

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pemanfaatan Teknologi Informasi dan Komunikasi semakin berkembang pesat pada abad 21, hal itu ditandai dengan dimana pada abad ini informasi bukan suatu hal yang sulit untuk didapatkan (Utama, 2016). Salah satu pemanfaatan Teknologi Informasi adalah pemanfaatan data digital baik yang berupa teks, gambar, dan video.

Hak cipta yang merupakan salah satu data digital yang sering digunakan oleh seorang pencipta agar dapat memiliki hak istimewa terhadap karya cipta mereka, seperti mengumumkan, memperbanyak atau memberi izin ciptaannya menurut undang-undang. Penggunaan data digital yang berupa hak cipta rawan terkena penyalahgunaan, hal itu disebabkan karena dengan mudahnya konten digital yang dapat dipertukarkan melalui Internet sehingga mengakibatkan masalah pelanggaran, termasuk pelanggaran hak cipta (Vidyasagar M. Potdar, 2005). Salah satu pelanggaran hak cipta adalah penyalinan tidak resmi dalam skala besar, dan ini menjadi perhatian besar bagi industri musik, penerbitan film, buku, dan perangkat lunak (Petitcolas, Anderson, & Kuhn, 1999). Perkembangan Teknologi Informasi yang kian pesat mengakibatkan lebih banyak perangkat lunak pengolah media yang kuat dan komputer pribadi yang lebih cepat, hal tersebut menghadirkan tantangan untuk melindungi data hak cipta yang mana biasanya permasalahannya adalah tentang penyalinan dan distribusi digital tanpa izin (Wang, Doherty, & Dyck, 2002) .

Salah satu pemanfaatan hak cipta yang paling banyak adalah di industri musik, namun sama halnya dengan hak cipta pada umumnya, hak cipta pada industri musik sangat rentan sekali dengan penyalahgunaan, hal itu dapat dilihat mengapa pada tahun 1980an dimulainya era hak cipta pada industri musik, karena itu disebabkan oleh peristiwa dimana pada tahun 1985 yaitu negara-negara seperti Brasil, Columbia, Meksiko dan Taiwan dilaporkan mempunyai kaset bajakan yang terdiri dari 100% total pasar industri musik mereka (O'Regan, 1991). Kenapa bisa seperti itu, hal tersebut tidak terlepas dari lemahnya keamanan hak cipta pada penggunaan kaset yang mana pada

tahun 1985 masih banyak masyarakat yang menggunakan kaset sebagai media musik dibandingkan media lain seperti CD (Ullman, 2017). Apalagi pada era sekarang yang mana konsumsi musik sangat berpengaruh dengan penggunaan internet, bahkan pada tahun-tahun sebelumnya, sebelum pengguna internet tahun lalu yang mencapai 3,6 miliar (Commission, 2018), pada tahun 2005 pengguna internet yang masih ratusan juta yaitu 533 juta (Enrique Bigne, 2005), pada waktu itu penjualan musik rugi US\$ 3,1 miliar (tiga koma 1 miliar dollar Amerika) pada tahun 2005, hal itu disebabkan karena pelanggaran hak cipta (Sudip Bhattacharjee, 2003), bahkan pelanggaran hak cipta musik sangat besar bagi negara-negara berkembang seperti negara Indonesia dimana penyalahgunaan musik secara ilegal pada tahun 2017 mencapai 84% (Joost Poort, 2018). Salah satu pelanggaran hak cipta pada industri musik adalah proliferasi klaim pelanggaran hak cipta terhadap musisi seperti Robin Thicke, Justin Bieber, dan Bruno Mars, dimana kasus-kasus mereka adalah jeleknya regulasi dalam penanganan hak cipta musik yang menjadi pengingat betapa buruknya penggunaan hak cipta pada media yang satu ini, dan ada juga Gilbert O'Sullivan, yang menuntut hak cipta kepada Rapper Biz Markie untuk penggunaan tiga kata dan sebagian dari musik dari lagunya "Alone Again (Naturally)," (Kennedy, 2017).

Untuk mengatasi kelemahan pada penggunaan hak cipta, maka dibutuhkan sebuah teknik atau metode yang aman. Salah satu metode yang paling terkenal adalah metode dimana data atau informasi dapat disisipkan pada sebuah format multimedia atau biasa disebut dengan metode Steganografi. Steganografi (*steganography*) adalah teknik atau seni untuk menyembunyikan sebuah pesan rahasia di dalam sebuah *file* multimedia sehingga keberadaan pesan rahasia tersebut tidak dapat diakses oleh orang lain yang tidak mempunyai kewenangan (Anwar, 2018), atau bisa dikatakan Steganografi adalah sebuah metode dimana data penting (misalnya. pin identitas) dapat di implementasikan ke dalam sebuah media yang pada umumnya digunakan masyarakat (mis. *fingerprint*) tanpa pihak ketiga, yang mana media tersebut dapat dibagikan kesiapaapun tanpa memperlihatkan bahwa informasi tersembunyi itu ada (Mandy Douglas, 2017) misalnya dalam penelitian ini informasi yang disembunyikan

