Aplikasi Kriptografi dalam Digital Rights Management

Mohd. Akbar[1], Fendi Wiracandra[2] dan Muhammad Rayhan[3]

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : *if12053@students.if.itb.ac.id*[1],*if12060@students.if.itb.ac.id*[2],
if12080@students.if.itb.ac.id[3]

Abstrak

Konten digital dapat didefinisikan sebagai objek-objek yang direpresentasikan dalam bentuk digital. Buku, lagu, gambar bisa direpresentasikan sebagai konten digital. Konten digital mempunyai kelebihan dari konten dari bentuk nyatanya, terutama dari sisi kompaknya ukuran, kemudahan distribusi dan kemudahan penggunaan. Namun hal ini juga membawa dampak buruk karena konten digital sangat mudah dibajak dan disalahgunakan. *Digital Rights Management* (DRM) lahir untuk mencegah terjadinya dampak buruk terhadap konten digital ini. Lebih jauh, DRM juga berperan untuk memberikan opsi untuk melakukan pengontrolan atas penggunaan *rights* dari sebuah konten digital. Banyak sekali teknik yang digunakan dalam implementasi DRM, dan salah satunya yang sangat penting adalah kriptografi. Berbagai macam teknik kriptografi telah diaplikasikan dalam DRM. Namun penggunaan kriptografi juga mempunyai beberapa celah dalam implementasinya. Kedudukan kriptografi sangat penting dalam DRM tetapi tidak cukup mengandalkan kriptografi saja untuk membangun sebuah sistem DRM yang ideal.

***Kata kunci**: makalah, kriptografi, tugas*

1. Pendahuluan

Perkembangan bisnis konten digital telah membawa peluang baru bagi kejahatan klasik di bidang teknologi informasi, yaitu pembajakan. Konten-konten yang seharusnya menjadi properti legal dari produsen dan secara legal dimiliki oleh orang yang telah membelinya, bisa dengan mudah disalahgunakan oleh pihak-pihak yang tidak bertanggungjawab. Konten digital seharusnya diproteksi tidak hanya ketika dikirimkan, tetapi juga ketika konten digital tersebut sampai kepada pemakainya[1)]. Misalnya, pihak yang telah membeli sebuah konten bisa saja mengirimkannya ke orang lain, atau membuat duplikatnya untuk nantinya dijual lagi. Oleh karena itu, dibutuhkan suatu mekanisme untuk mengatasi permasalahan pembajakan konten mobile ini. Dari sinilah *Digital Rights Management* lahir.

2. Definisi DRM

Digital Rights Management (DRM) dapat diartikan sebagai mekanisme proteksi konten digital secara persisten dan terintegrasi terkait dengan penyampaian dan penggunaan konten[1)]. Yang dimaksud dengan proteksi konten digital secara persisten adalah proteksi yang dilakukan terus menerus sepanjang konten digital tersebut ada. Sedangkan yang dimaksud dengan proteksi konten digital terintegrasi adalah mekanisme proteksi yang memenuhi spesifikasi yang

telah ditentukan sebelumnya dan mesti implementasikan oleh seluruh pihak terkait.

Dalam DRM, dikenal beberapa istilah umum sebagai berikut:

1. *DRM Content*
   Yang dimaksud dengan *DRM Content* adalah konten yang telah ditransformasikan menjadi sebuah konten digital sesuai dengan spesifikasi DRM yang digunakan.
2. *Rights*
   Right adalah hak penggunaan sebuah *DRM content*. *Rights* bisa membatasi penggunaan konten dalam beberapa aspek seperti rentang waktu penggunaan dan jumlah penggunaan. Instansiasi dari *rights* dinamakan *rights object.*
3. *DRM Agent*
   DRM Agent adalah perangkat (bisa berupa *hardware* atau *software*) yang digunakan untuk menggunakan *DRM content* beserta *rights* yang bersesuaian

Sebagai contoh, tinjau sebuah DRM XYZ. DRM XYZ akan digunakan untuk memproteksi konten digital, sebuah arsip musik digital. Untuk merealisasikannya, maka konten digital tersebut harus diubah ke bentuk *DRM content* sesuai spesifikasi DRM XYZ. Begitu juga perangkat *DRM Agent* yang akan digunakan untuk menggunakan konten tersebut, juga mesti memenuhi spesifikasi DRM XYZ. Inilah yang dimaksud dengan proteksi terintegrasi.

