PENERAPAN METODA FILE COMPRESSION PADA KRIPTOGRAFI KUNCI SIMETRI

Yuri Andri Gani – 13506118
Sekolah Teknik Elektro dan Informatika ITB, Bandung, 40132, email: if16118@students.if.itb.ac.id

Abstract *– Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Hal yang ditangani dalam kriptografi adalah kerahasiaan, integritas data, autentifikasi dan non-repudansi.*

Dalam manipulasi teknik manipulasi file, ada suatu algoritma yang dapat mengubah dan bahkan memperkecil ukuran data sekaligus mempertahankan integritas datanya, salah satunya adalah teknik pengompresan file. Dalam pengompresan file, bit-bit dari file dimanfaatkan sedemikian sehingga terpakai efektif dan efisien.

Pada makalah yang akan penulis buat nantinya, penulis akan mengusulkan suatu teknik kriptografi yang baru yang memanfaatkan teknik kompresi file, karena teknik kompresi dapat mempertahankan integritas data dan juga menghilangkan redundansi yang tidak perlu.

Masalah pada teknik penggunaan teknik kompresi pada kriptografi adalah, teknik kompresi harus membuat kunci sendiri (yang berbeda dari kunci yang di pakai user) untuk menjamin agar hasil kompresi dapat dibaca kembali. Oleh karena itu harus dipakai suatu cara agar kunci yang di gunakan pada kompresi file dapat disembunyikan dari pandagan orang ketiga.

Oleh karena itu pemulis mencoba untuk membuat suatu algoritma yang dapat menyembunyikan kunci kompresi dan juga menghancurkan keterhubungan statistik antar karakter pada file. Dengan mengawinkan kunci kompresi dan kunci kriptografi yang hasilnya dikawinkan lagi dengan pra-chiper textnya, sehingga tidak dapat ditebak hubungan antar karakter dan atau bit-nya.

1. PENDAHULUAN

Perkembangan teknologi informasi yang begitu pesat pada saat sekarang ini membuat setiap orang menjadi lebih banyak melakukan pengiriman data dan pesanmelalui media elektronik. Hal ini menyebabkan volume pertukaran data digital setiap hari mengalami penigkatan pesat. Data digital yang dipertukarkan disini sangat bervariasi dari mulai data yang tidak penting hingga data penting yang sifatnya sangat rahasia. Sering sekali pesan yang sifatnya rahasia tersebut dimanfaat oleh pihak lain yang tidak bertanggung jawab untuk kepentingannya sendiri.

Salah satu cara untuk mengatasi permasalahan diatas ialah dengan menggunakan kriptografi untuk melakukan enkripsi terhadap pesan yang dikirimkan. Sehingga hanya orang atau pihak yang berhak sajalah yang dapat mengetahui isi dari pesan tersebut.

Salah satu metoda yang sangat umum dipakai dalam kriptografi adalah metoda subtitusi yaitu dengan mengganti karakter, bit, atau kumpulan katakter atau bit dengan karakter atau bit lainnya. Metoda lainnya adalah transposisi dimana susunan karakter diubah-ubah sehingga tidak dimengerti lagi maknanya. Pada aplikasinya kedua metoda tersebut sering kali digunakan secara bersama-sama untuk menambah kerumitan kode.

Dalam kriptografi hal yang sangat penting dalam mejaga kerahasiaan pesan adalah kerahasian kunci, kerumitan kode, dan tidak adanya hubungan statistik pada *ciphertext*.
Jadi kriptorgafi yang baik adalah yang kuncinya tidak mudah ditebak, algoritmanya rumit, dan sangat sulit dicari kesamaanya dengan menggunakan *plaintext attact*.

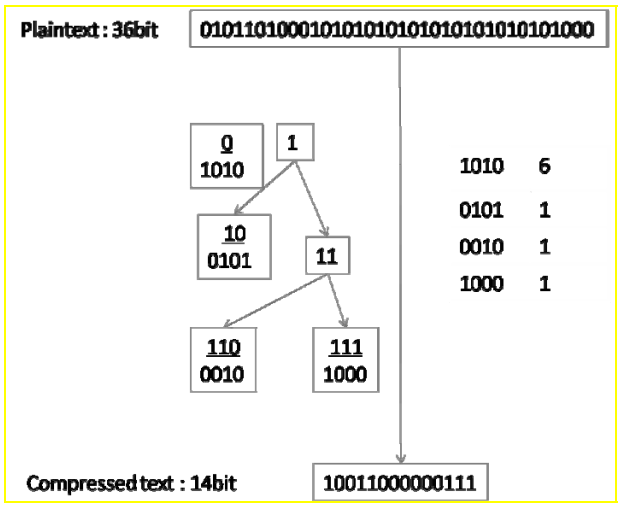
Dalam ilmu kriptografi banyak dikenal berbagai macam algoritma baik yang klasik maupun yang modern. Sering kali metoda dalam kriptografi ternyata hanya mengambil metoda-metoda lain yang bahkan kelihatannya tidak ada hubungan tujuan ataupun kemiripan algoritma. Karena itu kriptografi sering kali tidak hanya dianggap sebagai ilmu tetapi juga seni dalam menyembunyikan data.

