

BAB 5 KESIMPULAN

5.1 Kesimpulan

Berikut kesimpulan dari Implementasi Algoritma BC3 dan RSA Dalam mengamankan data hak cipta lagu yang disisipkan pada *file* audio mp3 menggunakan Algoritma LSB adalah sebagai berikut :

1. Implementasi Algoritma BC3 dan RSA dapat berjalan dengan baik dalam mengenkripsi data, hal tersebut terlihat dalam pengujian bahwa setiap masukan data yang berupa plainteks akan berubah sepenuhnya menjadi cipherteks, hal itu didukung juga dari jumlah bit yang sama semua, yaitu untuk RSA masukannya adalah 11 karakter yang mana sedangkan di BC3 adalah 10 karakter, namun hasil dari tiap enkripsi berbeda-beda.
2. Implementasi Algoritma LSB dapat berjalan dengan baik dalam menyisipkan data hak cipta kedalam *file* audio mp3 dan mengekstraknya kembali, hal itu terlihat dalam pengujian encoding dan decoding yang mana hasil sebelum encoding sama dengan hasil setelah di decoding.
2. Kinerja Algoritma BC3 dan RSA dalam mengamankan data hak cipta sangat baik hal itu didukung dengan adanya modifikasi pada cipherteks dan cipherkey pada kedua buah algoritma dan menghasilkan bahwa semua data sangat sensitif terhadap perubahan bahkan untuk 1 bit saja, walaupun tidak 100% sensitif tiap blok data, hal itu dikarenakan jumlah karakter pada Base64 terbatas hanya berkisar 64 karakter dan ditambah lagi masukan hanya berupa angka yang mana hanya 9 karakter unik, oleh karena ada kemungkinan satu blok pada data sama nilainya, tapi kesamaan itu sangat acak, jadi bisa saja blok ke 1 pada data ke 1 yang sama tapi ketika dimasukkan ke data ke 2 maka blok yang sama tidak akan di posisi blok yang sama seperti data sebelumnya, hal itu dapat dilihat pada modifikasi BC3 yang mana masukannya hanya beda satu angka saja, namun kesamaan blok berbeda-beda posisinya, maka dari itu terlihat

bahwa kedua buah algoritma dalam mengamankan data hak cipta sangat terjamin.

3. Pengaruh implementasi BC3, RSA dan LSB dalam tujuan kriptografi pada pengamanan data hak cipta memenuhi hal tersebut yaitu :

- a. Kerahasiaan, implementasi BC3 dan RSA sangat aman dalam mengamankan data hak cipta lagu, hal itu dapat dilihat pada pengujian bahwa 100% data sangat sensitif baik itu ada perubahan 1 bit ataupun perubahan cipherkey, apalagi jika sudah menggunakan LSB dan di encoding menggunakan kunci publik RSA, yang mana hasil modifikasi kunci menunjukkan 100% data berbeda tiap blok nya yang menandakan data sangat sensitif terhadap perubahan sehingga data sangat terjamin kerahasiaannya karena hanya orang-orang tertentu saja yang bisa mengakses data dengan benar
- b. Integritas data pada implementasi ini menunjukkan jika kunci yang berbeda saat mendekripsi maka 100% data plainteks hasil enkripsi akan berbeda dengan plainteks asli, hal itu menandakan bahwa data memiliki integritas.
- c. Autentikasi data pada implementasi ini menunjukkan jika penerima hanya bisa menggunakan kunci dari pengirim yang menandakan bahwa data rahasia tersebut memang berasal dari pengirim, karena jika salah kunci maka hasil saat mendekripsi pesan akan berbeda dengan yang aslinya.
- d. Non Repudiasi, bukti jejak digital yang berupa data hak cipta lagu akan selalu ada dalam lagu, walaupun sudah di dekoding data rahasia akan tetap ada dalam lagu tersebut.
- e. Pertukaran Kunci, pada penelitian terjadi pertukaran kunci antara pengirim dan penerima dimana penerima hanya bisa menggunakan

kunci yang diberikan oleh pengirim, dimana jika kunci yang dimasukan salah maka data yang dihasilkan pun salah.

4. Dalam pengujian *Stegano file*, data asli dan data audio yang telah disisipkan data hak cipta memiliki kemiripan yang sama, sehingga ketika diputar lagunya orang tidak akan tahu bahwa lagu tersebut didalamnya ada data enkripsi, sedangkan jika data yang telah disisipkan kemudian di konversi ke format yang lain lalu dikonversi ke format seperti yang awal maka akan terjadi perubahan pada tiap bit didalam data sehingga saat menggunakan algoritma lsb, data tidak bisa ditemukan

5. Lama waktu enkripsi dan dekripsi, karena dalam penelitian ini memiliki inputan yang sama, maka tidak heran dalam penghitung waktu tidak berbeda satu dengan yang liannya, yang membedakan adalah proses ke-1 pada saat menenkripsi, hal itu dikarenakan waktu awal-awal sistem harus memerlukan waktu dalam memproses masukan, kunci, dsb tidak seperti proses enkripsi kedua sampai terakhir, maka dapat disimpulkan bahwa walaupun jumlah inputan yang sama tapi waktu memproses data berbeda-beda, namun semuanya sangat cepat, tidak lebih dari 1 milidetik

6. Lama waktu enkoding dan dekoding lebih lama dibandingkan dengan proses enkripsi dan dekripsi, pada enkoding saja rata-rata memerlukan waktu lebih dari 30 milisecond, apalagi jika dekoding yang mana rata-rata impelementasinya 0,7 detik, hal itu dikarenakan ada proses pembuatan file teks.