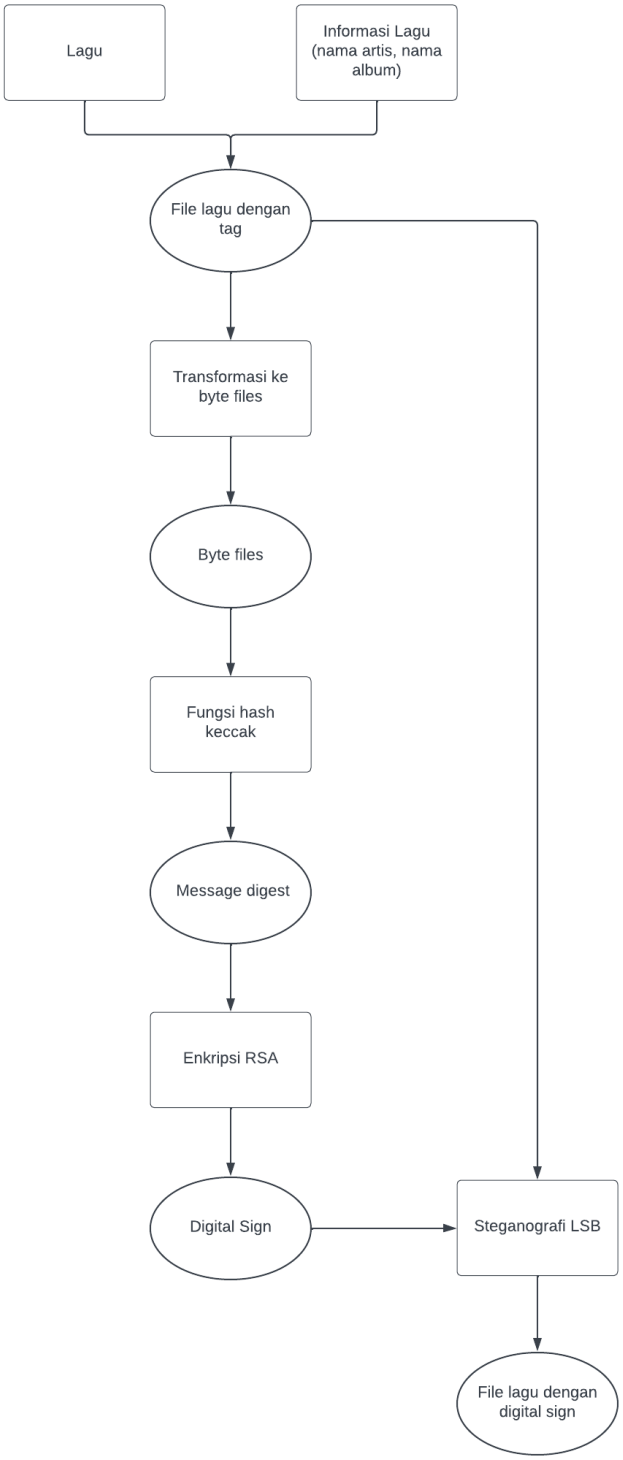
Seperti yang telah disebutkan pada pendahuluan rancangan solusi pada masalah ini adalah menambahkan digital sign menggunakan RSA, fungsi hash keccak dan steganografi pada lagu. Untuk menerapkan solusi ini maka akan dibagi dalam 2 proses yaitu penambahan digital sign dan verifikasi digital sign pada lagu. 2 proses ini akan dilakukan saat user akan mengunggah lagunya di aplikasi SoundCloud. SoundCloud akan melakukan pengecekan lagu dengan proses verifikasi untuk memastikan bahwa lagu yang diunggah tidak mengandung plagiarisme, setelah lagu terverifikasi maka lagu tersebut akan ditandatangani secara digital menggunakan RSA, fungsi hash keccak dan steganografi.

1) Tanda Tangan Digital

Pada tahapan tanda tangan digital akan digunakan RSA, fungsi hash keccak dan steganografi. Disini SoundCloud akan berperan sebagai issuer. Berikut adalah langkah - langkah untuk menambahkan tanda tangan digital pada lagu.

