Perbandingan Algoritma Cipher Aliran dan Cipher Blok dalam Enkripsi Dokumen

Amalia Rahmah [1)]
1) Jurusan Teknik Informatika ITB, Bandung, email: if14064@students.if.itb.ac.id

Abstract – *Makalah ini membahas mengenai hasil perbandingan algoritma cipher aliran dan cipher blok berdasarkan kategori tertentu dan perbandingan kedua algoritma tersebut dalam enkripsi beberapa jenis dokumen. Pada hasil perbandingan ini akan diperlihatkan kelebihan dan kekurangan masing-masing algoritma apabila digunakan untuk mengenkripsi suatu jenis dokumen tertentu.*

Kata Kunci*: cipher aliran, cipher blok, kunci, enkripsi*

1. PENDAHULUAN

Cipher aliran dan cipher blok adalah dua kategori cipher yang biasa digunakan untuk kriptografi klasik[7]. Cipher aliran dan cipher blok merupakan jenis algoritma sandi yang menggunakan kunci simetris dimana kunci yang digunakan untuk enkripsi dan dekripsi dokumen sama dan kunci dirahasiakan.

Cipher aliran adalah algoritma enkripsi yang mengenkripsi data sebagai aliran karakter-karakter atau bit-bit.[2] Cipher aliran menggunakan dua data aliran data yaitu aliran data masukan dan aliran data kunci semu. Aliran data kunci semu dibangkitkan menggunakan fungsi *pseudo random sequence generator* dimana *masukannya* adalah kunci induk enkripsi.

Enkripsi pada cipher aliran dilakukan dengan mengkombinasikan satu bit aliran data masukan dan satu bit aliran data kunci menggunakan fungsi sederhana tertentu, misal XOR. Proses ini berulang untuk setiap bit aliran data. Keamanan enkripsi lebih diusahakan melalui membuat aliran kunci yang sulit ditebak daripada membuat algoritma fungsi yang kompleks. Dekripsi bekerja sebaliknya yaitu dengan mengambil satu bit dari aliran data hasil enkripsi dana satu bit dari data kunci untuk mengembalikan bit aliran data masukan.Ini bekerja karena aliran kunci yang dibangkitkan selalu sama untuk setiap kunci enkripsi dan fungsi enkripsi memiliki operasi *reverse* sendiri yang sederhana.

Contoh algoritma cipher aliran meliputi cipher aliran sinkron dan cipher aliran asinkron. Pada cipher aliran sinkron, kunci dibangkitkan pada waktu yang berbeda selama proses enkirpsi. Contoh algoritma cipher aliran sinkron meliputi aliran DES dalam mode OFB. Salah satunya adalah RC4. Cipher aliran asinkron membangkitkan aliran kunci sebagai fungsi dari kunci dan sekumpulan bit cipherteks sebelumnya. Contoh algoritma cipher aliran asinkron adalah aliran DES dalam mode CFB. Salah satunya adalah R5 yang biasa digunakan untuk enkripsi komunikasi via GSM. Contoh lain algoritma enkripsi cipher aliran adalah one-time-pad.

Cipher blok adalah algoritma enkripsi dimana data yang dienkripsi dibagi-bagi menjadi blok-blok berukuran sama (biasanya 64 bit), dan setiap blok dienkripsi masing-masing [1]. Algoritma enkripsi ini memerlukan penambahan beberapa bit pada teks masukan dengan tujuan agar ukuran blok terakhir sesuai dengan ukuran blok lainnya. Algoritma dekripsi akan menghapus bit-bit tambahan tersebut sebelum mengembalikan teks hasil enkripsi (cipherteks) menjadi teks masukan semula (plainteks).

Operasi pada cipher blok adalah dengan mengambil sebuah blok dari plainteks dan sebuah blok dari kunci untuk menghasilkan cipherteks. Hal ini dapat dianalogikan menggunakan tabel yang berisi semua kemungkinan blok plainteks sebagai baris tabel dan semua kemungkinan blok kunci sebagai kolom tabel. Tabel ini mendefinisikan fungsi untuk enkripsi. Kemudian ada tabel lain yang mendefinisikan fungsi untuk dekripsi. Apabila ada blok plainteks M dan blok kunci K, kemudian fungsi enkripsi menghasilkan blok cipherteks O. Apabila melihat baris O dan kolom K dari tabel fungsi dekripsi, maka nilai yang diperoleh adalah M.

