JURNAL INTEGRASI
Vol. 7, No. 1, 2015, 77-81
ISSN: 2085-3858

Article History
Received February, 2015
Accepted March, 2015

Pemanfaatan Kriptografi Pada RESTFul Web Service

Festy Winda Sari[1], Andy Triwinarko[2]

[1]Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika

Politeknik Negeri Batam

Batam, Indonesia

festy@polibatam.ac.id

[2] Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika

Politeknik Negeri Batam

Batam, Indonesia

andy@polibatam.ac.id

Abstrak

Perkembangan teknologi komputer dan teknologi telekomunikasi pada saat ini telah mengubah cara pandang masyarakat dalam berkomunikasi. Perkembangan internet pada saat ini ditemukan pada teknologi web, khususnya pada RESTful web service. Kenyataan ini memberi pengaruh negatif terhadap setiap pertukaran data yang terjadi. Maka, pentingnya data bagi sebagian orang memungkinkan tindak kriminalitas didunia internet meningkat. Penelitian ini bertujuan untuk menerapkan kriptografi pada RESTful web service dan mengukur tingkat performansi dari algoritma yang digunakan. Maka, didalam penelitian ini, algoritma Rijndael dan 3DES digunakan dengan menggunakan metode perancangan konseptual dan perancangan sistem untuk mendapatkan hasil yang memuaskan terhadap kedua algoritma. Pengujian dilakukan pada sebuah website pengelolaan data perpustakaan dengan RESTful api. Ukuran dokumen yang berbeda digunakan namun memiliki panjang kunci yang sama. Berdasarkan pengujian dan analisa yang dilakukan, ditemukan bahwa algoritma Rijndael menunjukkan performansi yang lebih baik dibandingkan algoritma 3DES. Maka, algoritma Rijndael disarankan sangat baik untuk digunakan didalam web service sebagai pengaman data.
Kata kunci: Kriptografi, RESTFul, Web Service, Rijndael, 3DES.

Abstract

Nowadays, the development of computer technology and telecommunications technology has changed the way of people to communicate. The development of internet recently is found in web technology especially in RESTful web service. This fact contributes a negative influence for each data exchange orrurance. Therefore, the importance of the data for some people allow crime increased internet world. This study aimed to implement cryptography in RESTful web service and measured the level of performance of the algorithms used. 3DES and Rijndael algorithm used the conceptual design and the design of the system in order to obtain the satisfactory results for both algorithms. The tryout was conducted at a data management library website with RESTful fire. The document sizes were different but had the same key length. According to in-depth testing and analysis, it was found that Rijndael algorithm showed better performance than the 3DES algorithm. In a nutshell, Rijndael algorithm is best recommended to be used in the web service as a data security.
Keywords: Chryptograph, RESTFul, Web Service, Rijndael, 3DES.

1 PENDAHULUAN

Perkembangan teknologi komputer dan teknologi telekomunikasi pada saat ini telah mengubah cara pandang masyarakat dalam berkomunikasi. Sehingga berdampak negatif terhadap aspek keamanan data. Keterbukaan sistem memungkinkan penyadapan terhadap data yang sedang saling bertukar. Pentingnya data bagi sebagian orang memungkinkan tindak kriminalitas didunia internet meningkat, sehingga dibutuhkan sistem keamanan data yang mampu meminimalisir tingkat kriminalitas tersebut.

Kriptografi merupakan salah satu teknik yang digunakan untuk meningkatkan keamanan data yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. Kriptografi terdiri dari dua proses, yaitu enkripsi dan dekripsi. Penelitian ini menjadikan Rijndael sebagai algoritma yang digunakan dalam permasalahan diatas.

Penelitian ini dibatasi pada algoritma yang digunakan, yaitu Rijndael. Dan sebagai algoritma pembanding dalam pengujiannya digunakan algoritma 3DES. Pada hasilnya, didapat rekomendasi yang baik diantara keduannya untuk digunakan sebagai algoritma pengamanan data web service.

2 LANDASAN TEORI

Kode ASCII

Set karakter alfanumerik secara khusus mencakup 26 huruf alfabet (termasuk huruf besar dan huruf kecil), angka dalam digit sepuluh desimal, dan sejumlah simbol yang paling umum dipakai adalah ASCII (*American Standard Code for Information Interchange*) dan EBCDIC (*Extended Binary Coded Decimal Interchange Code*). ASCII merupakan kode 7-bit dan EBCDIC berupa kode 8- bit.