- Issuer menentukan pasangan kunci publik dan kunci privat
- Issuer akan membuat struktur file lagu dengan menambahkan tag data untuk nama artis, nama album, tanggal rilis, composer, lyricist, dan ID lagu pada lagu dengan menggunakan format ID3.
- File lagu yang telah disisipi tag akan diubah kedalam byte files
- Byte files di-hash menggunakan fungsi hash keccak dan menghasilkan message digest
- Message digest akan dienkripsi dengan kunci privat yang telah dibuat oleh issuer di awal untuk membentuk tanda tangan digital
- Tanda tangan digital yang telah dibuat akan disisipkan kedalam lagu menggunakan metode LSB
- Issuer mengunggah lagu pada platform SoundCloud dan kunci publik pada informasi lagu

Berikut adalah diagram alur dari proses penandatanganan digital pada lagu yang akan diunggah.



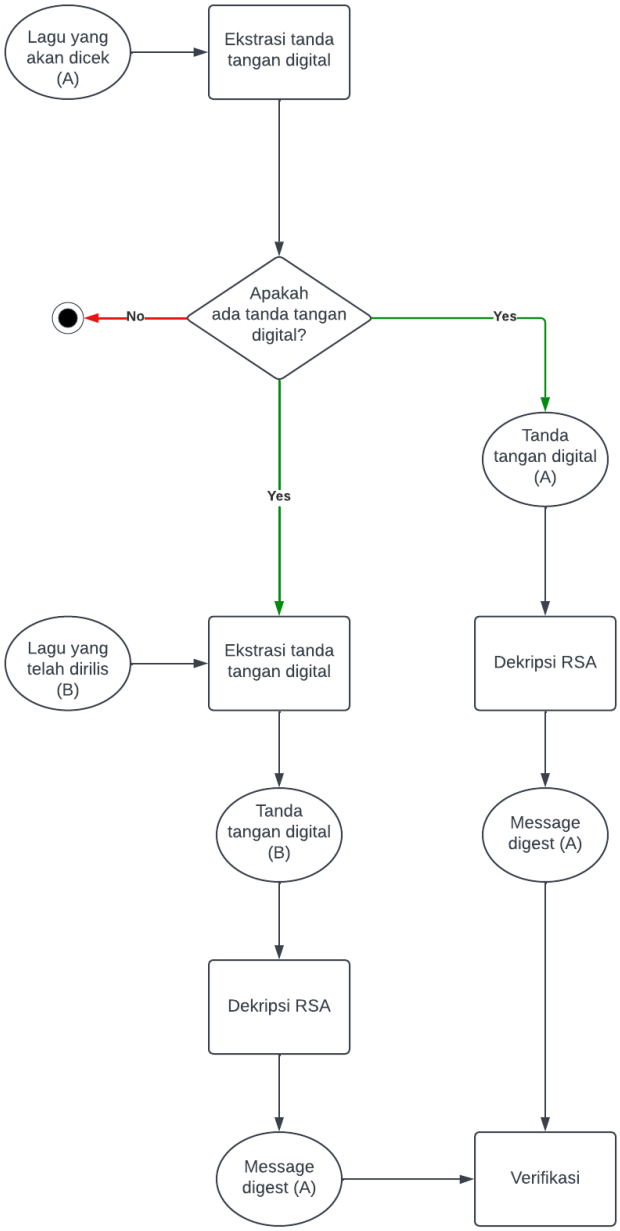
Gambar 3.1 Diagram alur dari proses penandatanganan digital

2) Verifikasi Tanda Tangan Digital

Pada tahap ini tanda tangan digital akan diekstraksi dari lagu yang diunggah untuk dicek apakah lagu ini memiliki tanda tangan digital yang sama dengan lagu lain atau tidak. Disini SoundCloud akan berperan sebagai verificator. Berikut adalah langkah - langkah untuk melakukan pengecekan tanda tangan digital pada lagu.

- Verificator menerima 2 file lagu yang akan dicek tanda tangan digitalnya. Yang satu adalah lagu yang akan dicek dan satu lagi adalah lagu yang sudah dirilis.
- Jika lagu yang akan dicek tidak memiliki tanda tangan digital maka lagu tersebut bukan plagiarisme
- Jika lagu tersebut memiliki tanda tangan digital maka lagu tersebut akan di dekripsi menggunakan RSA dengan kunci publik. Begitu juga lagu yang sudah dirilis, tanda tangan digitalnya akan didekripsi menggunakan RSA dengan kunci publik.
- Setelah dapat message digest kedua lagu maka akan dicek apakah message digest kedua lagu tersebut sama atau tidak, jika iya maka lagu tersebut adalah bentuk dari plagiarisme.