berupa data hak cipta. Metode Steganografi yang berbasis audio terdapat beberapa teknik dalam penyisipan pesan, salah satunya adalah metode *Least Significant Bit* atau biasa dikenal LSB yang merupakan cara paling sederhana untuk menanamkan informasi dalam sebuah *file* audio digital dengan mengganti bit paling tidak berpengaruh dari setiap titik pengambilan sampel dengan mengubah biner pada *file* tersebut (Ratul Chowdhury, 2016).

Tetapi hanya dengan penyisipan data hak cipta pada MP3 atau berkas audio saja tidak akan menjamin pesan tersebut aman dari luar, yang akan berakibat akan penyalahgunaan hak cipta, hal itu bisa saja terjadi karena steganografi rentan terhadap serangan analisis statistik dan proses steganalisis (Fatih Djebbar, 2012). Untuk mencegah hal tersebut penulis menggunakan metode *Blok Cipher* untuk mengenkripsi data pesan tersebut sebelum disisipkan ke dalam *file* MP3. *Blok Cipher* adalah algoritma deterministik pada kumpulan atau sekelompok bit dengan panjang tetap, yang mana sekumpulan bit ini disebut Blok (Hai Cheng, 2012). Namun dengan pesatnya perkembangan teknologi informasi, *Blok Cipher* mudah akan serangan dari luar, salah satunya adalah karena *Blok Cipher* versi awal (DES) hanya mendukung kunci dengan panjang 64 bit (Hai Cheng, 2012).

Oleh karena itu dalam skripsi ini menggunakan *Blok Cipher* versi terbaru sebagai metode enkripsi, yaitu *Blok Cipher 3*. *Blok Cipher 3* adalah algoritma *Blok Cipher* yang cukup mirip dengan AES dan Camellia, hal itu karena *Blok Cipher 3* dikembangkan dengan dua pertimbangan, pertama pertimbangan akan keamanan atau ketahanan *Blok Cipher* terhadap serangan dari luar dan yang kedua adalah efisiensi implementasi dari *Blok Cipher 3* (Arif Sasongko, 2011). *Blok Cipher 3* mendukung kunci sampai 128 bit atau lebih (Arif Sasongko, 2011).

Setelah dienkripsi data tersebut, dan disisipkan ke dalam *file* MP3, itu tidaklah cukup untuk mengamankan data pesan/hak cipta, maka diperlukan lah perlindungan ganda menggunakan sebuah metode dimana kunci dari data tersebut dapat di amankan, salah satunya adalah dengan metode enkripsi asimetris RSA. RSA adalah salah satu metode enkripsi asimetris yang paling banyak digunakan di seluruh dunia, algoritma

ini pada awalnya dikembangkan oleh Ron Rivest, Adi Shamir dan Leonard Adleman (Chaudhury, et al., 2017), pada tahun 1977 dan nama RSA muncul dengan menggunakan nama keluarga mereka (Liu, Gong, & Fan, 2018), metode ini juga dikenal sebagai algoritma kunci publik, dimana menjadi sangat populer karena kesederhanaannya dalam perhitungan (Fausto Meneses, 2016). Kelebihan dari metode ini adalah perhitungan untuk meng *generate* kunci dengan mudah namun sulit dipecahkan hal itu membuat metode ini sangat banyak digunakan karena dengan keadaan seperti itu keamanan sebuah data akan terjaga, karena sulitnya komputasi memfaktorkan produk dari dua bilangan bulat utama besar (jika ingin membobol algoritma ini) (Rui, Ju, & Guangwen, 2011), RSA juga merupakan salah satu algoritma kriptografi yang handal melawan *malware* pada sebuah sistem komputer (Sarika Khatarkar, 2015), adapun tahapan enkripsi Algoritma ini secara garis besar adalah dimulai dari pembangkitan kunci, enkripsi kunci publik, dan kunci pribadi /*Private Key* (Chu-Hsing Lin, 2014).

Setelah selesai menggunakan semua metode yang ada diatas maka data pesan atau hak cipta akan tersembunyi dalam media digital berupa audio dan data hak ciptanya pun sudah diamankan dengan metode enkripsi BC3 dan RSA. Pada skripsi kali ini mengapa membahas tentang mengamankan hak cipta, hal itu karena seperti dikatakan diatas MP3 adalah salah satu format multimedia paling populer terutama untuk mengkonsumsi musik . Ada miliaran MP3 yang tersebar di laptop, ponsel, Tablet, dan pemutar MP3 lainnya di Dunia. Pada tahun 2014, di di Amerika saja, 1, 1 miliar lagu yang berformat MP3 dibeli berdasarkan bayar per unduh dan 164 miliar dialirkan melalui langganan berbayar bulanan dan langganan yang didanai iklan (Denegri-Knott, 2015). Bayangkan saja jika ada orang yang curang memanipulasi hak cipta lagu seseorang, maka bisa dipastikan orang tersebut mendapatkan keuntungan yang sangat besar.