Saat ini telah banyak pihak yang mengeluarkan spesifikasi DRM, beberapa diantaranya adalah:

1. Microsoft DRM
   DRM yang menangani proteksi konten digital dengan format yang dikeluarkan Microsoft, seperti WMA (*Windows Media Audio*).
2. OMA-DRM
   OMA-DRM(*Open Mobile Alliance Digital Right Management)* merupakan DRM yang dikhususkan penggunaannya untuk memproteksi konten digital pada perangkat *mobile*
3. MediaSnap DRM
   MediaSnap DRM merupakan salah satu DRM yang memiliki tujuan untuk melindungi dokumen PDF (*portable document format*)
4. SecretSeal DRM
   DRM untuk memproteksi perangkat lunak dan arsip biner.

3. Tujuan DRM

Adapun beberapa tujuan umum dari DRM adalah sebagai berikut[1)]

3.1 Keamanan Pengiriman (Delivery Security) Konten Digital

Konten digital biasanya diterima oleh pihak yang telah membelinya melalui jalur yang tidak aman, seperti internet misalnya. Dalam internet, cukup besar kemungkinan data yang dikirimkan dipintas oleh pihak lain yang tidak mempunyai wewenang. Salah satu tujuan DRM adalah bagaimana konten digital yang dikirim bisa diterima hanya oleh orang yang berhak, dan dalam keadaan utuh sebagaimana kondisi pada saat awal pengiriman.

3.2 Pengontrolan Distribusi Konten Digital

Konten digital merupakan objek yang sangat mudah didistribusikan. Konten digital bisa dengan mudah disebarluaskan, misalnya, dengan meletakkannya pada suatu *server* yang terhubung ke internet, sehingga bisa diakses oleh orang di seluruh dunia. Atau contoh yang lebih sederhana, seseorang yang telah membeli konten digital secara resmi, kemudian bisa saja menjual kembali konten tersebut kepada

temannya dengan cara yang sangat mudah, yaitu dengan mengirimkannya saja.

3.3 Pengontrolan Penggunaan Konten Digital

Pengontrolan penggunaan konten digital kadang juga diperlukan dalam bisnis konten digital pada saat ini. Sebagai contoh, tinjau sebuah konten digital berupa musik digital. Pihak penjual musik digital tersebut ingin menjual musik tersebut dengan harga sesuai dengan lama penggunaan musik tersebut. Misalnya, sebuah musik digital bisa dijual untuk digunakan selama satu bulan, tiga bulan, atau untuk waktu yang tidak terbatas. Penggunaan *rights* pada DRM bisa mengakomodasi kebutuhan ini.

3.4 Pencegahan Penyalahgunaan Konten Digital

Penyalahgunaan konten digital (*digital content abuse*) merupakan salah satu masalah serius yang berkembang akhir-akhir ini. Beberapa contoh penyalahgunaan konten digital tersebut adalah:

- Perubahan isi sebagian konten digital
- Klaim ilegal kepemilikan konten digital
- Pengutipan/penyaduran sebagian atau seluruh isi konten digital secara ilegal

Permasalahan penyalahgunaan konten digital bisa dicegah dengan menggunakan teknik *digital signature* dan *digital watermarking*.

4. Aplikasi Kriptografi

4.1 Enkripsi

Enkripsi merupakan salah satu teknik yang paling banyak diterapkan dalam implementasi DRM. Cukup banyak variasi enkripsi yang digunakan dalam DRM untuk mewujudkan tujuan DRM yang telah dibahas diatas.