Berikut adalah diagram alur dari proses verifikasi pada 2 lagu yang akan dicek.



Gambar 3.2 Diagram alur dari proses verifikasi

B. *Implementasi*

Implementasi solusi dalam makalah ini akan berupa prototype dari ide solusi yang diajukan. Implementasi dari solusi akan menggunakan bahasa python. Disini system akan dibagi menjadi beberapa fungsi mengacu pada proses – proses yang ada dalam sistem.

1) Pembangkitan Kunci

Pada proses ini akan dibangkitkan kunci privat dan kunci publik. Dalam algoritmanya digunakan algoritma Rabin Miller untuk pengecekan bilangan apakah bilangan teresbut prima atau bukan. Algoritma Rabin Miller ditujukan untuk melakukan pengecekan bilangan yang sangat besar. Kunci publik akan disimpan dalam format .pub dan kunci privat akan disimpan dalam format .pri. Didalam file tersebut akan ada 2 bilangan yaitu n yang merupakan hasil perkalian p dan q, dan bilangan yang kedua adalah kuncinya. Kedua bilangan tersebut dipisah oleh simbol ",". Berikut adalah contoh hasil dari file kunci publik dan kunci privat.

Kunci Privat :

```
364241763957669360091163201131799316002377986852
475465941810508188937080807702821,18661207163254
457358241585696467540070613488661704411508472357
7702023201130592123
```

Kunci Public:

```
364241763957669360091163201131799316002377986852
475465941810508188937080807702821,31615179430580
732996851336166361239913840044759129519526911687
1838403787007852535
```

2) Penandatangan digital

Pada proses ini, tanda tangan digital akan dibangun menggunakan kunci privat. Namun sebelum itu file lagu akan di hash terlebih dahulu menggunakan keccak. Berikut adalah hasil dari tanda tangan digital.

```
294221928093848715482615498988508938566033507057
425013460750142932714286448352490
```

Tanda tangan digital tersebut akan disisipi kedalam lagu dengan metode steganografi LSB

3) Proses Verifikasi

Pada proses ini verifikasi terhadap 2 lagu akan dilakukan. Disini ada beberapa respon yang akan dikeluarkan untuk kasus kasus yang dapat terjadi pada proses ini. Berikut adalah respon yang dapat dikeluarkan oleh sistem.

TABLE I. RESPON VERIFIKASI

Kasus	Respon
Tidak ada tangan digital tidak ditemukan pada lagu	"Tidak ditemukan tanda tangan"
Tanda tangan digital pada lagu yang akan dicek dan lagu yang telah dirilis tidak sama	"Lagu tidak mengandung plagiarisme"
Tanda tangan digital ditemukan pada lagu yang akan dicek	"Lagu mengandung plagiarisme"

IV. RANCANGAN PENGUJIAN DAN PEMBAHASAN

A. *Rancangan pengujian*

Dikarenakan penulis tidak bisa mengakses sistem dari aplikasi SoundCloud, maka pengujian dilakukan dengan menggunakan local environment menggunakan Visual Studio Code sebagai IDE pembangunan algoritma.

Pengujian dilakukan sebanyak tiga kali untuk kasus yang berbeda dengan input yang berbeda. Berikut adalah kasus pengujian yang aka diuji.

TABLE II. RANCANGAN PENGUJIAN

No	Input	Ekspektasi Output
1	Lagu yang tidak memiliki tanda tangan digital	"Tidak ditemukan tanda tangan"
2	Kedua lagu yang memilki tanda tangan digital yang berbeda	"Lagu memilki tanda tangan digital yang berbeda"
3	Kedua lagu memiliki tanda tangan digital yang sama	"Lagu mengandung plagiarisme"

Berikut adalah hasil dari pengujian diatas menggunakan sistem yang telah dibangun pada *local environment* menggunakan python.

