

ENKRIPSI DATA
Harindra Wisnu Pradhana (L2F004481)
Teknik Elektro Universitas Diponegoro

Abstrak

Akhir-akhir ini sistem informasi semakin berkembang. Sebagai indikator dapat dilihat kemajuan teknologi dalam pengiriman data yang semakin lama semakin berkembang seiring dengan kebutuhan manusia akan komunikasi data. Suatu data dapat ditransmisikan dengan berbagai cara baik melalui sinyal di udara, maupun dengan saluran kabel. Penggunaan media transmisi ini memungkinkan orang-orang yang tidak bertanggung jawab membaca isi data tersebut, oleh karena itu diperlukan adanya enkripsi data untuk mengamankan data yang ditransmisikan.

I. PENDAHULUAN

Sistem pengiriman data belakangan ini menunjukkan perkembangan yang begitu pesat. Hal ini ditunjukkan dengan semakin berkembangnya teknologi informasi baik metode pengirimannya, maupun besarnya data yang dikirimkan.

Pada umumnya data dapat dipisahkan menjadi dua yaitu data analog dan data digital. Sebelum teknologi digital diciptakan, hanya ada data berupa analog yang pada umumnya berupa suara. Pada saat itu data ditransmisikan dengan saluran telepon maupun dimodulasikan pada gelombang untuk dipancarkan sebagai sinyal-sinyal radio.

Selain data analog, data digital juga dipancarkan dengan media yang sama, hanya saja masih berupa kode-kode morse. Kode-kode ini merepresentasikan huruf-huruf yang dikirimkan secara beruntun sehingga membentuk kata-kata dan kalimat yang akan ditransmisikan. Pengiriman dilakukan secara beruntun karena keterbatasan bidang transmisi.

Dengan perkembangan jaman, kode morse dirasa kurang memadai karena semakin berkembangnya data yang dikirim. Ada kalanya dokumen-dokumen yang perlu dikirim memuat karakter-karakter yang tidak terdapat pada *alphabet*. Maka diciptakanlah standar penulisan karakter secara digital yang disebut ASCII yang merupakan kependekan dari American Standard Code for Information Interchange yaitu standar kode digital sepanjang satu byte yang mencakup abjad baik huruf kecil maupun

kapital, angka nol sampai sembilan, dan karakter-karakter standar lain yang diwakili dengan tujuh dari delapan bit yang ada. Namun seiring perkembangan teknologi, bit kedelapan digunakan untuk menambahkan 128 karakter dan simbol-simbol baru pada extended ASCII yang telah diimplementasikan pada komputer-komputer x-86.

Perkembangan jaman yang semakin pesat menjadikan kebutuhan akan transmisi data yang semakin besar pula. Keterbatasan bidang transmisi membuat manusia melakukan penggandaan kanal. Ada dua cara penggandaan kanal, yaitu dengan memodulasikan pada sinyal dengan frekuensi yang berbeda sehingga dapat dikirim pada saluran yang sama yang disebut frequency division multiplexing dan dengan memotong-motong data untuk dikirimkan secara bergantian yang disebut time division multiplexing. Data analog yang cenderung berurutan relatif sulit dipotong-potong untuk dikirim bergantian, sedangkan data digital memungkinkan dilakukan penggandaan kanal dengan kedua cara diatas. Selain itu, data digital jauh lebih mudah untuk diolah, dan disimpan. Hal ini membuat banyak data analog dikonversi menjadi data digital baik untuk disimpan maupun ditransmisikan. Hal ini menghasilkan berbagai format data analog yang disimpan dalam bentuk digital misalnya jpg, bmp, dan gif untuk gambar, wav, mp3, dan pcm untuk suara serta mpg, avi, dan mov untuk video.

Hal ini memungkinkan data semakin fleksibel untuk disimpan, diolah, dan ditransmisikan baik dengan memodulusinya pada sinyal-sinyal radio, maupun dengan protokol-protokol jaringan yang ada.

II. KONSEP ENKRIPSI DATA

Perkembangan transmisi data selain menimbulkan masalah pada bidang transmisi, juga memunculkan keragu-raguan akan keamanan jalur transmisi. Masalah lebar bidang yang sedikit teratasi dengan penggandaan kanal dan perkembangan peralatan transmisi membuat manusia menengok ke arah keamanan data yang dikirimkan.