Contoh penggunaan enkripsi paling sederhana adalah untuk keamanan pengiriman konten digital. Sebelum dikirim, konten dienkripsi dengan sebuah kunci C_k yang diketahui baik oleh pengirim maupun penerima. Algoritma enkripsi yang digunakan adalah algoritma enkripsi simetri.

Algoritma enkripsi simetri tidak cukup jika kita ingin melakukan pengontrolan distribusi konten digital dengan DRM. Salah satu teknik yang bisa digunakan untuk mewujudkan itu adalah enkripsi kunci publik. Contoh implementasinya misalnya sebagai berikut.

1. Setiap *DRM Agent* mempunyai pasangan kunci publik-privat yang unik satu sama lainnya.
2. Seluruh kunci publik masing-masing *DRM Agent* tersebut diketahui oleh pihak pengiriman konten digital
3. *DRM Agent* hanya bisa menerima konten digital dari pengirim konten digital, tidak bisa dari *DRM Agent* lain
4. Ketika akan melakukan pengiriman konten, pengirim konten mengenkripsi konten terlebih dahulu dengan kunci publik *DRM Agent* yang dituju. *DRM Agent* kemudian melakukan dekripsi konten tersebut dengan kunci privat miliknya.

Untuk pengontrolan penggunaan konten digital, skema enkripsi juga bisa digunakan, seperti yang telah diimplementasikan pada metode *separate delivery* dalam OMA-DRM.

Dalam metode *separate delivery* OMA-DRM, terdapat dua objek terpisah yang diperlukan untuk menggunakan konten digital, yaitu *DRM content*, dan *right object*. *DRM content* adalah konten digital yang dienkripsi menggunakan algoritma AES dengan panjang kunci 128-bit. *Rights object*

adalah objek yang membatasi penggunaan *DRM content* (misalnya dalam waktu penggunaan, dan jumlah penggunaan). Selain itu, *rights object* juga memiliki kunci yang diperlukan untuk mengdekripsi *DRM content*. Dalam pengirimannya, *DRM content* bisa dikirimkan melalui jalur *unsecure* sedangkan *rights object* mesti dikirimkan melalui jalur yang *secure*.

Pengontrolan penggunaan konten digital bisa diwujudkan dengan menggunakan skema tersebut, karena sebuah *DRM content* bisa memiliki banyak *rights object*. Misalkan A dan B masing-masing telah memiliki *DRM content*. Baik A dan B memerlukan sebuah *rights object* karena mereka belum memiliki kunci dekripsi *DRM content*. Tetapi, A ingin menggunakan *DRM content* selama satu bulan saja, dan B ingin menggunakannya tanpa waktu penggunaaan. Untuk mewujudkan itu, pengirim konten bisa mengirimkan *rights object* yang berbeda untuk A maupun B.

4.2 Content Scrambling

Yang dimaksud dengan *content scrambling* adalah pengacauan isi konten digital dengan menggunakan sekumpulan besar pustaka algoritma enkripsi[4)]. Pemilihan algoritma enkripsi dilakukan sedemikian rupa sehingga untuk suatu waktu, hanya pengirim konten digital dan *DRM agent* yang mengetahuinya. *Content scrambling* lebih menekankan pada jumlah koleksi algoritma enkripsi yang semakin besar (kuantitas), ketimbang kekuatan masing-masing algoritma enkripsi (kualitas).

Content scrambling diterapkan pada MediaSnap DRM. Untuk memperkuat tingkat keamanan, selain melakukan enkripsi dengan algoritma AES, MediaSnap DRM juga menerapkan *content scrambling* sebelum konten dienkripsi. Tentu saja, setelah konten didekripsi, *content de-scrambling* juga harus dilakukan untuk mengembalikannya ke bentuk asalnya.

