Sebuah Rancangan Sistem Otentikasi File Musik untuk Toko Musik Digital dengan Menggunakan Digital Signature dan Kriptografi Kunci Publik

Marhadiasha Kusumawardhana / 13508091[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18091@students.if.itb.ac.id

***Abstrak*—Perubahan besar pada garis besar haluan industri musik saat ini sedang berjalan. Awalnya musik di simpan di media fisik seperti kaset dan CD, kini musik disimpan di media "gaib", yakni file musik seperti MP3, AAC, dan FLAC. Maka distribusi musik pun akan berubah dari toko musik retail fisik ke toko file musik yang beroperasi secara online. Masalahnya, file musik sangat mudah disalin dan disebar secara gratis. Bagaimana agar ekonomi file musik dan tokonya ini tetap bertahan? Pada makalah ini, penulis akan mencoba menyelesaikan masalah ini dengan memanfaatkan beberapa teori, yaitu teori *Digital Signature* (tandatangan digital) dan kriptografi kunci publik. Secara konsep, dengan penggunaan teori pada makalah yang penulis tulis ini, maka file musik tidak bisa didistribusikan secara sembarangan karena file musik tidak dnegan mudah dibuka oleh kakas pemain musik. Sehingga dengan penggunaan teori ini, ekonomi penjualan file musik masi mungkin tetap bertahan.**

***Index Terms*—Musik digital, toko musik, file musik, distribusi bebas, tandatangan digital, kriptografi kunci publik, ekonomi.**

I. PENDAHULUAN

Masih adakah orang yang mendengar musik dengan tape recorder, kaset, bahkan piringan hitam? Mungkin ada, namun mereka hanyalah enthusiast-enthusiast yang persentasinya sangat kecil dari mayoritas masyarakat di dunia saat ini yang menikmati musik dengan media digital. Namun, ada dua cara untuk menikmati musik dengan cara digital. Cara pertama adalah cara "fisik", atau dengan media berwujud seperti CD, DVD, dain lain sebagainya. Cara kedua adalah cara "gaib", yaitu dengan media file berwujud MP3, AAC, FLAC, dan lain sebagianya. Sekarang mari kita tanya diri sendiri. Berapa persenkah orang yang menggunakan media fisik digital (CD, misalnya) untuk mendengarkan mayoritas lagunya? Jawabannya tentu sangat kecil. Tren kini, musik bukanlah sesuatu yang berwujud yang bisa rusak atau hilang. Penyimpanan media musik kini adalah dalam bentuk file yang disimpan di sistem file komputer, tentunya lebih aman, tidak mudah hilang, dan tidak akan rusak. Musik disimpan dalam kondisi terkompres lossy, seperti MP3, AAC, dan sebagainya atau dalam kondisi lossless seperti FLAC, WAV, ALAC, atau AIFF.

Bisnis retail musik pun berubah drastis dengan perubahan trend penyimpanan media musik ini. Toko kaset sudah bisa dibilang punah. Walaupun masih ada (sangat sedikit), namun pasarnya sudah mayoritas hilang. Bagaimana dengan toko musik fisik (CD)? Lambat laun toko-toko ini akan hilang satu-persatu. Sebagai contoh, Aquarius di Dago yang mungkin 10-20 tahun lalu ramai, kini sudah tutup. Oleh karena itu, perubahan media musik ini merupakan peluang besar untuk membuka toko musik digital. "Toko" di sini bukanlah toko yang ada di pinggir jalan raya. Jelas, untuk hal digital, apalagi file musik yang berukuran relatif kecil (tidak lebih dari satu GB), delivery barang sangatlah tidak cocok bila secara fisik (dengan membuka toko retail di jalan). Dengan seiring berjalannya waktu, koneksi internet masyarakat semakin accessible dan semakin cepat. Oleh karena itu, toko musik digital haruslah online. Selain mudah dalam mengirim barang (download), toko online juga 24 jam tanpa perlu banyak karyawan (tidak perlu *storeclerk*, misalnya).

Namun, pengadaan toko musik digital ini tidak semudah menonton progress bar. Dengan mudah dan amannya penyimpanan musik digital, maka komputer dengan mudah juga menyalin file. Bagaiamana bila file musik yang kita jual itu disebarkan secara luas? Bukankah tiap orang tinggal menekan CTRL+C dan CTRL+V di mana pun kapanpun, maka file musik sudah bisa disebarkan. Dengan cara ini, tentunya penjualan file musik kita akan menurun drastis. Masyarakat tinggal menyalin file yang satu orang beli dari toko kita. Kita tidak mendapat keuntungan dari pasar yang luas dnegan fenomena ini. Oleh karena itu, sistem toko musik digital perlu sistem otentikasi dan keamanan yang baik agar sistem ekonomi musik digital juga tidak rusak.

Beberapa ilmu kriptografi yang sudah penulis pelajari di kuliah di ITB tentunya sangat berguna bagi saya dan tentunya dalam penyusunan makalah ini. Saya tentunya jadi memperoleh ide dan muncul buah pikiran tentang bagaimana membuat sistem otentikasi file musik bila kita ingin membuka toko musik digital online. Ilmu yang

berguna--salah satunya--adalah Digital Signature, dan algoritma kunci publik. Dari ilmu ini, saya menemukan ide untuk membuat sistem ini.

Untuk membuka toko musik digital, kita harus membuat sistem kemanan yang robust dan benar benar reliable. Tidak hanya pengamanan nomor kartu kredit, password, atau informasi pribadi, namun juga bagaimana sistem ekonomi yang dibentuk dari sistem toko musik digital ini pun tidak rusak dan hancur sehingga menyebabkan toko ini bangkrut. Bagaimana cara mengamankan sistem ekonomi ini? Tentunya kita harus membuat barang yang kita jual tidak menjadi "murah" dengan mempersulit file musik yang kita jual untuk disebarluaskan.

Beberapa batasan makalah, atau dalam kata lain, asumsi yang dipegang penulis adalah:

- Penegakan hukum hak cipta kuat. Bila penegakan hukum, terutama hukum hak cipta, lemah, maka sistem ini tidak berguna sama sekali (contoh negara yang penegakan hukum hak ciptanya lemah: Indonesia). Jadi, butuh kerja sama pihak kepolisian dan kesadaran masyarakat untuk menjalankan sistem ini.
- Kunci privat tidak disebarluaskan pengguna. Karena kunci nanti akan dienkripsi dan di simpan di sistem file pengguna, maka bahaya bila pengguna tahu letaknya dan bisa membukanya. Walaupun sudah disiapkan beberapa trik agar pengguna tidak menyebarkannya, tetap saja aspek dari sistem ini rawan.