Metoda lain yang dapat menyembunyikan pesan contohnya metoda kompresi. Dimana kumpulan bit disusun ulang sehingga ukurannya menjadi lebih kecil. Namun metoda kompresi bukanlah metoda yang baik karena mudah ditebak dengan memanfaatkan *plaintext* attack. Oleh karena itu harus di pasangkan dengan metoda lain yang dapat mencegah hal tersebut misalnya metoda *block cipher*.

2. KONSEP DASAR

2.1 Metoda kompresi

Metoda kompresi ialah segala macam cara yang digunakan untuk memperkecil ukuran file. Misalnya dengan mengganti string-string yang sering berulang dengan sring yang lebih kecil. Cara itulah yang akan penulis gunakan dalam makalah ini. Karena tujuan dari makalah ini adalah metoda kriptografi maka *ciphertext* yang dihasilkan tidak selalu lebih kecil dari *plaintext*-nya.
Proses kompresi dimulai dengan memecah *plaintext* menjadi blok-blok dengan ukuran beberapa bit. Blok-blok tersebut kemudian diurutkan berdasarkan frekuensi kemunculan. Yang paling sering muncul diletakkan pada urutan teratas. Kemudian didapat tabel frekuensi kemunculan tiap-tiap blok. Dari tabel tersebut kemudian buatkan bit-bit representasinya dengan pola blok yang paling sering muncul mendapat reprsentasi yang urutannya paling kecil dan seterusnya. Sehingga secara teori ukuran file akan berubah dan kemungkinan besar menjadi lebih kecil. Jika digunakan 1 blok = 8 bit maka ukuran bit-bit yang merepresentasikan tiap blok bervariasi dari 1 bit sampai maksimal 256 bit. Untuk lebih jelas lihat gambar 1.

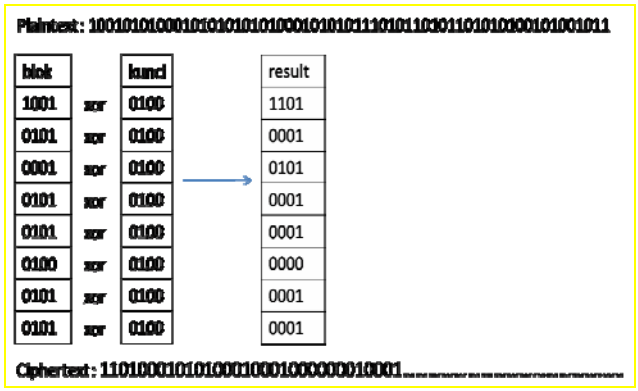


Gambar 1: teknik kompresi

Pada gambar 1 pengakhiran adalah bit 0. Pada aplikasinya tidak harus selalu seperti itu bisa sebaliknya atau pun campuran.

2.2 Metoda block *cipher*

Block *cipher* adalah teknik dimana plain text dipecah-pecah terlebih dahulu menjadi kumpulan blok-blok dan kemudian tiap-tiap bloknya dienkripsi secara terpisah. Enkripsi dilakukan terhadap blok bit *plaintext* menggunakan bit-bit kunci yang ukurannya sama dengan ukuran blok *plaintext*. Jadi, biasanya ukuran dari *cipher* text dan *plaintext* tidak jauh berbeda dan bahkan kemungkinan besar sama. Untuk menambah kerumitan biasanya dilakukan transposisi dan iterasi berkali-kali sehingga sangat sulit dicari hubungan statistiknya. Keamanan pada metoda block *cipher* sangat bergantung pada panjang kunci. Lihat gambar 2.