TABLE III. HASIL PENGUJIAN

No	Input	Output
1	Lagu yang tidak memiliki tanda tangan digital	"Tidak ditemukan tanda tangan"
2	Kedua lagu yang memilki tanda tangan digital yang berbeda	"Lagu memilki tanda tangan digital yang berbeda"
3	Kedua lagu memiliki tanda tangan digital yang sama	"Lagu mengandung plagiarisme"

B. Pembahasan

Berikut adalah pembahasan untuk pengujian yang telah dilakukan.

1) Lagu yang tidak memiliki tanda tangan digital

Pada kasus ini lagu yang diuji adalah lagu yang tidak memilki tanda tangan digital. Lagu yang tidak memiliki tanda tangan digital artinya belum pernah diunggah pada situs SoundCloud sehingga lagu ini dimasukkan pada lagu yang baru. Oleh karena itu output seharusnya menunjukan "Tidak ditemukan tanda tangan". Pada hasil yang telah diujikan, Ekspektasi output dengan output yang ada sama. Oleh karena itu, kasus ini berhasil

2) Kedua lagu yang memilki tanda tangan digital yang berbeda

Pada kasus ini kedua lagu yang memilki tanda tangan digital yang berbeda. Lagu yang memilki tanda tangan digital berarti lagu pernah diunggah pada SoundCloud, jika tanda tangan digital berbeda berarti lagu tidak memplagiasi lagu yang satunya lagi. Ekspektasi output pada kasus ini adalah "Lagu memilki tanda tangan digital yang berbeda". Hasil pengujian mengeluarkan output yang sama, oleh karena itu kasus ini berhasil.

3) Kedua lagu memiliki tanda tangan digital yang sama

Pada kasus ini kedua lagu memiliki tanda tangan digital yang sama. Jika kedua lagu memiliki tanda tangan digital yang sama maka sudah dapat dipastikan bahwa kedua lagu tersebut sama oleh karena itu respon yang diberikan adalah "Lagu mengandung plagiarisme". Hasil pengujian mengeluarkan output yang sama, oleh karena itu kasus ini berhasil.

V. KESIMPULAN DAN SARAN

Tanda tangan digital dengan menggunakan RSA, fungsi hash keccak dan steganografi LSB dapat disisipkan pada karya music seseorang untuk menjaga integritas dari lagu serta hak cipta dari lagu musisi tersebut. Dengan menggunakan local environment, tanda tangan berhasil dibangkitkan dan berhasil menangangi test case yang telah dibuat sesuai dengan tujuan dari makalah ini.

Untuk pengembangan di masa depan, algoritma yang telah dibuat bisa diimplementasikan dan di uji coba langsung pada aplikasi SoundCloud. Dengan demikian proteksi hak cipta dan integritas dari lagu – lagu pada platform SoundCloud lebih terjamin dan aman.

REFERENCES

[1] Timotius. (2020, February 18). Apa Itu SoundCloud? Mengapa Banyak Penggunanya? ToffeeDev; ToffeeDev. https://toffeedev.com/blog/apa-itu-soundcloud-mengapa-banyak-penggunanya/

[2] *Keccak Team*. (2022). Keccak.team. https://keccak.team/keccak_specs_summary.html.

[3] Conrad, K. (n.d.). *THE MILLER-RABIN TEST*. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf

[4] *What are SoundCloud's copyright policies?* (2021). SoundCloud Help Center. https://help.soundcloud.com/hc/en-us/articles/4402636813979-What-are-SoundCloud-s-copyright-policies-#:~:text=We%20are%20required%20by%20copyright,dispute%20with%20the%20reporting%20party.

[5] Munir, Rinaldi. 2022. Slide Kuliah II4031 Kriptografi dan Koding: Steganografi

[6] Munir, Rinaldi. 2022. Slide Kuliah II4031 Kriptografi dan Koding: Fungsi hash

[7] Munir, Rinaldi. 2022. Slide Kuliah II4031 Kriptografi dan Koding: Tanda-tangan digital (digital signature)

[8] Munir, Rinaldi. 2022. Slide Kuliah II4031 Kriptografi dan Koding: Fungsi hash SHA-3 (Keccak)

[9] Munir, Rinaldi. 2022. Slide Kuliah II4031 Kriptografi dan Koding: Kriptografi Kunci-Publik (Public-key Cryptography)

[10] Munir, Rinaldi. 2022. Slide Kuliah II4031 Kriptografi dan Koding: Algoritma RSA

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 22 May 2023

Pavita Andrea
18220014