Tujuan dari penelitian ini tentu saja adalah merancang sistem otentikasi file musik pada toko musik digital sehingga sistem ekonomi yang dibuat oleh toko musik digital online ini tetap stabil dan tidak rusak.

Manfaat dari penelitian ini ada dapat dilihat dari dua segi. Dari segi personal penulis, penulis dapat meluangkan ide penulis dalam makalah sehingga meningkatkan skill komunikasi penulis. Dari segi umum/kemasyarakatan, dari penelitian ini semoga dapat dibangun sistem otentikasi toko musik online sehingga ada sistem toko musik digital online yang berjalan dan sukses. Dengan begini, ekonomi dan konsumsi musik bisa menjadi sehat, legal, dan halal.

Penelitian yang akan penulis lakukan adalah dengan studi beberapa ilmu kriptografi seperti digital signature dan beberapa algoritma kunci publik. Selain itu, penulis akan mempelejari sistem yang digunakan pada sistem toko musik digital online tersukses, FairPlay dan membandingkannya dengan sistem ini. Selain itu, bila sempat dan ada waktu, penulis akan menlihat trend hacking dan pembajakan saat ini sehingga bisa membuat sistem ini kebal terhadapnya. Sekali lagi, bila penulis senggang dan sempat, sistem ini bisa saja dibuat secara prototipnya sehingga bisa dianalisis secara objektif.

II. Dasar Teori Algoritma Kunci Publik

Sejak zama dahulu, manusia sudah mencoba "menyamarkan" pesan yang dikirimkan khusus pada orang lain agar yang bisa mengerti pesan tersebut adalah orang yang dikirimkan saja. Proses atau peristiwa penyamaran pesan ini disebut dengan enkripsi. Biasanya pesan "dirusak" atau huruf-huruf dan informasi yang ada didalamnya diacak, diganti, dan lain sebagainya sedemikian rupa sehingga orang lain selain tujuan tidak dapat mengerti pesan tersebut. Biasanya, pesan itu dienkripsi dengan sebuah "kunci" atau secara matematis, "fungsi" yang mengubah dari pesan asli (setelah ini disebut plaintext) ke pesan yang disamarkan (setelah ini disebut ciphertext). Biasanya juga, dari fungsi pengenkripsi dapat diperoleh fungsi kebalikan yang bisa membalikan dari ciphertext menuju plaintext, atau prosesnya disebut dengan dekripsi.

Fungsi kebalikan (setelah ini disebut fungsi dekripsi) ini dengan mudah dapat diperoleh dari fungsi enkripsi. Artinya, biasanya relasi antar fungsi enkripsi dan fungsi dekripsi adalah 1-1. Oleh karena itu, bila fungsi enkripsi (atau sebaliknya fungsi dekripsi) diketahui orang banyak, maka percuma orang yang berkomunikais tadi mengirim pesan yang terenkripsi, karena orang lain bisa "membuka"nya dengan menggunakan fungsi-fungsi yang telah disebar tadi. Hal ini disebabkan fungsi enkripsi dapat diperoleh dari fungsi dekripsi dnegan mudah, begitu juga sebaliknya.

Namun, karena manusia pada dasarnya cukup pintar, mereka membuat bagaimana agar apabila salah satu dari fungsi enkripsi atau fungsi dekripsi tersebut disebarluaskan, maka ciphertext tetap tidak dapat "dibuka". Pengenkripsian dnegan fungsi-fungsi enkripsi atau dekripsi ini disebut dengan **kriptografi kunci publik**. Mengapa disebut kunci publik? Karena salah satu kunci (enkripsi atau dekripsi) bisa disebarluaskan (oleh karena itu, *publik*) namun ciphertext tetap tidak bisa sembarangan dibuka. Mengapa? Karena relasi fungsi enkripsi dan fungsi dekripsi tidkalah 1-1, tetapi 1-banyak, bahkan 1-"banyak sekali". Butuh "superman" untuk menebak fungsi yang tepat dari kemungkinan pasangan dari kunci publik tersebut.

Namun semua itu percuma dilakukan apabila kunci pasangan dari kunci publik disebarluaskan juga. Bila kunci yang satu lagi tersebut disebarluaskan, maka orang lain tinggal menggunakan salah satunya (pasti benar) untuk membuka pesan tersebut. Oleh karena itu, dari kedua fungsi tersebut haruslah satu buah saja yang disebarluaskan dan satu lagi wajib disimpan atau dirahasiakan. Maka dari itu, kunci pasangan dari kunci publik ini disebut dengan kunci privat.

Bagaimana kedua kunci dengan hubungan 1ke banyak ini dapat direalisasikan? Ternyata sistem kriptografi kunci publik ini benar-benar memanfaatkan teori-teori yang ada di bidang ilmu matematika. Pembangkitan kedua kunci

didasarkan pada dua persoalan matematika klasik, yaitu persoalan pemfaktoran dan logaritma diskrit.[1]

Pembaca sekalian pasti tahu apa itu pemfaktoran. Pemfaktoran adalah penentuan bilangan apa saja yang menjadi "dasar" atau kumpulan bilangan prima yang bila dikalikan menghasilkan bilangan yang difaktorkan tersebut. Sebagai contoh, 10 memiliki faktor 2*5, 60 memiliki faktor 2*2*3*5. Sejauh ini memang simpel, namun bagaimana dengan $2^{13} - 1$? Faktor dari $2^{13} - 1$ adalah 3391 * 23279 * 65993 * 1868569 * 1066818132868207. Luar biasa kan? Itu saja masih salah satu kemunkinan dari faktor-faktornya. Mungkin saja masih ada faktor-faktor lain yang bila dikombinasikan menjadi $2^{13} - 1$. Tidak hanya itu, walaupun semua faktor dapat ditemukan, namun secara komputasi, otak siapa yang bisa menemukannya dengan cepat. Pasti butuh waktu dan *effort* yang sangat lama (mungkin bertahun-tahun) untuk menemukannya. Bahkan algoritma komputer manapun sangat sulit untuk menemukannya dalam waktu singkat (butuh bulanan, bahkan tahunan). Algoritma kunci publik memanfaatkan sifat ini.