Gambar 2 : proses *cipher* blok sederhana

3. IMPLEMENTASI

Pada metoda *cipher* blok sederhana ukuran file tidak tidak tersembunyikan. Maka dari itu digunakanlah metoda kompresi yang dapat menyembunyikan ukuran file sekaligus menjadi penambah kerumitan algoritma.

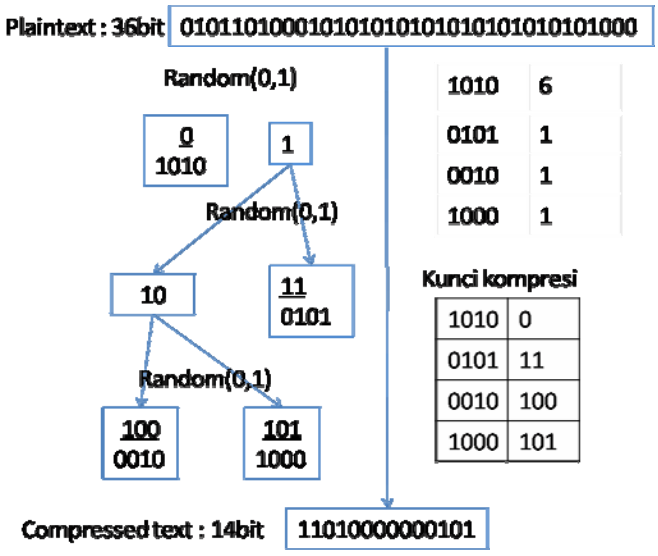
Cara penerapanya adalah tidak terbatas, tergantung selera dari *programmer* (pengembang). Berikutnya dalam makalah ini penulis akan menjelaskan salah satu cara penggunaannya secara sederhana.

Penerapan metoda kompresi dapat dilakukan dengan cara:

- Kompresi dilakukan pada masing masing blok sebelum/sesudah di xor dengan kunci
- Kompresi dilakukan pada *plaintext*/semi *plaintext* sebelum memulai enkripsi
- Kompresi dilakukan pada akhir enkripsi

Untuk makalah ini penulis akan menggunakan teknik kedua, yaitu dimulai dengan mengkompresi dan kemudian baru digunakan metoda *cipher* blok.

Ketika melakukan teknik kompresi kita akan menggunakan bit akhiran yang acak tidak seperti pada gambar 1. Pada gambar 1 akan sangat mudah menebak tiap-tiap blok kompresi. Sehingga dapat melemahkan kekuatan kriptografi. Cara yang akan dipakai adalah seperti pada gambar 3.

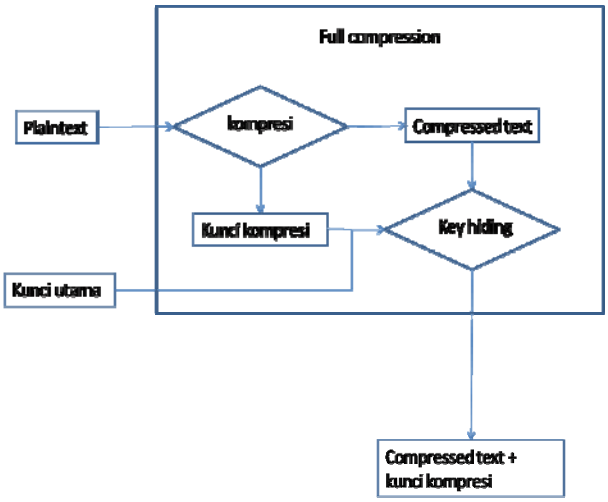


Gambar 3 : kompresi dengan bilangan akhir random

Penggunaan 4 bit dalam satu blok kompresi sangat menghawatirkan karena umum dipakai. Jadi sebaiknya tiap blok berukuran yang tidak sama dengan perpangkatan 2, agar hasil kompresi sangat acak.

Sebagaimana terlihat pada gambar 3, selain menghasilkan *compressed text* proses kompresi juga menghasilkan kunci kompresi. Tentu saja kunci ini rahasia, walaupun pada kenyataannya dengan mengetahui kunci ini masih sulit untuk mendekripsi *ciphertext* tanpa mengetahui kunci utamanya jika proses enkripsi dilakukan berulang sampai beberapa kali tentu saja penulis sangat menyarankan hal tersebut.

