ANALISIS PENYIMPANAN FILE ONLINE DENGAN ENKRIPSI MENGGUNAKAN ALGORITMA AES (ADVANCED ENCRYPTION STANDARD) RIJNDAEL

Bagus Budiharto Pratama, Raden[1], Endro Ariyanto [2], Andrian Rakhmatsyah[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

---

Abstrak

Layanan internet menjadi salah satu cara untuk mendapatkan berbagai macam informasi karena memudahkan pengguna untuk melakukan berbagai kegiatan. Fasilitas penyimpanan file secara online pada internet mempermudah proses pengaksesan data. File yang disimpan secara online tidak sepenuhnya aman, seharusnya keamanan penyimpanan mutlak diperlukan.

Salah satu algoritma kriptografi cipher blok adalah algoritma Rijndael. Rijndael merupakan algoritma kriptografi AES yang beroperasi dalam byte, bukan dalam bit dan mampu melakukan enkripsi terhadap plain text sebesar 16 byte atau 128 bit. Algoritma ini terdapat kunci internal yang disebut round key dimana pembangkitannya diambil dari cipher key, sehingga sangat cocok diterapkan dalam enkripsi file yang disimpan secara online. Salah satu cara untuk mengetahui tingkat keamanan suatu algoritma kriptografi dapat dilakukan dengan cara menghitung nilai avalanche effect dari file yang telah terenkripsi. Karena algoritma Rijndael beroperasi pada byte, maka avalanche effect cocok untuk mengetahui tingkat keamanan suatu algoritma kriptografi.

Perbedaan ukuran file yang di-upload berbanding lurus dengan waktu yang dibutuhkan untuk mengenkripsi file. Faktor-faktor yang mempengaruhi waktu enkripsi adalah ukuran file, tipe file, batas maksimum memori, maksimum waktu eksekusi. Tipe file yang paling rendah waktu enkripsinya adalah tipe text, sedangkan yang paling tinggi adalah tipe zip. Faktor-faktor yang berpengaruh terhadap hasil ciphertext adalah plaintext dan key. Perhitungan avalanche effect yang dihasilkan tidak sama disebabkan karena pengaruh dari penjadwalan kunci yang dilakukan dalam algoritma Rijndael.

Kata Kunci : algoritma rijndael, avalanche effect, kriptografi, enkripsi, dekripsi, tipe file.

Abstract

Internet service into one of the ways to get various kinds of information because it easier for users to perform various activities. Online file storage facility on the Internet ease the process of accessing data. The files stored online are not completely safe, storage security should be an absolute necessity.

One of the cryptographic algorithm is a block cipher Rijndael algorithm. Rijndael is the AES cryptographic algorithm that operates in bytes, not in bits and able to perform the encryption of the plain text of 16 bytes or 128 bits. These algorithms are called the internal lock key round in which pembangkitannya taken from the cipher key, making it very suitable to be applied in encrypting files stored online. One way to determine a security level of cryptographic algorithms can be done by calculating the value of avalanche effect of the files that have been encrypted. Because the Rijndael algorithm, operates on bytes, the avalanche effect suitable to determine the security level of a cryptographic algorithm.

Differences in the size of the uploaded file is proportional to the time needed to encrypt a file. Factors that affect the encryption time is file size, file type, maximum memory, maximum execution time. The lowest type of file encryption time is type text, while the highest are the type of zip. Factors influencing the results of the plaintext and ciphertext is the key. Avalanche effect resulting calculation is not the same due to the influence of key scheduling is done in the Rijndael algorithm.

Keywords : rijndael algorithm, avalanche effect, cryptography, encryption, decryption, file type.

---

1. Pendahuluan

1.1 Latar belakang

Informasi adalah hal terpenting untuk berkomunikasi. Tukar menukar informasi merupakan salah satu komunikasi antar dua belah pihak yang saling membutuhkan informasi. Pertukaran informasi banyak dilakukan di dunia maya, yaitu melalui teknologi Internet. Layanan internet yang ada sekarang menjadi salah satu cara untuk mendapatkan berbagai macam informasi sesuai dengan keinginan selain dengan cara membaca buku. Keberadaan internet sangat memudahkan para pengguna layanan internet untuk melakukan berbagai kegiatan. Seiring dengan berkembangnya teknologi, perkembangan teknologi mengenai aplikasi web juga berkembang cukup pesat, para developer web akan terus mengembangkan aplikasinya dengan interaktif dan responsive sehingga akan menarik minat para pengguna web untuk membuka aplikasi yang dibangunnya.