Contoh algoritma cipher blok adalah DES (ukuran blok 64 bit), AES (ukuran blok 128 bit), RSA (ukuran blok bervariasi), dan Diffie-Hellman (ukuran blok bervariasi)

3. HASIL DAN PEMBAHASAN

3.1 Perbandingan berdasarkan Kategori

Hasil perbandingan berdasarkan kategori, dijabarkan di bawah ini sebagai berikut:

a. Ukuran cipherteks

Hasi enkripsi pada cipher aliran berukuran sama dengan plainteks. Sedangkan pada cipher blok, penambahan bit (*pad*) pada cipher blok pada akhirnya akan menambah ukuran *file* hasil enkripsi sebesar 1 sampai ukuran blok - 1.

b. Kerahasiaan

Cipher blok menawarkan penjaminan kerahasiaan yang lebih daripada cipher aliran karena operasi yang dilakukan dikenakan pada blok data dan bukan bit per bit data. Cipher aliran lebih mudah dimanipulasi dan tidak ada *error propagation*.

c. Kecepatan

Cipher aliran cenderung lebih cepat daripada cipher blok dan ini dapat terjadi karena cipher aliran dijalankan pada *bit level* dan kompleksitasnya lebih rendah.

d. Kompleksitas

Cipher blok cenderung lebih kompleks apabila dilihat dari sisi penggunaan *hardware* dan cipher aliran lebih kompleks apabila dilihat dari sisi *software* karena mereka diaplikasikan pada *bit level*.

e. *Error Propagation* / perambatan kesalahan

Error propagation adalah hal yang dapat menimbulkan *error* baru akibat adanya *error* yang lainnya. Pada cipher aliran, tidak ada *error propagation* karena ekripsi dikenakan pada setiap bit secara terpisah dan tidak ada umpan balik. Pada cipher blok, bisa saja terjadi *error propagation* yang menghasilkan efek berbeda pada cipherteks atau plainteks tergantung mode enkripsi yang digunakan (*cipher block chaining* dan *cipher feedback*).

f. Panjang kunci

Panjang kunci pada cipher aliran adalah sama dengan panjang plainteks. Panjang kunci pada cipher blok adalah tidak harus sama dengan ukuran blok (pada DES sama dengan 64 bit).

g. Biaya operasi (*overhead*)

Biaya operasi untuk stream cipher lebih besar daripada cipher blok dan membutuhkan dinkronisasi parameter antara pengirim dan penerima.

h. Ketahanan terhadap Serangan

Cipher aliran rentan terhadap terjadinya kerusakan karena pengubahan terhadap teks dibatasi. Pengubahan satu bit pada teks hasil enkripsi tidak akan memberikan efek pada bit-bit lainnya. Berbeda dengan cipher blok, pengubahan satu bit pada blok hasil enkripsi berakibat pada keseluruhan bit dalam blok tersebut. Sehingga adanya pengubahan pada cipher blok lebih mudah diidentifikasikan.

Ada pula beberapa metode serangan yang dilakukan pada cipher aliran apabila menggunakan aliran kunci yang sama untuk banyak *file*. Hal ini diakibatkan karena kunci enkripsi hanya bisa membangkitkan kombinasi aliran kunci yang terbatas. Sehingga enkripsi yang lebih aman memerlukan kunci enkripsi dengan jumlah bit yang lebih banyak.

Kelemahan cipher blok adalah bahwa apabila menggunakan blok kunci yang tetap dan ada sebagian blok dari plainteks berulang, maka blok plainteks yang berulang dan hasil enkripsinya akan berulang dan terlihat korepondensinya. Hal ini akan memudahkan kriptanalis memecahkan cipherteks berdasarkan pola perulangan tersebut.