Salah satu teori matematis yang dimanfaatkan lagi adalah logaritma diskrit. Contoh persoalan algoritma diskrit adalah Temukan x sedemikian sehingga $3^x === 15$ (mod 17). Dapat ditemukan bahwa x = 6. Namun, menemukan jawaban itu saja sudah cukup lama dan sulit. Bagaimana bila 3 pada soal itu adalah 2^{13} - 1 , 15 pada soal itu adalah 644556, dan 17 adalah 13^8? Tidak hanya manusia yang sulit dan lama menemukan jawaban x, tetapi juga komputer. Butuh waktu tahunan untuk menemukan jawabannya. Kriptografi kunci publik memanfaatkan sifat ini.

Fungsi utama dari penggunaan kriptografi kunci publik adalah bahwa kunci publik dapat dipublikasikan namun pesan tetap terenkripsi dan sistem kriptografi tidak rusak. Kelemahan dari enkripsi biasa adalah harusnya sang pengirim untuk mengirim kunci untuk dekripsi pada sang penerima. Mengapa sebuah pesan dienkripsi? Agar pengendus atau orang lain tidak tahu artinya. Namun apabila kunci enkripsi dari pesan tersebut harus dikirimkan juga, maka bisa saja kunci tersebut ditangkap dan dibaca pengendus sehingga pengengkripsian tidak berarti karena kunci sudah diperoleh sang pengendus.

Kriptografi kunci publik dapat mengatasi masalah tersebut. Dengan mendekripsi dengan kunci privat dan mengenkripsi dengan kunci publik, maka walaupun kunci dikirim lewat saluran komunikasi yang tidak aman dan dapat diperoleh pengendus, pesan tetap tidak bisa dibaca karena untuk mendekripsi pesan tersebut butuh kunci privat. Sang pengendus hanya tahu cara menenkripsi pesan, namun tidak tahu cara mendekripsinya. Sistem otentikasi pada makalah ini memanfaatkan sifat kunci publik ini.

III. Dasar Teori Tandatangan Digital

Sejak zama dahulu, manusia sudah berusaha untuk membuktikan bahwa sesuatu (dokumen, barang, dll) berasal dari pihak tertentu, hanya pihak tersebut dan tidak mungkin pihak lain. Biasanya, untuk membuktikan bahwa sesuatu hal terasosiasi dengan suatu pihak tersebut adalah andanya tanda khusus atau "jejak" pada suatu hal tersebut yang menandakan bahwa hal tersebut berasosiasi dengan pihak yang memberikan tanda tersebut. Tanda ini biasa disebut dengan tandatangan.

Pada zaman sebelum luasnya penggunaan komputer biasanya untuk menandai bahwa suatu dokumen atau isi suatu dokumen disetujui atau berasal dari suatu pihak, biasanya dokumen tersebut diberi sebuah tandatangan. Tandatangan ini bisanya unik untuk suatu pihak, tidak sah bila digandakan, dan tidak dapat disangkal bahwa tandatangan tersebut berasal dari pihak yang memberinya.

Namun, pada zaman yang semuanya suda serba digital dengan komputerisasi? Masih valid dan digunakankah tandatangan? Tentu saja, pemberian tandatangan pada sebuah dokumen —atau apapun— yang berwujud file digital bisa diimplementasikan. Namun, bagaimana caranya?

Pada dasarnya, ada dua macam cara untuk mengimplementasikan tandatangan digital. Keduanya menggunakan ilmu kriptografi. Namun, jenis algoritma kriptografi dari kedua jenis cara tersebut berbeda secara prinsip. Jenis implementasi tandatanagn digital yang pertama adalah dengan teknik kriptografi simetri. Kriptografi simetri adalah cara mengenkripsi sesuatu dengan menggunakan kunci enkripsi dan dekripsi yang mana bila salah satu kunci diketahui, maka dengan mudah kunci yang lain diketahui. Cara tersebut sangat tidak praktis dan sangat jarang dipakai untuk pengimplementasian tandatangan digital. Oleh karena itu, pada makalah ini, penulis hanya berfokus pada jenis tandatangan digital dengan kriptograif kunci publik.

Seperti yang pembaca ketahui ada dua jenis kunci pada kriptografi kunci publik, yaitu kunci publik dan kunci privat. Salah satu dari tujuan penggunaan algoritma kunci publik adalah bahwa kunci publik dapat disebarluaskan dan enkripsi akan tetap bertahan. Namun, ada fungsi lain lagi dari kriptografi kunci publik yang dapat dimanfaatkan untuk implementasi tandatangan digital. Pada pemanfaatannya, kunci privat (kunci khusus yang hanya diketahui suatu pihak) dijadikan "penanda" bahwa suatu dokumen berasal dari pihak tersebut.

Seperti yang pembaca ketahui, sebuah kunci privat pasti mempunyai pasangan sebuah kunci publik. Kunci privat digunakan untuk mengenkripsi suatu dokumen dan kunci publik digunakan untuk membukanya (mendekripsi) dapat dijadikan skema untuk membuktikan bahwa sebuah dokumen benar-benar berasal dari pihak yang mempunyai kunci publik tersebut. Hal ini bisa dipahami karena kunci privat tersebut hanya dimiliki oleh satu pihak, yakni pihak tersebut. Selain itu, dengan cara ini, pengandaan atau pemalsuan tandatangan pastilah sangat sulit dilakukan.

Ada aspek lain dari konsep tandatangan digital ini. Bagaimana bila merahasiakan pesan tidak perlu dilakukan, yang perlu dicek hanyalah otentikasi pesan. Yang dimaksud dengan otentikasi pesan ini adalah bahwa pesan tidak diubah bila sang pengendus mengubah hash yang disisipkan di pesan menjadi hash yang dibuat oleh masukan pesan yang telah diubah. Oleh karena itu, butuh teknik agar isi hash ini tidak bisa diubah. Caranya adalah dengan memanfaatkan fitur algoritma kunci publik tadi. Benar, yautu dengan mengenkripsi hash yang disisipkan dengan kunci privat sang pengirim. Sang pengendus memang bisa membuka enkripsi ini, namun sang pengendus tidak bisa mengenkripsi hash palsu yang ia ingin sisipkan karena Ia tidak mengetahui kunci privat sang pengirim.