Internet memiliki cakupan daerah yang luas, sehingga dapat dipergunakan untuk penyebaran informasi, transaksi, dan penyimpanan data secara online. Penyimpanan file secara online sudah banyak dilakukan. Teknik ini mempermudah proses pengaksesan data karena tidak dibatasi kapan dan dimana kita membutuhkan file tersebut. Tidak lagi memerlukan tempat menyimpan data dengan kapasitas besar yang harus dibawa kemana-mana. Hanya memerlukan koneksi internet dan langsung dapat mengakses file yang diinginkan kapan saja, dimana saja.

File yang disimpan secara online tidak sepenuhnya aman. Padahal keamanan file yang disimpan secara online mutlak diperlukan. Mulai dari keamanan dari perubahan oleh yang tidak berhak merubahnya, hingga keamanan dari pencurian file. Terutama untuk file-file yang sifatnya rahasia, hanya pihak-pihak tertentu saja yang memiliki wewenang mengakses file tersebut.

Pada saat melakukan enkripsi terhadap file yang akan disimpan secara online, *file encryption* beroperasi dalam *byte*. Oleh karena itu untuk membangun sistem enkripsi seperti ini, algoritma enkripsi yang dipakai adalah algoritma yang bekerja dengan *byte* juga. Jenis algoritma seperti itu dinamakan *cipher* blok (*block cipher*). Rangkaian bit *plaintext*/*ciphertext* yang akan dienkripsi atau didekripsi dibagi menjadi blok-blok bit yang panjangnya sama dan sudah ditentukan sebelumnya.

Terdapat berbagai macam algoritma kriptografi, klasik maupun modern, bersifat simetris dan asimetris. Begitu juga dengan algoritma kriptografi *cipher* blok yang sudah pernah dipublikasikan. Salah satu algoritma kriptografi *cipher* blok yang terbaru adalah algoritma Rijndael. Algoritma ini adalah pemenang sayembara terbuka yang diadakan oleh *NIST* (*National Institute of Standards and Technology*) pada tahun 2001. Algoritma Rijndael menjadi standard kriptografi yang dominan paling sedikit selama 10 tahun.

Algoritma Rijndael adalah algoritma yang beroperasi dalam *byte*, bukan dalam *bit*. Algoritma ini mampu melakukan enkripsi terhadap *plaintext* sebesar 16 *byte* atau 128 *bit*. Selain itu, algoritma ini juga menggunakan kunci sebanyak 16 *byte*. Dengan kunci sepanjang 128 *bit*, maka terdapat 2128 = 3,4 x 1038 kemungkinan kunci. Selain panjang kunci yang lumayan banyak, kunci internal pada algoritma

ini juga selalu berubah pada setiap putarannya. Kunci internal ini disebut dengan *round key* yang pembangkitannya diambil dari *cipher key*, sehingga sangat cocok diterapkan dalam enkripsi file yang akan disimpan secara online.

Algoritma kriptografi Rijndael merupakan algoritma kriptografi AES. Untuk menilai tingkat keamanan sebuah algoritma kriptografi dapat menggunakan banyak cara, seperti *avalanche effect, block size, key size, modes of operation*, dan *weak key*[13]. Salah satu cara untuk mengetahui tingkat keamanan suatu algoritma kriptografi dapat dilakukan dengan cara menghitung nilai *avalanche effect* dari file yang telah terenkripsi. *Avalanche effect* menghitung perbedaan bit pada dua *chipertext* yang keluar dari hasil enkripsi menggunakan algoritma kriptografi. Karena algoritma Rijndael beroperasi pada *byte*, maka *avalanche effect* cocok untuk mengetahui tingkat keamanan suatu algoritma kriptografi.

1.2 Perumusan masalah

Karena terdapat masalah-masalah seperti yang telah dipaparkan pada latar belakang, yaitu :

1. data yang disimpan secara online tidak sepenuhnya aman,
2. diperlukan sebuah aplikasi berbasis web untuk menyimpan file dengan enkripsi menggunakan algoritma kriptografi berbasis web,
3. menilai *avalanche effect* dalam penyimpanan file online dengan algoritma Rijndael,

maka diperlukan sebuah aplikasi dapat membantu memecahkan masalah-masalah tersebut. Permasalahan yang akan dibahas pada tugas akhir ini adalah

1. bagaimana membuat aplikasi penyimpanan file online dengan enkripsi
2. karakteristik untuk menentukan avalanche effect pada suatu aplikasi dengan menggunakan algoritma kriptografi.