Dengan berkembangnya teknologi informasi, data dapat ditransmisikan dengan cara yang begitu beragam, dan diterima dengan cara yang beragam pula. Jalur transmisi yang cukup panjang memungkinkan orang lain menguping saluran transmisi ini dan dimungkinkan untuk mengetahui data yang sedang dikirim. Untuk data informasi biasa pengirim maupun penerima mungkin tidak akan keberatan bila isi data diketahui oleh orang lain. Namun seiring perkembangan jaman, diperlukan pula pengiriman untuk data-data yang vital yang memerlukan kerahasiaan. Data tersebut dapat berupa dokumen-dokumen perusahaan, catatan-catatan hingga password atau nomor kombinasi. Bila hal ini diketahui orang yang tidak bertanggung jawab, dimungkinkan terjadi penyalahgunaan data tersebut yang mengakibatkan kerugian baik di pihak pengirim data maupun penerima data.

Faktor keamanan ini membuat manusia tak hanya memikirkan bagaimana data dimampatkan sehingga pengiriman informasi menjadi efektif, melainkan juga bagaimana data diolah sehingga data yang ditransmisikan berisi informasi yang hanya dapat diketahui oleh penerima yang seharusnya. Sehingga terciptalah pengolahan data dengan kunci tertentu yang disebut enkripsi data. Sedangkan data yang telah diolah ini disebut data terenkripsi.

Pada dasarnya proses enkripsi data adalah proses mengubah bentuk data dengan

kata kunci tertentu tanpa menghilangkan informasi yang ada pada data tersebut. Proses enkripsi ini dilakukan dengan metode-metode tertentu.

Pada jaman dahulu, enkripsi data telah digunakan oleh Julius Caesar dalam menyampaikan pesan rahasia pada pasukan-pasukan. Konsepnya adalah mengganti huruf pada alfabet dengan huruf yang lain secara berurutan dengan kunci tertentu. Misalnya dengan kunci "4" maka urutan alfabet akan bergeser empat langkah kedepan yaitu ABCDEFGHIJKLMNOPQRSTUVWXYZ akan terenkripsi menjadi EFGHIJKLMNOPQRSTUVWXYZABCD. Konsep ini begitu sederhana, sehingga kata "RAHASIA" dienkripsi menjadi "VELEWME" untuk mengetahui data sebenarnya cukup dengan membalik proses ini dengan kata kunci yang sama atau mundur empat abjad.

Enkripsi ini menghasilkan data terenkripsi dengan panjang tepat sama dengan data aslinya, dan hanya menggunakan suatu angka sebagai kunci yang hanya memiliki 26 variasi sesuai dengan panjang alfabet. Meskipun sangat berguna bagi Caesar, enkripsi ini begitu mudah dipecahkan terutama dengan komputasi modern yang begitu cepat. 26 kemungkinan ini dapat dicari dalam waktu singkat, dan data asli dapat didapat dalam waktu yang sama.

III. PERKEMBANGAN ENKRIPSI DATA

Enkripsi data semakin berkembang seiring dengan perkembangan waktu. Karakteristik algoritma enkripsinya pun bervariasi tergantung jenis data dan kebutuhan tingkat keamanan data.

3.1 Enkripsi password

Password merupakan kata kunci untuk mengakses sesuatu. Akhir-akhir ini password telah menjadi hal yang umum di kalangan masyarakat. Password biasanya berupa satu kata berisi kombinasi huruf, angka maupun keduanya dengan panjang tertentu. Karena kedudukannya sebagai pembatas akses, keamanan password mutlak

diperlukan untuk menghindari akses bebas akibat terbongkarnya password. Karena perlunya tingkat keamanan yang tinggi, password yang telah terenkripsi sering memiliki ukuran yang beberapa kali lebih besar dari panjang password sebenarnya, dan menggunakan algoritma enkripsi yang sangat rumit. Dua contoh enkripsi password yang populer adalah dengan algoritma DES dan MD5.

DES merupakan singkatan dari Data Encryption Standard. DES dikembangkan oleh pemerintah AS bekerjasama dengan IBM dan umumnya diimplementasikan untuk enkripsi password pada sistem operasi berbasis Unix.

Algoritma ini menggunakan dua input yaitu password yang akan dienkripsi dan kata kunci tambahan yang disebut *salt*. Salt dapat berupa karakter huruf maupun angka. Disini tujuh bit awal dari setiap karakter password diolah dengan algoritma tertentu dan menghasilkan 56bit kata kunci. Kata kunci inilah yang akan digunakan untuk mengenkripsi salt dan hasilnya berupa 13 karakter password terenkripsi dengan dua karakter pertama adalah salt. Disini keamanan cukup terjamin mengingat bukan password yang dienkripsi dengan salt, melainkan sebaliknya, salt dienkripsi dengan password. Sehingga secara teori proses dekripsi tidak mungkin dilakukan atau sering disebut enkripsi searah. Proses verifikasi password dilakukan dengan cara melakukan enkripsi yang sama pada password yang diinputkan pengguna, dan membandingkan hasilnya dengan data password terenkripsi yang telah tersimpan sebelumnya.