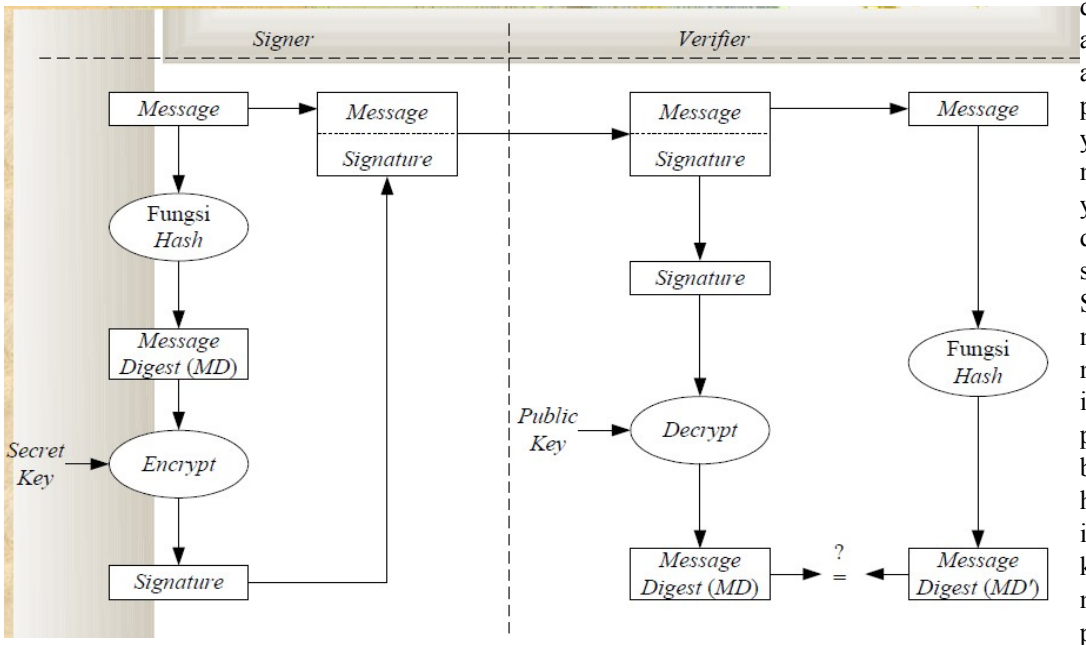

Illustration 1: Skema Implementasi Tandatangan Digital

bahwa pesan tidak berubah dari saat dibuat oleh sang pembuat (penandatangan) sampai dengan pesan ditangan sang penerima. Artinya tidak ada satu byte pun yang hilang, terganti, atau bertambah dari pesan tersebut. Di sinilah fungsi hash digunakan.

Fungsi hash adalah fungsi satu arah (tidak dapat dikembalikan, ireversibel) dari array of byte → array of byte dengan apabila ada satu perubahan array of byte masukan membuat array of byte keluaran berbeda jauh dengan array of byte keluaran bila array of byte masukan belum diubah. Selain itu, panjang array of byte keluaran fungsi hash ini tetap berapapun panjang array of byte masukan.

Karena jumlah array of byte keluaran biasanya tidak terlalu panjang (biasanya 20-40 byte), maka pengecekan dengan membandingkan hasil hash dari pengirim dengan hasil hash yang didapatkan penerima, maka otentikasi suatu pesan dapat diverifikasi. Hal ini disebabkan bila hash awal dengan hash akhir sama, maka pesan tidak berubah. Sebaliknya, bila ada satu byte saja yang berubah, maka hash akan berbeda.

Oleh karena itu, pada pengimplementasian tantatangan digital ini, hasil hash dari pengirim (hasil fungsi hash pesan asli yang dikirim oleh pengirim) disisipkan di pesan. Biasanya hash ini disisipkan di akhir pesan. Dengan cara ini, bila ditengah jalan ada yang mengubah isi pesan, sang penerima sudah bisa mendeteksinya dengan mengecek hash yang disisipkan dengan hash pesan yang baru ia terima.

Namun bagaimana bila selain mengubah isi pesan sang pengendus juga mengubah hash yang disisipkan di pesan? Sang pengirim tetap bisa tertipu dan menganggap bahwa

IV. Rancangan Sistem Otentikasi File Musik untuk Toko Musik Digital

3.1 Deskripsi Umum Toko Musik

Setelah pembaca mengerti dasar teori tandatangan digital dan kriptografi kunci publik, maka mari kita coba mengaplikasikan ilmu tersebut menjadi sebuah sistem yang aplikatif dan dapat digunakan. Sistem yang dibahas pada makalah kali ini adalah sistem otentikasi file musik.

Sebelum mendeskripsikan rancangan, penulis akanb mendeskripsikan kondisi atau bagaina sistem toko musik yang penulis maksud. Sistem toko musik ini terinspirasi dari toko musik digital yang paling sukses yang pernah ada, yakni iTunes Store. Walaupun agak berbeda, sistem ini cukup mirip dengan iTunesStore.

Intinya, ada tiga elemen komponen pada sistem ini. Komponen yang pertama adalah “client”, yaitu program music player, sebut saja “WaveHouse”. Komponen kedua adalah “server”, yaitu server “toko” yang menyimpan seluruh file musik yang dijual dan merupakan letak database tiap akun pembeli dan identitasnya, sebut saja “WaveHouse Store”. Komponen selanjutnya adalah “file”, yaitu file musik yang dijual oleh toko musik dan bisa dibuka dan dijalankan oleh client, sebut saja “WaveHouse Music File”. Perlu dicatat juga untuk berkomunikasi dengan server, client menggunakan sistem sendiri tanpa perlu perantara sistem lain. Sebagai contoh, apabila user ingin me”browse” toko, atau memilih-memilih file yang ingin dibeli, tidak boleh menggunakan web browser atau cara lain, harus lewat client resmi WaveHouse. Hal ini bisa dilakukan karena di dalam program client tersebut

sudah ter-embed web browser dengan protokol tersediri.

Ekonomi sistem toko musik tersebut adalah sebagai berikut. Client mendownload file ini dari server dengan akun yang mempunyai nomor kartu kredit. Dengan mendownload file ini lewat server, berarti akun yang digunakan client "membeli" file ini dan di*charge* akun di banknya sesuai dengan harga file musik tersebut.

3.2 Sistem Toko Musik Yang *Reliable*

Seperti yang sudah dibahas pada Bab I, sistem ini butuh sistem otentikasi dan keamanan yang reliable. Apabila tidak, maka ekonomi akan hancur. Pada dasarnya ada beberapa keadaan yang harus dipenuhi agar ekonomi toko musik ini tetap berjalan:

- File musik hanya dapat dijalankan pengguna yang memiliki akun yang membeli file tersebut.
- File musik dapat dibuka oleh client atau music player lain.
- Satu akun hanya boleh menggunakan satu buah komputer pada saat tertentu.