Agar tujuan tercapai maka diperlukan adanya ruang lingkup yang menjadi batasan masalah. Pada tugas akhir ini yang menjadi batasan masalah, yaitu :

1. algoritma kriptografi yang digunakan adalah algoritma kriptografi AES Rijndael
2. proses enkripsi dan dekripsi file menggunakan bahasa pemrograman PHP dengan algoritma kriptografi Rijndael
3. file dapat di download sebagai original (file aslinya pada saat di upload), enkripsi (file telah di enkripsi), dekripsi (file yang telah di dekripsi).
4. tidak membahas masalah jaringan dan trafiknya.

1.3 Tujuan

Dari masalah-masalah yang telah dirumuskan, dimaksudkan untuk membuat sebuah Aplikasi penyimpanan file online dengan enkripsi menggunakan algoritma AES (Advanced Encryption Standard) Rijndael. Tujuan dari pembuatan aplikasi ini adalah :

1. mengenkripsi file yang akan di simpan dalam penyimpanan file online.
2. menganalisa tingkat keamanan dari algoritma kriptografi Rijndael dengan menghitung nilai *Avalanche Effect* nya.
3. menganalisa lama waktu proses enkripsi menggunakan algoritma Rijndael.

1.4 Metodologi penyelesaian masalah

Metodologi yang digunakan dalam memecahkan masalah di atas adalah dengan menggunakan langkah-langkah berikut:

1. Studi Literatur dan pustaka.
   Pencarian dan penambahan wawasan dari jurnal, buku, artikel, sumber-sumber lain yang layak seperti informasi-informasi yang tersedia di internet mengenai implementasi algoritma kriptografi rijndael, metodelogi kriptografi khususnya rijndael, keamanan system dalam aplikasi online, serta aplikasi untuk menunjang pembuatan Tugas Akhir ini.
2. Pengumpulan Data dan informasi yang berkaitan dengan file yang sering Disimpan secara online sebagai studi kasus, dalam tugas akhir ini adalah data yang akan diolah dalam aplikasi online yang dibuat.
3. Implementasi Sistem.
   Pengembangan aplikasi penyimpanan file online dengan enkripsi menggunakan algoritma AES (Advanced Encryption Standard) Rijndael dengan tahap sebagai berikut :
   - Identifikasi masalah
     Permasalahan yang ada dalam mengidentifikasi masalah tugas akhir ini adalah bagaimana mengamankan file dengan cara *file encryption*, Sehingga dapat mempresentasikan *file encryption* menggunakan algoritma kriptografi Rijndael.
   - Pemodelan Algoritma AES Rijndael
     Permasalahan yang ada dalam mengidentifikasi masalah tugas akhir ini adalah bagaimana mengamankan file dengan cara *file encryption*, menentukan avalance effect dalam enkripsi file.

   Aplikasi yang akan dibangun adalah aplikasi berbasis web dengan kemampuan :
   - menyimpan (*upload*) data berupa file pada penyimpanan file online,
   - meng-enkripsi file yang akan disimpan pada penyimpanan file online,
   - mendekripsi file yang tersimpan pada penyimpanan file online,
   - mengambil (*download*) data berupa file yang terdekripsi dari penyimpanan file online,
   - menghitung *Avalanche Effect*.

   Proses menyimpan file pada penyimpanan file online dan mengambil file dari penyimpanan file online dilakukan dengan cara transfer file menggunakan *Hypertext Transfer Protocol* (HTTP).
4. Pengujian Sistem dan Analisis Hasil.
   Melakukan proses pengujian terhadap aplikasi online yang dibuat kemudian melakukan analisa hasil yang diperoleh untuk mencapai kesimpulan.
5. Pengambilan kesimpulan dan penyusunan laporan Tugas Akhir

5. Kesimpulan dan Saran

5.1 Kesimpulan

Kesimpulan yang dapat diambil pada tugas akhir ini antara lain :