RESTFul Web Service

Pada dasarnya, RESTful harus memenuhi beberapa constraint. *Constraint* tersebut mendefinisikan bagaimana data ditransfer antar komponen dan keuntungan apa yang didapat. Tidak perlu mencari protokol jaringan baru untuk mengimplementasikannya, karena RESTful dapat diaplikasikan ke infrastruktur jaringan yang sudah ada seperti web, sehingga muncul RESTful *web service*.

Kriptografi

Kriptografi adalah ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. Kriptografi terdiri dari dua proses, yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengacak data sehingga tidak dapat dibaca dan dimengerti. Rijndael merupakan algoritma yang ditetapkan sebagai standar metode enkripsi modern pengganti DES (*Data Encryption Standard*). Sedangkan dekripsi adalah proses mengubah *ciphertext* menjadi *plaintext*, sehingga merupakan proses pembalikan dari enkripsi.

Algoritma kunci simetris

Skema algoritma sandi akan disebut kunci-simetris apabila untuk setiap proses enkripsi maupun dekripsi data secara keseluruhan digunakan kunci yang sama. Skema ini berdasarkan jumlah data per-proses dan alur pengolahan data didalamnya dibedakan menjadi dua kelas, yaitu *block-cipher* dan *stream-cipher*.

Algoritma kunci asimetris

Skema ini adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Skema ini disebut juga sebagai sistem kriptografi kunci publik karena kunci untuk enkripsi dibuat untuk diketahui oleh umum (*public-key*) atau dapat diketahui siapa saja. Tapi untuk proses dekripsinya hanya dapat dilakukan oleh yang berwenang yang memiliki kunci rahasia untuk mendekripsinya, disebut *private-key*.

Algoritma Rijndael

Algoritma Rijndael meliputi tiga tipe kunci yaitu kunci berkapasitas 256 bit, 192 bit, dan 128 bit. Besar kapasitas kunci berpengaruh terhadap jumlah putaran (*round*) yang diimplementasikan dalam algoritma ini.

Algoritma 3DES

3DES (Triple Data Encryption Standard) merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Proses yang dilakukan dalam penyandian datanya, yaitu proses enkripsi dan proses dekripsi. Algoritma 3DES adalah suatu algoritma pengembangan dari algoritma DES (Data Encryption Standard). Algoritma ini digunakan sebagai pembanding terhadap algoritma Rijndael.

3 HASIL DAN PEMBAHASAN

Implementasi dilakukan pada sebuah RESTful web service sederhana, yaitu web service untuk sebuah digital library dimana terdapat fungsi pengguna menggugah dan mengunduh dokumen.

3.1 Ujicoba Generate Key

Pengujian pertama dilakukan untuk meliihat kecepatan proses *generate* kunci oleh algoritma Rijndael-128. Ujicoba dilakukan di lingkungan intranet dengan kecepatan 72 Mbps dan koneksi yang dilakukan menggunakan jaringan wi-fi. Kecepatan proses generate key AES ditentukan dari panjang key. Dapat dilihat bahwa semakin panjang kunci, maka waktu yang diperlukan untuk proses generate key akan semakin lama. Hasil ujicoba dapat dilihat dalam table berikut:

Tabel 3.1 Hasil Ujicoba Algoritma Rijndael

Ujicoba ke-	Panjang kunci		Rata-rata waktu generate (ms)
	kata	karakter	
1	1	4	0.083
2	2	8	0.162
3	3	17	0.245
4	4	27	0.356

5	5	31	0.391

Untuk mengukur tingkat efisien waktu yang diperlukan, hasil ujicoba akan dibandingkan dengan sesama algoritma simetris, yaitu algoritma 3DES. Berikut adalah hasil ujicoba 3DES:

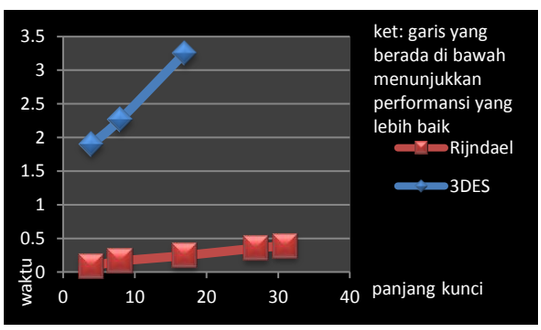
Tabel 3.2 Hasil Ujicoba Algoritma 3DES

Ujicoba ke-	Panjang kunci		Rata-rata waktu generate (ms)
	kata	karakter	
1	1	4	1.9
2	2	8	2.27
3	3	17	3.26
4	4	27	Error
5	5	31	Error

Pada algoritma 3DES, batas maksimum key berada pada 168 bit yang setara dengan 21 karakter. Sehingga ketika digunakan kunci dengan 27 karakter, sintaks akan membaca bahwa kunci terlalu panjang dan tidak dapat di proses.

Dapat dilihat perbandingan keduanya, pada algoritma Rijndael kenaikan waktu pada saat *generate key* berada pada persentase rata-rata 50% setiap ujicoba. Sedangkan pada algoritma 3DES, berada pada persentase rata-rata 32%. Maksudnya adalah, algoritma Rijndael membutuhkan waktu yang lebih cepat untuk *generate key* pada setiap perubahan key yang digunakan dibandingkan dengan algoritma 3DES.

Untuk lebih jelasnya, dapat digambarkan dalam grafik seperti berikut:



Gambar 3.1 Grafik Perbedaan Rijndael dan 3DES

3.2 Ujicoba Enkripsi Dokumen

Pengujian dilakukan untuk mengetahui hasil enkripsi terhadap dokumen, serta untuk mengetahui waktu yang dibutuhkan untuk melakukan enkripsi terhadap beberapa dokumen dengan ukuran dokumen yang berbeda. Untuk proses enkripsi, dilakukan pada saat user mengunggah dokumen. Uji coba fungsi unggah dilakukan pada aplikasi web dengan kecepatan koneksi adalah 72 Mbps dan koneksi yang dilakukan menggunakan jaringan wi-fi. Untuk melakukan enkripsi, digunakan kunci dengan panjang 14 karakter (112 bit).

Berikut adalah hasil ujicoba enkripsi dokumen:

Tabel 3.3 Hasil Ujicoba Enkripsi Dokumen Dengan Algoritma Rijndael

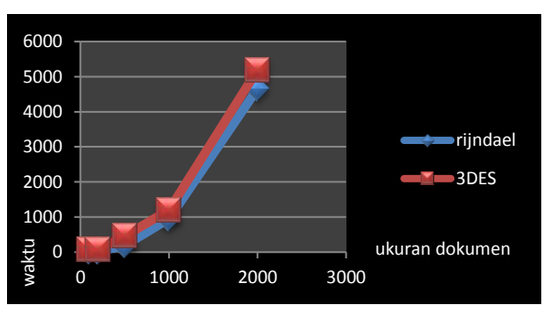
No	Ukuran dokumen sebelum dienkripsi (Kb)	Ukuran dokumen sesudah dienkripsi (Kb)	Waktu (ms)
1	100	138	20.40
2	200	277	20.90
3	500	678	196.80
4	1000	1359	948.86
5	2000	2790	4661.28

Untuk mengukur tingkat efisiensi waktu yang dibutuhkan algoritma dalam proses enkripsi dokumen, digunakan algoritma 3DES sebagai algoritma pembanding. Kunci yang digunakan adalah kunci yang serupa dengan penggunaan pada algoritma Rijndael. Berikut adalah hasil ujicoba enkripsi dokumen menggunakan algoritma 3DES:

Tabel 3.4 Hasil Ujicoba Enkripsi Dokumen Dengan Algoritma 3DES

No	Ukuran dokumen sebelum dienkripsi (Kb)	Ukuran dokumen sesudah dienkripsi (Kb)	Waktu (ms)
1	100	138	74.44
2	200	277	75.86
3	500	678	458.92
4	1000	1359	1202.96
5	2000	2790	5192.78