Mengapa poin pertama harus dipenuhi? Sebenarnya penjelasan mengapa pada poin ini adalah penjelasan "stating the obvious". Apabila hal ini tidak dipenuhi, maka siapapun bisa membuka file tersebut dan ini jelas merusak ekonomi dan membuat file yang server jual tidak berharga. Orang tidak akan mau mengeluarkan uang untuk mendapatkan file tersebut karena file tersebut sudah tersebar dan dapat didapatkan dengan mudah dan gratis. Oleh karena itu, kita harus menghalangi hal ini terjadi.

Poin kedua juga harus dipenuhi. Apabil player lain dapat membuka file ini, maka bisa saja sistem yang sudah kita gunakan untuk mencegah poin pertama di-bypass oleh program ini. Program "unofficial" ini tinggal membaca audiostreamnya saja tanpa perlu mengecek keaslian dan melakukan skema otentikasi yang dilakukan player official. Sehingga, sama saja, file bisa tersebar luas walaupun sudah ditambahkan skema otentikasi didalamnya apabila ada client lain yang bisa mem-bypass skema otentikasi ini. Oleh karena itu, diharuskan hanya satu jenis program yang bisa membuka WaveHouse Music File, yaitu WaveHouse (music player resmi dari toko yang menjual file musik tersebut).

Poin ketiga juga sangat penting. Sekarang, apabila sistem kita sudah mengotentikasi bahwa file musik ini hanya dapat dibuka oleh program WaveHouse dengan akun tertentu (akun yang membeli file tersebut). Namun, bagaimana bila sang pemilik akun menyebarkan password akunnya sehingga orang lain bisa berpura-pura menjadi orang yang membeli file tersebut? Apabila kasusnya seperti itu, maka percuma saja, file bisa tersebar ke siapapun asal dia dapat mengotentikasi bahwa dia adalah pemiliki file tersebut dengan menuliskan password akun yang membelinya. Ini jelas tidak boleh terjadi. Oleh karen itu, satu akun hanya dibolehkan membuka file-file yang ia beli dari satu komputer saat bersamaan, tidak boleh komputer lain.

3.3 Pendaftaran Pengguna

Setelah mengetahui apa yang harus dicegah untuk mendapatkan sistem ekonomi toko musik yang bertahan, sekarang penulis akan mendeskripsi sistem otentikasi tersebut sebelum melihat ke skema visual yang mudah dimengerti. Pertama-tama tiap pengguna harus memiliki akun untuk berbelanja di WaveHouse Store. Akun ini harus memiliki username yang unik. Untuk mendapatkan akun ini, pengguna harus mendaftar ke WaveHouse Store. Pengguna harus mendaftar lewat program WaveHouse tersebut.

Pada saat pendaftaran, tanpa diketahui oleh pengguna, program mengirimkan "Machine Code" atau kode mesin yang merupakan kode identifikasi komputer. Biasanya yang dijadikan kode mesin ini adalah alamat MAC dari kartu jaringan milik komputer tersebut. Apa guna dari kode ini? Fungsinya adalah pemenuhan poin ketiga, yaitu tiap akun memiliki hanya satu komputer "aktif", yaitu komputer yang bisa membuka file yang akun ini beli. Dengan mengirimkan kode komputer ini, maka sistem bisa mendeteksi bila komputer lain digunakan untuk membuka file yang akun ini beli.

3.4 Struktur File Musik

Agar file musik yang dijual tidak sembarang dibaca dan dijalankan oleh siapapun, maka file musik tersebut harus dibuat semacam sistem proteksi. Sistem ini seharusnya membuat bagaimana agar:

- File ini hanya bisa dibuka oleh player WaveHouse resmi.
- Di dalamnya ada semacam "tandatangan digital" untuk mengecek otentikasi file dan audiostream.
- File ini tidak bisa dengan mudah diedit, sehingga bisa mem-bypass sistem proteksi ini.
- Audiostream (musik) tidak bisa diekstrak sembarangan.

Berikut beberapa hal yang terkait file musik WaveHouse yang ada di benak penulis:

1. **Audiostream dikompresi.** Baik dengan kompresi MP3, AAC, apapun caranya tidak apa-apa, karena tidak berpengaruh pada sistem otentikasi. Audiostream adalah payload, bagian dari fileyang harus diproteksi sehingga tidak bisa dibaca dan dijalankan sembarang client.
2. **Disisipkan tandatangan digital diakhir audiostream.** Tandatangan digital ini berisi hash dari audiostream.
3. **Audiostream dienkripsi dengan kunci publik dan didekripsi dengan kunci privat**. Yang mengenkripsi adalah server (toko musik), yaitu yang mengirimkan file tersebut. Pihak yang mendekripsi adalah client dengan kunci privat yang sudah disimpan. Skema komunikasi pengiriman kunci akan dijelaskan kemudian. Kunci-kunci ini secara digenerasi secara random.
4. **Audiostream yang telah dienkripsi dan tandatangan digital dibungkus dan dienkripsi**

dengan skema enkripsi simetri yang canggih. Enkripsi yang canggih ini misalnya adalah kriptografi cipherblock yang dibuat sendiri oleh sistem toko musik (agar sulit memecahkannya) atau dengan algoritma canggih yang terkenal, misalnya AES.

5. **Kunci dari enkripsi yang dijelaskan poin 4 mengandung identitas akun pembeli file ditambah kunci khusus yang hanya pihak WaveHouse yang tahu.** Kunci khusus ini harus terembed di dalam binary program WaveHouse agar sulit untuk menebaknya. Selain itu, pihak toko musik juga **jangan sampai** menyebarkan kunci khusus ini. Bila disebarkan dan orang lain mengetahuinya dan mengetahui akun yang membeli file tersebut, maka orang lain tersebut dengan mudah membuka enkripsi file dan bisa mempelajari struktur file.