Namun karena DES merupakan hasil pengembangan pemerintah AS, penggunaan enkripsi DES tidak dibenarkan di luar wilayah AS. Lalu dikembangkanlah Algoritma enkripsi MD5 yang merupakan versi perbaikan dari DES. MD5 memiliki kelebihan yaitu pada panjangnya password yang tidak terbatas, dan tidak digunakannya salt. Hasil keluaran dari algoritma MD5 ini berupa serentetan karakter yang jauh lebih panjang daripada hasil keluaran DES. Namun karena tidak digunakannya salt,

meski peluangnya sangat kecil dimungkinkan muncul password terenkripsi yang sama meski password sebenarnya berbeda. Namun hingga kini belum ada keluhan tentang hal ini, dan enkripsi MD5 juga merupakan enkripsi searah yang secara teori tidak mungkin di lakukan dekripsi.

3.2 Enkripsi data

Berbeda dengan enkripsi password, enkripsi data yang akan ditransmisikan harus bisa di dekripsi atau dikembalikan ke bentuk asal karena harus diketahui pihak penerima. Untuk memungkinkan proses dekripsi diperlukan algoritma yang memiliki algoritma pembalikannya.

Enkripsi data yang cukup terkenal adalah PGP yang merupakan kependekan dari Pretty Good Privacy. PGP adalah produk dari Network Associates Inc yang telah dipasarkan di berbagai penjuru dunia dalam bentuk program enkripsi yang mampu mengenkripsi maupun mendekripsi data.

PGP menggabungkan teknik enkripsi konvensional dengan kriptografi umum, yaitu proses kriptografi yang kata kunci untuk mengenkripsinya diketahui umum, namun tidak semuanya mampu mendekripsinya. Pertama-tama dokumen yang akan dienkripsi dimampatkan dengan algoritma tertentu untuk menghemat waktu dan jalur transmisi, serta media penyimpanan. Dan yang tak kalah penting, proses pemampatan data akan memperkuat enkripsi.

Setelah data termampatkan, PGP akan membuat kata kunci secara acak yang berbeda setiap saat yang disebut *session key*. Kata kunci ini seketika akan digunakan untuk mengenkripsi data, lalu kata kunci itu sendiri akan dienkripsi dengan kunci umum atau *public key* yang diketahui pengirim maupun penerima. Sehingga terdapat dua data pertama data yang terenkripsi oleh *session key* dan kedua *session key* yang terenkripsi oleh *public key*. Kedua data inilah yang akan ditransmisikan pada penerima.

Sedangkan proses dekripsi merupakan kebalikannya. Data kedua didekripsi dengan *public key* sehingga didapatkan *session key*

lalu session key inilah yang digunakan untuk mendekripsi data pertama sehingga data sebenarnya dapat diketahui. Dengan demikian proses enkripsi ini disebut proses enkripsi dua arah.

IV. PENUTUP

Proses enkripsi data dapat dibedakan menjadi dua, proses enkripsi searah dan dua arah. Proses enkripsi searah digunakan untuk mengenkripsi data yang relatif pendek namun memerlukan tingkat keamanan yang sangat tinggi dan tidak untuk dibaca kembali data sebenarnya. Enkripsi ini digunakan untuk mengamankan password yang harus dihafal oleh pengguna untuk proses verifikasi. Proses verifikasi dilakukan dengan membandingkan password yang telah terenkripsi pada memori dan yang diinputkan pengguna. Dengan demikian tidak diperlukan proses dekripsi untuk menampilkan data sebenarnya. Contoh implementasiannya adalah password pada sistem operasi dengan *multiuser*. Sedangkan pada enkripsi dua arah dimungkinkan proses dekripsi untuk menampilkan data sebenarnya. Enkripsi ini diimplementasikan pada transmisi data yang memerlukan pengamanan data. Proses dekripsi diperlukan karena data harus dapat dibaca oleh penerima. Contoh implementasinya

adalah sistem pengamanan pada pengiriman data melalui internet.

Daftar Pustaka

1. McClure, Stuart et al, *Hacking Exposed: Network Security Secret And Solutions*, McGraw-Hill Companies, 2001
2. Zimmermann, Phil, *An Introduction to Cryptography*, Network Associates, Inc, 1998



HARINDRA WISNU P (L2F004481).

Dilahirkan di Blora 19 tahun yang lalu. Menempuh pendidikan dari sekolah dasar sampai sekolah menengah pertama di Blora dan melanjutkan sekolah menengah atas di Semarang. Dari tahun 2004 sampai saat ini sedang menyelesaikan studi Strata-1 di Jurusan Teknik Elektro Fakultas Teknik Universitas Diponegoro Semarang, konsentrasi Informatika dan Komputer.

Semarang, 28 September 2006