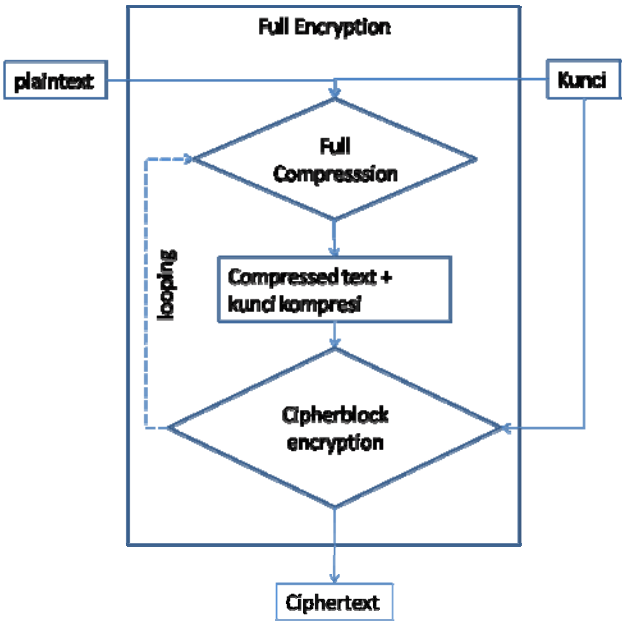
Untuk berjaga-jaga, kunci kompresi sebaiknya disembunyikan dalam hasil kompresi dengan format tertentu yang memanfaatkan kunci utama (misalnya panjang kunci, jumlah bit 0 atau satu dll). Bisa sekaligus bisa juga dipecah-pecah menjadi beberapa bagian.



Gambar 4 : kompresi dengan menyembunyikan kunci kompresi

Setelah proses kompresi selesai baru kemudian dilanjutkan dengan enkripsi *cipher* blok dengan cara yang sesuai dengan keinginan pengembang. Penulis tidak akan membatasi apa yang bisa pengembang lakukan pada enkripsi *cipher* blok.

Jika pengembang menerapkan looping dalam enkripsinya maka sebaiknya proses kompresi diikutkan dalam looping tersebut. Sehingga ukuran file semakin kecil dan semakin sulit untuk diserang.



Gambar 5 : Full Encription sederhana dengan looping

4. ANALISIS KELEBIHAN DAN KEKURANGAN METODA

Seperti halnya kriptografi *cipher* blok lainnya, kekuatan kriptografi sangat bergantung pada kerahasiaan kunci dan panjang kunci. Namun penambahan teknik kompresi ini bukanlah percuma. Pada umumnya pada kriptografi *cipher* blok ukuran *ciphertext* dan *plaintext* sama. Dengan menambahkan teknik compresi maka ukuran *ciphertext* diharapkan akan sangat berkurang. Selain itu kerumitan algoritma yang menjadi salah satu faktor dalam mengukur kekuatan kriptografi akan bertambah. Jadi tentu saja penggunaan teknik kompresi akan menambah kekuatan kriptografi.

Kekurangan dengan penambahan teknik ini adalah waktu komputasi yang tentu saja akan bertambah dan juga memori yang digunakan akan meningkat tajam, berbanding lurus dengan variasi blok-blok kompresi.

Serangan pada metoda ini kurang lebih sama dengan serangan yang biasa digunakan pada metoda *cipher* blok lainnya yaitu *exhaustive search.* Selain cara tersebut penulis tidak bisa membayangkannya. Karena kemiripan statistik sama sekali tidak ada. Penyerangn dengan *plaintext attack* sama sekali tidak berguna karena dengan *plaintext* yang sedikit berbeda saja hasilnya akan berbeda jauh.

5. KESIMPULAN

Pada dasarnya full compression pada gambar 4, sudah merupakan teknik enkripsi tersendiri. Jadi tanpa enkripsi *cipher* blok pun sudah dapat menyembunyikan pesan. Namun karena kekuatanya apabila berdiri sendiri belum dapat diukur maka sebaiknya tetap digandengkan dengan teknik enkripsi lain (tidak harus *blockcipher*)

Makalah ini penulis biarkan tanpa implementasi dalam program yang utuh karena penulis ingin agar metoda ini dikerjakan dalam berbagai macam cara sesuai kreativitas pengembang.

Makalah yang penulis paparkan tidaklah sempurna sehingga diperlukan adanya perbaikan dan improfisasi dari pembaca. Makalah ini tidak ditujukan untuk menjadi panduan lengkap,

melainkan hanya sebagai penambah wawasan dan diharapkan agar dapat member ide untuk pengembangan yang lebih baik.

DAFTAR PUSTAKA

1. Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2006