3.2 Enkripsi pada Dokumen

Berikut ini akan dijelaskan algoritma apa yang cocok untuk diterapkan pada enkripsi dokumen-dokumen di bawah ini:

a. Dokumen berukuran kecil

Seperti yang telah dijelaskan pada sub-bab sebelumnya, bahwa pada cipher blok, ada penambahan bit-bit pada blok terakhir agar ukurannya sesuai. Sehingga dokumen berukuran kecil tidak efektif jika dienkripsi menggunakan algoritma cipher blok.

b. Dokumen dengan ukuran yang tidak diketahui

Ada aplikasi tertentu dimana enkripsi dilakukan pada plainteks yang tidak diketahui ukuran pastinya, misal: koneksi aman tanpa kabel (*wireless*). Apabila menggunakan cipher blok untuk aplikasi jenis ini, perancang program harus memilih antara efisiensi transmisi atau kompleksitas implementasi karena cipher blok tidak dapat langsung beroperasi pada blok berukuran lebih pendek daripada ukuran blok yang seharusnya. Sehingga untuk enkripsi dokumen jenis ini, cipher aliran lebih cocok untuk digunakan.

c. Kriptografi militer

Manfaat cipher aliran pada kriptografi militer adalah dimana cipher aliran dapat dibangkitkan dari aplikasi terpisah dengan tujuan untuk keamanan dan menjadi masukan untuk device lain, seperti radio set, yang akan menjalankan operasi XOR sebagai bagian dari fungsi.

d. Video

Karakteristik dokumen video adalah berkukuran besar dan dijalankan pada aplikasi *real time*. Untuk itu lebih baik digunakan algoritma cipher aliran untuk enkripsi *file* tersebut. Namun karena ukuran file yang besar, maka algoritma yang digunakan adalah kombinasi beberapa algoritma cipher aliran.

e. *Internet Telephony* pada jaringan yang homogen

Apabila jaringan lingkungan implementasinya adalah homogen, memiih algoritma cipher lebih mudah untuk memilih algoritma enkripsi. Jelas

bahwa cipher aliran memiliki peformansi yang lebih baik daripada cipher blok dalam enkripsi paket yang melewati jaringan apabila terjadinya *loss* dapat diabaikan, namun *corrupt* tidak dapat ditoleransi.

Sebaliknya, cipher blok memiliki performansi lebih baik daripada cipher aliran dalam enkripsi paket yang melewati jaringan apabila terjadinya *corruption* dapat diabaikan, namun terjadinya *loss* tidak dapat ditoleransi.

Sekarang ini, banyak aplikasi paket teleponi dengan jaminan keamanan menggunakan agoritma enkripsi cipher blok.

f. VoIP

Voice over Internet Protocol (VoIP) adalah metode untuk mengambil sinyal suara analog, seperti pada saat mendengarkan pembicaraan melalui telepon, dan mengubahnya menjadi data digital yang bisa ditransmisi melalui internet[11]. VoIP yang diibahas disini adalah yang dijalankan pada jaringan internet heterogen.

Karakteristik VoIP adalah sebagai berikut:

1. Aplikasi *real time*
2. *Scalable* dalam menangani jumlah panggilan yang banyak(*large call volume*)
3. *Merupakan* teknologi paket, menyerupai paket data seperti didalam LAN dan WAN.
4. Memiliki *traffic priorization* yang akan menjamin bahwa *voice packet* dapat dengan cepat diproses didalam jaringan
5. Lebih toleransi terhadap terjadinya kehilangan (*loss*) daripada kerusakan (*corruption*)

Apabila terjadi kehilangan, maka yang hilang hanyalah berupa paket. Penerima akan

Karakteristik enkripsi voip yang diperlukan

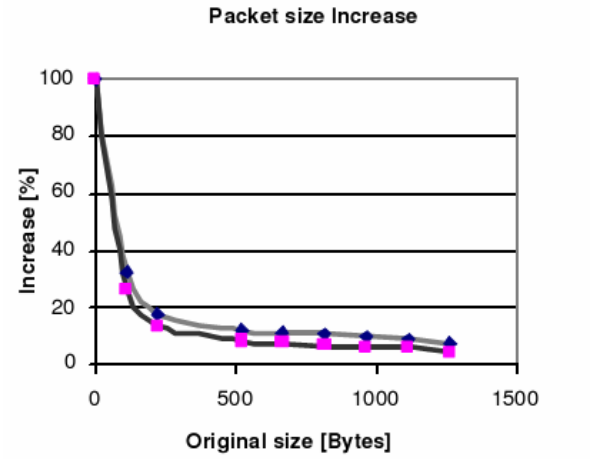
1. Ada jaminan keamanan
2. Algoritma yang kemungkinan menyebabkan terjadinya *corruption* kecil.
3. Dapat diimplementasikan pada aplikasi *real time*