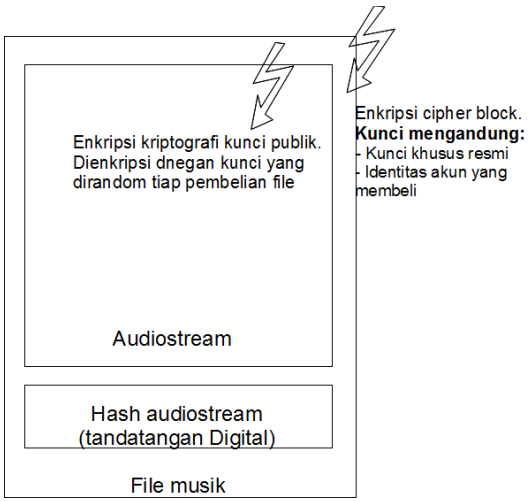

Illustration 2: Struktur file musik dengan sistem otentikasi ini

Intinya, di file musik ini ada audiostream (payload), atau stream musik yang dijalankan yang harus diproteksi. Audiostream ini dienkripsi dengan kriptografi kunci publik yang kuncinya digenerasi secara random setiap pembelian. Ada tandatangan digital yang disisipkan diakhinya untuk mengecek otentikasi apakah isi file sudah ada yang diubah. Akhirnya semua itu dienkripsi dengan kriptografi cipherblock yang canggih dengan kunci mengandung kunci khusus dari WaveHouse (agar hanya bisa dibuka player resmi) kunci khusus identitas akun yang membeli (agar hanya akun yang membeli yang bisa membukanya).

3.5 Gudang Penyimpanan Kunci

Seperti yang sudah dipaparkan di subab 3.4, audiostream yang ada di dalam file dienkripsi dengan kriptografi kunci publik yang digenerasi secara random di setiap pembelian. Artinya, setiap file musik mempunyai kunci yang berbeda-beda atau unik. Oleh karena itu, butuh sebuah "gudang kunci". Gudang kunci ini adalah sebuah file teks yang berisi daftar file musik dan daftar kuncinya. Saat audiostream ingin didekripsi music player membuka dulu gudang kunci ini dan mengambil kunci yang tepat untuk file musik yang ingin dibuka.

Fungsi gudang kunci ini adalah menyimpan semua kunci untuk setiap file musik yang dibeli pengguna. Kunci untuk membuka enkripsi audiostream ini adalah kunci privat, artinya kunci ini tidak boleh disebar, berpindah tangan, dan tidak boleh ketahuan siapapun. Apabila dipikir lagi lebih dalam, bahkan pengguna tidak juga boleh membuka kunci privat ini. Pengguna bisa saja menyebar kunci privat ini bila pengguna tahu karena pengguna tidak rugi bila menyebarkannya.

Agar pengguna dan siapapun tidak tahu isi gudang kunci ini, maka gudang kunci ini harus dienkripsi. Emkripsi yang digunakan adalah enkripsi canggih buatan WaveHouse sendiri (agar sulit dipecahkan) atau enkripsi cipherblock canggih yang terkenal seperti AES. Intinya, sama dengan pengenkripsian file musik.

Kunci untuk mendekripsi dan mengenkripsi gudang kunci ini haruslah mengandung **kunci khusus WaveHouse**, identitas **akun yang mempunyai** gudang kunci ini, dan **machine code yang dimiliki akun** tersebut. Jawaban mengapa harus kunci khusus WaveHouse dan mengapa harus ada identitas akun sudah ada di poin 5 di subab 3.4, yaitu agar hanya player resmi yang bisa membukanya dan hanya yang mempunyai akun tersebut yang bisa membukanya. Sedangkan kandungan ketiga, machine code yang dimiliki akun ini juga tak kalah pentingnya. Inilah yang membuat satu akun hanya boleh menggunakan satu komputer untuk membuka file-filenya. Tujuannya pun sudah dijelaskan di subab 3.2, yaitu mencegah penggunaan akun di banyak tempat.

Selain itu letak file gudang kunci ini benar-benar harus tersembunyi dan tersimpan dalam di dalam sistem file pengguna dan kalau bisa, jangan sampai pengguna mengetahui letaknya.

3.6 Pemindahan Komputer Pengguna

Pertanyaan selanjutnya, bagaimana bila pengguna mengganti komputer? Bukankah kunci pengenkripsi file gudang kunci mengandung machine code yang unik di

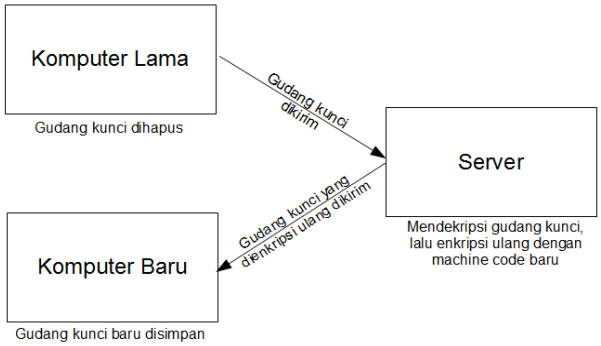

Illustration 3: Proses yang harus dilakukan pengguna untuk berpindah komputer

setiap komputer? Bagaimana bila kartu jaringannya diganti? Karena masalah-masalah ini, butuh sistem untuk mengganti machine code pengguna. Machine code pengguna ini selalu disimpan di server, oleh karena itu bisa diganti.

Di program client seharusnya ada pilihan untuk "meng-authorize" komputer baru, untuk mengantisipasi bila pengguna mempunyai komputer baru. Artinya mengubah machine code yang terasosiasi dengan akun tersebut (machine code komputer lama) menjadi machine code komputer baru.

Sistem otorisasi komputer baru ini juga tidak boleh sembarangan. Bila tiap komputer bisa diotorisasi menjadi dianggap milik suatu akun dengan hanya memberikan password akun tersebut tetap jelas sangat berbahaya. Bila pemilik akun tersebut menyebar passwordnya, maka tiap komputer bisa dianggap dimiliki akun tersebut dan penyebaran file musik secara ilegal menjadi mudah.

Karena kebijakannya adalah satu akun hanya memiliki satu komputer, maka seharusnya client tidak hanya memiliki fitur "Authorize Computer", tetapi juga "Deauthorize Computer". Artinya menghilangkan asosiasi komputer ini dengan suatu akun. Dengam men-"deauthorize" komputer tersebut, maka gudang penyimpanan kunci dikirimkan ke server dan disimpan server dan gudang kunci tersebut dihapus sehingga tidak ada lagi di komputer client. Dengan begini, komputer yang men"deauthorize" komputernya tidak dapat lagi memainkan file musik tersebut, atau sudah tidak "aktif" lagi.