4.3 Digital Watermarking

Digital watermarking adalah teknik penyisipan sidik digital ke dalam sebuah konten digital, yang mana sidik digital tersebut berfungsi sebagai bukti kepemilikan (*copyright*). *Digital watermarking* diterapkan dalam beberapa DRM, seperti MediaSnap DRM dan Microsoft DRM. Dalam konteks DRM, *Digital watermarking* bertujuan untuk menjaga dan melacak terjadinya penyalahgunaan konten digital seperti adanya klaim kepemilikan konten yang tidak benar.

4. Analisis Aplikasi Kriptografi dalam DRM

Enkripsi tidak sepenuhnya bisa digunakan pada implementasi DRM. Enkripsi kunci publik misalnya, hanya cocok digunakan pada konten digital yang berukuran kecil, karena enkripsi kunci publik pada konten digital berukuran besar akan memakan *resource* yang sangat besar, yang mana tidak semua *DRM Agent* memiliki kapabilitas untuk itu.

Selain itu, enkripsi pada DRM yang algoritmanya dipublikasikan, sangat rentan untuk diserang. Beberapa DRM lama bahkan menggunakan algoritma yang sudah *obsolete*, yang pada masa sekarang dipecahkan dalam waktu yang relatif singkat. Beberapa DRM mengimplementasikan kombinasi enkripsi dengan *content scrambling* untuk tingkat keamanan konten digital yang lebih tinggi, seperti yang diimplementasikan MediaSnap DRM. secretSeal DRM mengambil pendekatan lain, yaitu dengan menerapkan

konsep *variable-length encrypted keys* dan *morphogenic algorithm*[2)]. Yang dimaksud dengan *variable-length encrypted keys* adalah panjang kunci enkripsi yang selalu berubah-rubah setiap kali enkripsi dilakukan. *Morphogenic algorithm* adalah algoritma enkripsi yang selalu berubah-berubah, dan implementasinya dalam *DRM Agent* tidak mudah untuk dipecahkan.

Bagaimana dengan pemakaian algoritma enkripsi yang tidak standar. Pemakaian algoritma yang tidak standar memiliki kelemahan dari sisi tingkat kepercayaan (*trustworthy)* dan efesiensi. Pihak yang terlibat dalam bisnis konten digital akan enggan menggunakan suatu DRM apabila DRM tersebut menggunakan algoritma enkripsi yang tidak standar.

DRM yang mengandalkan kriptografi dalam implementasinya sebaiknya juga membatasi masa berlaku spesifikasi DRM-nya. Dengan kata lain, spesifikasi implementasi kriptografi pada DRM sebaiknya diperbaharui dalam waktu berkala untuk menjamin tingkat keamanan konten digital. Hal ini dilakukan mengingat serangan terhadap sebuah enkripsi dari waktu ke waktu selalu berkembang.

Terakhir, pembatasan akses di sisi *hardware* dan *operating system DRM Agent* juga bisa membantu tingkat keamanan kriptografi pada DRM. Salah satu contohnya adalah pembatasan akses terhadap program enkripsi pada *DRM Agent* sehingga tidak ada pihak yang bisa melakukan *reengineering* untuk menemukan celah yang ada dalam implementasinya.

5. Kesimpulan.

Peranan kriptografi dalam DRM sangat penting, tetapi tidak cukup hanya mengandalkan teknik kriptografi yang sederhana saja untuk membangun sebuah DRM yang ideal. Beberapa teknik kriptografi bisa dikombinasikan untuk menghasilkan tingkat keamanan yang lebih tinggi. Selain itu, proteksi pada sisi *hardware* dan *operating system DRM Agent* juga dibutuhkan untuk mendukung aplikasi kriptografi dalam DRM.

[1] E. Fife Dr, *Digital Rights Management: Challenges and Issues in the Emerging Mobile, 2004*
[2] O. Pitkänen, *Toward a Digital Right Managements Framework, 2000.*
[3] secretSeal, *secretSeal Technologies Corporation press release,* 2000.
[4] M. Stamp, *Digital Rights Management : The Technology Behind The Hype*, San Jose State University, 2003.