Oleh karena itu dengan banyaknya penyalahgunaan hak cipta, metode-metode diatas bertujuan agar dapat memberikan pengamanan ekstra terhadap data hak cipta, walaupun sudah ada beberapa penelitian yang meneliti bagaimana caranya

mengamankan data yang nantinya akan dimasukkan ke dalam media audio, seperti halnya penelitian pertama yang berjudul “*Implementation of Low Bit Coding Algorithm and Cipher Block with Electronic Code Book Mode for Data Legality in Audio Steganographic Streaming* “ yang mana mengamankan data hak cipta buku pada format mp3 menggunakan *Block Cipher* (Muhamad Nursalman, 2018) ataupun penelitian yang kedua berjudul “IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4 DAN METODE STEGANOGRAFI AUDIO 2LSB PADA SISTEM KEAMANAN INFORMASI” dimana pada penelitian ini yang menjadi fokus utamanya adalah melihat bagaimana pesan apapun itu, aman dengan di enkripsi terlebih dahulu menggunakan algoritma RC4 dan disisipkan menggunakan 2LSB yang nantinya dimasukkan ke dalam berkas audio (Apriyani, 2017). Adapun dalam penelitian ini menggunakan dua metode kriptografi yaitu RSA dan BC3 dan untuk menyisipkan pesan atau hak cipta yang terenkripsinya tersebut menggunakan metode steganografi yaitu LSB, jika dibandingkan dengan penelitian “*Implementation of Low Bit Coding Algorithm and Cipher Block with Electronic Code Book Mode for Data Legality in Audio Steganographic Streaming* “ dan “IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4 DAN METODE STEGANOGRAFI AUDIO 2LSB PADA SISTEM KEAMANAN INFORMASI”, penelitian ini memiliki kelebihan dibandingkan penelitian “*Implementation of Low Bit Coding Algorithm and Cipher Block with Electronic Code Book Mode for Data Legality in Audio Steganographic Streaming* “, karena pada penelitian ini menggunakan dua teknik kriptografi dalam pengenkripsannya, adapun versi *block cipher* nya pun sudah versi yang mana merupakan versi terbaru setelah *block cipher 2* (Arif Sasongko, 2011), adapun jika dibandingkan dengan penelitian “IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4 DAN METODE STEGANOGRAFI AUDIO 2LSB PADA SISTEM KEAMANAN INFORMASI” dimana penelitiannya menggunakan satu teknik kriptografi simetris yaitu RC4 yang mana masih lebih baik BC3 karena BC3 efisiensi algoritamanya 4x lebih cepat dari pada AES (Arif Sasongko, 2011) sedangkan untuk RC4 hanya 20% lebih cepat dibandingkan AES (Prabhudesai KevalKetan, 2012) ditambah dengan keamanan RSA yang mana lebih aman daripada RC4 (Akinyele A

Ariswara, 2020

IMPLEMENTASI ALGORITMA BLOK CIPHER 3 DAN RSA DALAM MENGENKRIPSI DATA HAK CIPTA YANG DISISIPKAN PADA AUDIO MP3 MENGGUNAKAN METODE LEAST SIGNIFICANT BIT

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

Okeola, 2015) sedangkan untuk teknik 2LSB lebih bagus daripada LSB karena daya tampungnya lebih besar (Apriyani, 2017), namun karena penelitian ini menggunakan data hak cipta lagu yang mana tidak terlalu besar maka LSB lebih cocok karena lebih efisien penggunaannya dibandingkan 2LSB.

1.2 Identifikasi Masalah

1. Banyaknya penyalahgunaan Hak Cipta terutama dalam industri musik yang berupa lagu.

1.3 Rumusan Masalah

1. Bagaimana implementasi algoritma RSA dan BC3 dalam mengenkripsi dan mendekripsi data hak cipta.
2. Bagaimana implementasi algoritma LSB dalam menyisipkan dan mengekstrak data hak cipta.
3. Bagaimana kinerja algoritma RSA dan BC3 dalam mengamankan data hak cipta terhadap perubahan data yang berupa kunci dan cipherteks.
4. Bagaimana pengaruh algoritma RSA, dan BC3 terhadap tujuan kriptografi.
5. Bagaimana kinerja *file* audio setelah dimasukan data hak cipta apakah ada perubahan atau tidak dengan cara melihat tingkat kenyaringan *file* audio tersebut, dan juga melihat apakah jika dikonversikan *file* audio bisa diekstrak atau tidak.
6. Berapa lama implementasi algoritma RSA dan BC3 dalam mengenkripsi dan mendekripsi data hak cipta.
7. Berapa lama implementasi algoritma LSB dalam menyisipkan dan mengekstrak data hak cipta.