Jadi, apabila ada komputer lain yang membuktikan bahwa ia adalah milik suatu akun (dengan memberikan passwordnya) pada proses "Authorize Computer", server seharusnya tetap menolaknya bila komputer tadi belum di "deauthorize". Dengan begitu, tidak bisa dua komputer yang aktif secara bersamaan. Oleh karena itu, untuk pengguna yang ingin mengganti komputernya, harus men"deauthorize" komputer sebelumnya dulu sebelum mengotorisasi komputer barunya.

Di atas telah dijelaskan bahwa dengan mende-authorize suatu komputer maka gudang penyimpanan kuncinya dikirim ke server dan dihapus dari client. Sebaliknya pada proses "authorize", server mengirim gudang penyimpanan kunci ke komputer baru. Pengenkripsian gudang kunci ini juga sudah harus berbeda dengan pengenkripsian sebelumnya, karena machine code komputer sudah baru. Oleh karena itu, server harus mendekripsi file gudang kunci tersebut, lalu mengenkripsinya lagi dengan kunci baru sebelum mengirimkannya ke komputer client. Tentu saja, dengan adanya gudang kunci tersebut, komputer baru ini sudah bisa menjalankan file musik yang dimiliki akun tersebut di komputer baru itu.

3.7 Proses Pembelian File Musik

Apa yang terjadi pada saat seorang pengguna membeli file musik? Seperti yang sudah dijelaskan di atas, bahwa tiap file musik yang dibeli pengguna apapun dan apapun judul lagunya itu pasti unik filenya. Hal ini disebabkan audiostream dari file tersebut dienkripsi dengan kriptografi kunci publik yang kunci-kuncinya digenerasi secara random di setiap pembelian.

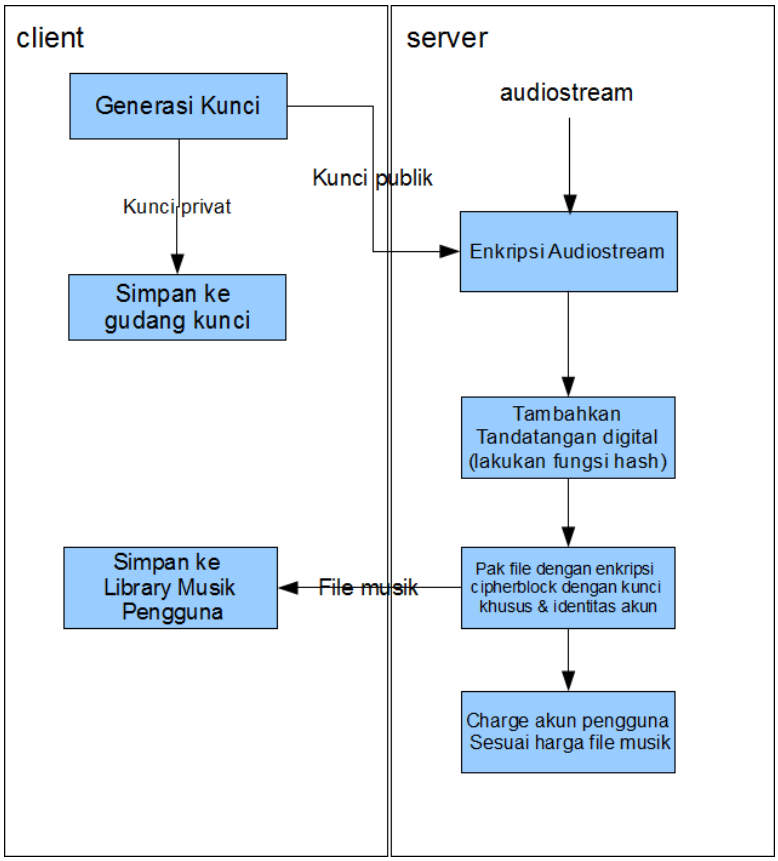

Illustration 4: Proses pembelian file musik

Berikut proses yang terjadi saat seorang pengguna membeli sebuah file musik. Pertama-tama client (client, *bukan* server) melakukan generasi kunci secara random. Dari generasi ini didapatkan kunci publik dan kunci privat. Kunci privat ini disimpan dan dimasukkan kedalam gudang penyimpanan kunci. Caranya program harus mendekripsi file gudang terlebih dahulu, lalu menambahkan kunci privat baru ini, lalu mengenkripsinya lagi. Ingat kembali bahwa hanya program resmi, akun yang mempunyai gudang tersebut dan komputer yang terdaftarlah yang bisa membuka gudang kunci tersebut. Lalu kunci publik hasil generasi tadi dikirim ke server. Keuntungan dari penggunaan kriptografi kunci publik ini adalah pengiriman kunci publik ini tidak perlu ada dalam jalur

komunikasi yang aman.

Setelah kunci publik dikirimkan ke server, server akan mem-"paket" file musik untuk dikirmkan ke client. Server mengenkripsi audiostream dengan kunci publik ini, menambahkantandatangan digital, lalu membungkusnya menjadi suatu file musik yang telah terenkripsi. Ingat kembali bahwa kunci enkripsi file musik adalah kunci khusus WaveHouse dan identitas akun pembeli. Karena server mengetahui semua informasi tersebut (akun yang membeli diketahui server), maka pemaketan file ini bisa dilakukan di server. Setelah paket file musik terwujud, kini server tinggal mengirimkan file musik ini ke client.

File yang diteirma client ini tidak hanya sudah bisa dinikmati oleh client, tapi juga sudah terproteksi agar hanya client itu dan komputer itu saja yang bisa menjalankan file tersebut.

3.8 Proses Memainkan File Musik

Setelah mengetahui struktur dari file musik, gudang kunci, dan proses membeli file musik, kini mari kita bahas proses yang terjadi pada saat menjalankan file musik resmi yang sudah diproteksi khusus tersebut. Proses ini harus juga buka proses biasa karena bertujuan menjaga agar hanya player resmi yang bisa memainkan file musik tersebut, hanya akun yang membelinya dan hanya dikomputer yang machine codenya terdaftar milik akun tersebut.