1. Perbedaan ukuran file berpengaruh pada waktu enkripsi. Perbedaan ukuran file yang di-*upload* berbanding lurus dengan waktu yang dibutuhkan untuk mengenkripsi file, semakin besar file semakin lama proses enkripsi file tersebut.
2. Faktor-faktor yang mempengaruhi waktu enkripsi adalah ukuran file, tipe file, maksimum memori, maksimum waktu eksekusi. Faktor-faktor tersebut memiliki pengaruh yang berbeda-beda. Semakin besar ukuran file, maksimum memori, dan maksimum eksekusi, waktu enkripsi yang dihasilkan semakin besar. Tipe file yang paling rendah waktu enkripsinya adalah tipe file text, sedangkan yang paling tinggi waktu enkripsinya adalah tipe file zip.
3. Faktor-faktor yang berpengaruh terhadap hasil *ciphertext* setelah dilakukan enkripsi menggunakan algoritma Kriptografi Rijndael antara lain *plaintext* dan key. Faktor-faktor tersebut memiliki pengaruh yang berbeda-beda. Perubahan yang kecil pada *plaintext* maupun key akan menyebabkan perubahan yang signifikan terhadap *ciphertext* yang dihasilkan.
4. Perhitungan *avalanche effect* dilakukan dua cara yaitu dua kunci yang memiliki perbedaan satu bit dengan satu masukkan plainteks dan dua plainteks yang memiliki perbedaan satu bit dengan satu masukan kunci, dari tiap *avalanche effect* yang dihasilkan tidak sama disebabkan karena pengaruh dari penjadwalan kunci yang dilakukan dalam algoritma Rijndael. Rata-rata *avalance effect* yang dihasilkan 45 % sampai dengan 60 %, sehingga termasuk algoritma kriptografi yang baik terhadap penyimpanan file online.

5.2 Saran

Saran-saran untuk pengembangan tahap selanjutnya antara lain :

1. Dilakukan pengujian dengan jaringan yang berbeda untuk dianalisa pengaruh trafik jaringan terhadap hasil pengujian.
2. Dilakukan pengujian dengan spesifikasi komputer yang berbeda untuk dianalisa pengaruh penggunaan spesifikasi komputer terhadap hasil pengujian.

Referensi

[1] Ariyus, Dony, *Kriptografi Keamanan Data & Komunikasi*, Graha Ilmu, 2008.

[2] Ariyus, Dony, *Pengantar Ilmu Kriptografi : Teori Analisis dan Implementasi*, Andi Publisher, 2008.

[3] Daemen, Joan, and Rijmen, Vincent, *The Rijndael Block Cipher*, AES Proposal : Rijndael, 1999

[4] Johnson, Paul D, dan Blauch, Andrew J, *Structured Design Using Flowcharts*, Grand Valley State University, 2001

[5] Kadyanan, I Gusti Agung Gede Arya, dan Wicaksono, Soetam Rizky, *Proteksi File Pada Pocket PC Menggunakan Algoritma Rijndael dengan kombinasi serialisasi XML dan Kunci Device ID*, Seminar Nasional Sistem dan Informasi, 2007.

[6] Kurniawan, Yusuf, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, informatika, 2007.

[7] Kuswardono, Danang, *Algoritma Kriptografi Modern*, Teknik Informatika UDINUS.

[8] Munir, Rinaldi, *Kriptografi*, Informatika, 2006

[9] Munir, Rinaldi, *Matematika Diskrit*, Informatika, 2005

[10] Munir, Rinaldi, *Perancangan Algoritma Stream Cipher dengan Chaos*, Institut Teknologi Bandung, 2005

[11] Pangabean, Igor Bonny Tua, *Perbandingan Algoritma RC6 dengan Rijndael pada AES*, Jurusan Teknik Informatika ITB.

[12] Schneier, Bruce, *Aplied Cryptography 2nd*, John Wiley & Sons, 1996

[13] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
diakses sejak maret 2010

[14] http://en.wikipedia.org/wiki/Rijndael_key_schedule
diakses sejak Mei 2010

[15] http://id.wikipedia.org/wiki/Kriptografi
diakses sejak Maret 2010

[16] http://id.wikipedia.org/wiki/php
diakses sejak Mei 2010

[17] http://www.nist.gov/index.html
diakses sejak Mei 2010

[18] www.wikipedia.org
diakses sejak Februari 2010

[19] http://cakephp.org/
diakses sejak Februari 2010