Cipher blok melipatgandakan bit *error*. Adanya satu bit salah pada cipherteks yang diterima oleh dekriptor akan meghasilkan banyak bit *error* pada plainteks hasil keluaran dekriptor. Untuk VoIP, lebih baik meggunakan cipher blok selama layanan VoIP menjamin adanya *maintain framing* pada paket suara.

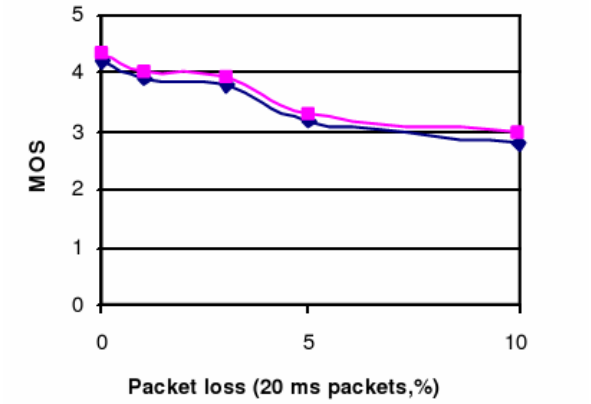
Cipher aliran tidak merambatkan terjadinya kesalahan, namun merambatkan kesalahan sinkronisasi akibat adanya penyisipan atau penghapusan bit.

Apabila dilihat dari sudut pandang suara yang diterima dan karakteristik utama VoIP yaitu aplikasi *real-time*, maka lebih baik jika menggunakan algoritma enkripsi cipher aliran dibandingkan dngan cipher blok dengan prekondisi **sebelum terjadi** paket hilang.

Adanya sinkronisasi cipher aliran pada setiap paket, tanpa tambahan biaya operasi akibat adanya tambahan vektor inisialisasi pada *header* paket atau tanpa perawatan pada setiap statu pada data hasil enkripsi terakhir.



Gambar di atas merupakan grafik penambahan ukuran paket pada cipher blok dan cipher aliran



Gambar di atas merupakan grafik efek paket *loss* terhadap kualitas keberterimaan suara.

4. KESIMPULAN

a. Enkripsi dokumen berukuran kecil atau dokumen dengan ukuran yang tidak diketahui lebih efektif menggunakan cipher aliran
b. Algoritma yang cocok untuk digunakan untuk aplikasi *real time* adalah cipher aliran.
c. Pemilihan algoritma untuk enkripsi paket yang dikirimkan melalui internet dapat dilakukan dengan melihat apakah lingkungan implementasi aplikasi lebih toleran terhadap terjadinya

kehilangan (*loss*) atau terjadinya kerusakan (*corrupt*) pada paket.

d. Penggunaan algoritma cipher aliran untuk aplikasi real time yang menggunakan pengiriman paket via jaringan lebih baik selama tidak terjadi paket hilang (*loss).*

DAFTAR REFERENSI

[1] survey.netcraft.com/surveys/analysis/https/2005/ Jun/glossary

[2] www.nemesys.com/Content/Core/Glossary.php

[3] www.ecrypt.eu.org/stvl/sasc/slides25.pdf

[4]www.ftsm.ukm.my/jitm/abstracts/vol1_abstract7.pdf

[5] lever.cs.ucla.edu/kfe/research/AMSW01.pdf [6] http://rvl4.ecn.purdue.edu/~kak/courses-i-teach/compsec/NewLectures/Lecture3.pdf

[7] http://www.tech-faq.com/block-stream-cipher.shtml

[8] http://blogs.msdn.com/drnick/

[9] www.cert.or.id/~budi/courses/security/2006-2007/Report-Sujono.doc

[10] http://bletchleypark.net/cryptology/Symmetric_Stream_Ciphers.html

[11] http://communication.howstuffworks.com/ip-telephony.htm