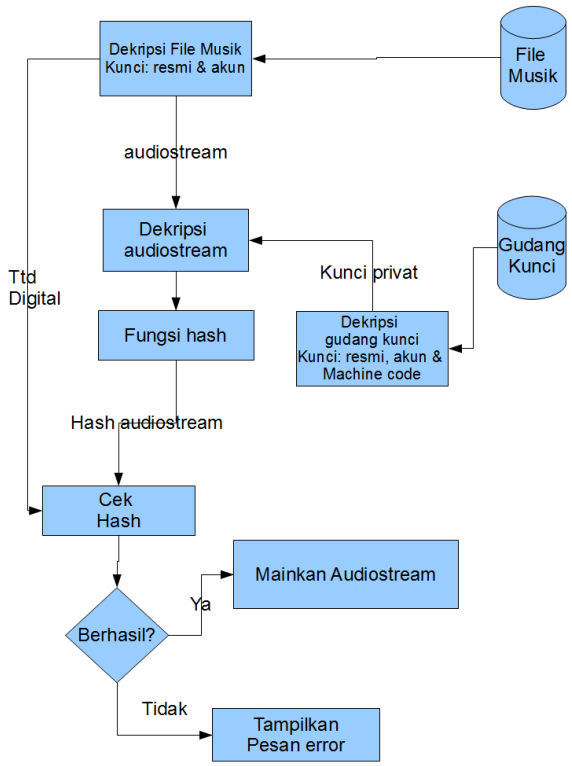

Illustration 5: Urutan Proses memainkan File Musik

Pertama-tama, player resmi mendekripsi file musik tersebut dengan kunci. Kunci ini, seperti yang telah dijelaskan sebelumnya, mengandung dua informasi. Yaitu, kunci khusus yang hanya diketahui player resmi dan identitas akun yang membelinya. Karena setiap client (player) mempunyai akun yang terasosiasi dengannya, maka informasi akun diperoleh. Dengan kunci ini player bisa mendekripsi file musik tersebut.

Setelah itu, player mendekripsi audiostream. Pertama-tama player membuka gudang kunci. Gudang kunci, seperti yang dijelaskan sebelumnya, memiliki kunci yang mengandung informasi kunci khusus, identitas akun, dan machine code. Kunci khusus diperoleh karena player tersebut adlah player resmi, begitu juga identitas akun. Machine code diperoleh dengan mengambil informasi alamat MAC dari kartu jaringan. Dengan kunci ini gudang penyimpanan kunci bisa dibuka.

Setelah membuka gudang kunci, kini giliran mencari kunci mana yang sesuai dengan file musik tersebut. Setelah mendapatkannya, gunakan kunci privat yang diperoleh untuk mendekripsi audiostreamnya.

Sebelum menjalankan audiostream yang bisa dibuka tersebut, player harus mengecek otentikasinya dengan membandingkan hasil hash audiostream tersebut dengan tandatangan digital yang tersisipkan di akhir file. Bila gagal, maka player menolak untuk membuka file dan memberikan pesan error (otentikasi gagal). Bila otentikasi berhasil, maka audiostream tersebut bisa di akses player untuk dimainkan.

V. Analisis Ketahanan Sistem Terhadap Beberapa Serangan

Sekarang mari kita cona melakukan serangan "imajinatif" kepada sistem untuk membuktikan bahwa sistem ini cukup reliable untuk diimplementasikan pada toko musik dijital. Serangan yang dicoba bertujuan bukan untuk merusak client atau merusak server, melainkan serangan yang bertujuan mencari bagaimana caranya agar file musik yang dibeli suatu pengguna dapat disebarluaskan dengan mudah. Kita mencari contoh serangan dari yang paling naif sampai yang agak canggih.

- **Pengguna menyebarluaskan file dengan copy paste biasa (CTRL+C + CTRL+V).** Untuk membuka file, butuh player resmi karena file terenkripsi dengan kunci khusus resmi dan kunci identitas akun pembeli. Walaupun tujuan salinan membukanya dengan player resmi, kalau akun yang terasosiasi dengan player resmi tersebut bukan akun pembeli, file tetap tidak bisa dibuka.
- **Pengguna menyebarluaskan file dengan copy paste biasa (CTRL+C + CTRL+V) dan menyebarkan password akunnya.** Dengan cara ini, player tetap tidak bisa menjalankan file tersebut. Hal ini disebabkan sistem ini butuh proses "authorize" dan "deauthorize" kompuer bila ingin menggunakan dua kmputer dengan

player yang terasosiasi dengan akun yang sama. Selain itu, gudang penyimpan kunci tujuan juga pasti berbeda kunci untuk membukanya.

- **Pengguna menyebarluaskan file dengan copy paste biasa (CTRL+C + CTRL+V) dan menyebarkan password akunnya, sekaligus menyebarkan gudang kuncinya.** Sekali lagi, karena sistem ini membutuhkan proses "authorize" dan "deauthorize", serangan ini tetap tidak berguna. Apabila gudang kunci di copy-paste, player yang menyalin tetap tidak bisa membuka gudang kunci karena machine code yang digunakan untuk mengenkripsi gudang kunci berbeda dengan tempat file tersebut disalin.
- **Membuat player tidak resmi untuk mengekstrak audiostream dan menjalankannya.** Cara ini jelas tidak bisa dilakukan karena file telah dienkripsi dengan kunci khusus yang hanya diketahui player resmi. Kunci ini juga rahasia dan tersimpan di dalam binari kode player, sehingga susah dilihat.
- **Pengendus meng-intercept komunikasi client-server saat proses pembelian.** Tetap tidak berguna. Komunikasi antar client dan server adalah pengiriman kunci publik dan pengiriman file. Apabila pengendus mendapatkan kunci publik dan file yang dibeli, pengendus tetap tidak bisa membuka file tersebut karena kunci untuk mendekripsi audiostream adalah kunci privat yan tidak pernah dikirimkan lewat jalur komunikasi apapun (disimpan secara offline). Selain itu, dan file juga terenkripsi.

VI. KESIMPULAN

Dari rancangan di atas dan ketahanan sistem tersebut terhadap serangan-serangan yang digunakan untuk menyebarluaskan file musik, dapat disimpulkan sistem ini cukup handal dalam mempertahankan ekonomi sistem toko musik. Yaitu dengan mencegah penyebarluasan file musik yang dijual oleh toko musik secara ilegal.

REFERENSI

[1] Munir, R. "Sistem Kriptografi Kunci Publik" di Slide Kuliah Kriptografi. Sekolah Teknik Informatika ITB, 2011.

[2] Munir, R. "Tandatangan Digital" di Slide Kuliah Kriptografi. Sekolah Teknik Informatika ITB, 2011.

[3] http://en.wikipedia.org/wiki/FairPlay , diakses 26 April 2011 ~21.00

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, 29 April 2010

Marhadiasha Kusumawardhana / 13508091