1.4 Tujuan Penelitian

1. Mendapatkan hasil implementasi algoritma RSA dan BC3 yang nantinya akan dianalisis hasilnya untuk melihat apakah implementasi algoritma RSA dan BC3 dalam mengenkripsi atau dekripsi hak cipta sudah benar atau tidak.
2. Mendapatkan hasil implementasi algoritma LSB yang nantinya akan dianalisis hasilnya untuk melihat apakah implementasi algoritma LSB dalam menyisipkan dan mengekstrasi data hak cipta sudah benar atau tidak.
3. Mendapatkan data kinerja algoritma RSA dan BC3 dalam mengamankan data hak cipta terhadap perubahan cipherteks dan kunci, dan melakukan analisis data tersebut untuk melihat seperti apa kinerja algoritma RSA dan BC3 dalam mengamankan data hak cipta.
4. Mendapatkan data kinerja algoritma RSA, BC3, dan LSB dalam mengamankan data hak cipta terhadap perubahan cipherteks, cipherkey, dan melakukan analisis data tersebut untuk melihat seperti apa kinerja algoritma RSA dan BC3 terhadap tujuan kriptografi.
5. Mendapatkan data kinerja *file* audio setelah disisipkan data hak cipta kedalamnya dan setelah di konversikan kedalam format lain, dan melakukan analisis data tersebut untuk melihat apakah ada perubahan yang signifikan atau tidak terhadap kualitas *file* audio dengan alat ukur yaitu tingkat kenyaringan serta melihat apakah data hak cipta dapat diekstrak setelah di konversikan ke format lain.
6. Mendapatkan data berapa lama waktu algoritma RSA dan BC3 dalam mengenkripsi dan mendekripsi data hak cipta, dan melakukan analisis data tersebut untuk melihat apakah ada perbedaan lama waktu pada kedua buah algoritma kriptografi.
7. Mendapatkan data berapa lama waktu algoritma LSB dalam menyisipkan dan mengekstrasi data hak cipta, dan melakukan analisis data tersebut untuk melihat apakah ada perbedaan lama waktu pada saat proses encoding dan decoding.

1.5 Manfaat Penelitian

1. Bagi produser musik, penelitian ini dapat mengamankan karya musik mereka dari penyalahgunaan hak cipta
2. Bagi musisi, penelitian ini berguna dalam mengatasi orang lain menggunakan lagu mereka dan menjualnya tanpa sepengetahuan mereka
3. Bagi masyarakat umum, penelitian ini berguna untuk mengetahui apakah lagu yang mereka *download* itu legal atau illegal

1.6 Sistematika Penulisan

A. BAB 1 PENDAHULUAN

a. Latar belakang

Pada bagian ini menjelaskan mengapa memilih permasalahan hak cipta, mengapa metode RSA, BC3, dan LSB yang dipakai, dan perbandingan dengan penelitian sebelumnya.

b. Rumusan masalah

Pada bagian ini penulis melist apa saja rumusan masalah pada yang bisa diambil dari latar belakang masalah.

c. Identifikasi masalah

Identifikasi masalah berisi tentang bagaimana implemementasi metode yang dipakai sehingga menyelesaikan permasalahan yang ada.

d. Tujuan penelitian

Pada bagian ini membuat list yang mana berisi hasil yang akan didapatkan dalam implementasi point-point yang ada di identifikasi masalah.

e. Manfaat penelitian

Pada bagian ini memberikan point-point apa saja manfaat dari penelitian ini bagi masyarakat luas.

f. Sistematika penulisan

Berisi tentang ringkasan bab-bab yang ada pada penelitian ini.

B. BAB 2 KAJIAN PUSTAKA

Pada bab ini berisi tentang definisi, algoritma ataupun fungsi dari metode-metode yang dipakai dalam penelitian ini.

C. BAB 3 METODE PENELITIAN

Berisi tentang metode yang dipakai dalam membuat penelitian ini, bagaimana tahapan-tahapannya, bagaimana metode untuk alur sistem dalam implementasi metode-metode yang ada dalam mengamankan data hak cipta dan bagaimana gambaran kasar dari implementasi metode-metode yang ada baik berupa aplikasi ataupun diagram.

D. BAB 4 HASIL PENELITIAN DAN PEMBAHASAN

Berisi tentang pengujian dan pembahasan dari penelitian yang dilakukan menggunakan algoritma RSA, BC3, dan LSB.

E. BAB 5 KESIMPULAN

Berisi tentang kesimpulan setelah dilakukan pengujian dan implemmentasi pada penelitian.