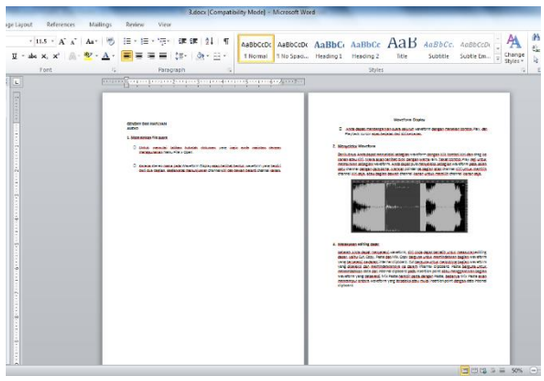
Hasil pada ujicoba enkripsi dokumen menghasilkan waktu yang berbeda pada masing-masing algoritma. Bahwa semakin besar ukuran dokumen, algoritma membutuhkan waktu yang lebih untuk proses enkripsi. Dapat dilihat pada grafik dibawah, perbedaan waktu tidak terlalu besar dikarenakan panjang kunci yang digunakan adalah sama. Namun, algoritma Rijndael lebih cepat mengenkripsi dokumen dibandingkan dengan algoritma 3DES.



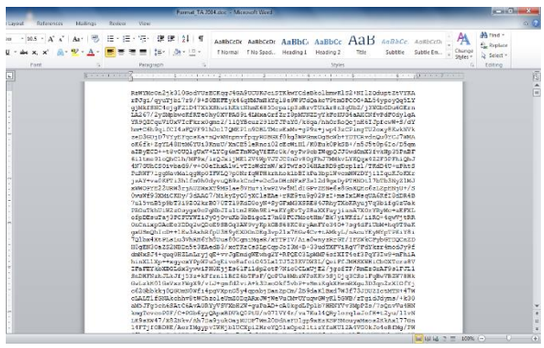
Gambar 3.2 Grafik Perbedaan Waktu Proses Enkripsi Rijndael dan 3DES

3.3 Ujicoba Hasil Enkripsi Dokumen

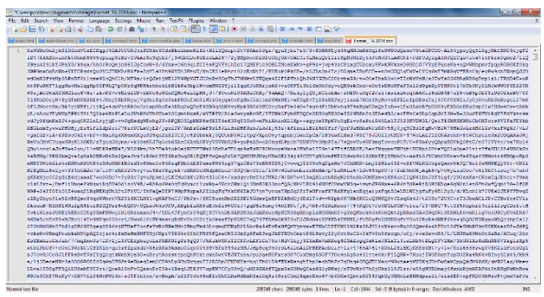
Pengujian ini dilakukan terhadap dokumen hasil enkripsi dengan tujuan memastikan bahwa dokumen hasil enkripsi tidak dapat dibuka pada text editor manapun. Berikut penampakan dokumen sebelum di enkripsi dan dokumen hasil enkripsi:



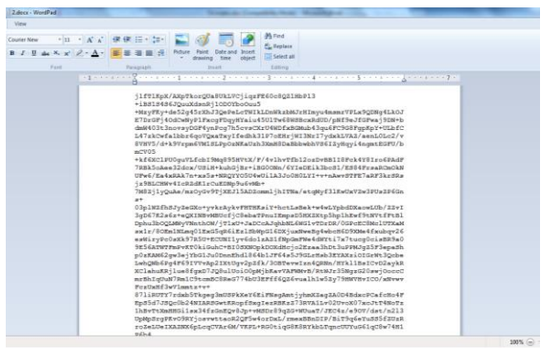
Gambar 3.3 Dokumen Sebelum Dienkripsi



Gambar 3.4 Dokumen Terenkripsi Dibuka Dengan Ms. Word



Gambar 3.5 Dokumen Terenkripsi Dibuka Dengan Notepad++



Gambar 3.6 Dokumen Terenkripsi Dibuka Dengan WordPad

4 KESIMPULAN

Berdasarkan penjabaran dari hasil ujicoba, dapat diambil beberapa kesimpulan, yaitu:

1. Kecepatan enkripsi yang dilakukan pada kedua algoritma berbanding lurus terhadap panjang kunci yang digunakan, semakin panjang kunci maka semakin lama waktu yang dibutuhkan untuk enkripsi dokumen.
2. Perbandingan hasil ujicoba *generate* kunci pada algoritma Rijndael dan 3DES membuktikan bahwa algoritma Rijndael lebih unggul secara performansi, karena membutuhkan waktu enkripsi yang lebih pendek dari algoritma 3DES dengan kunci yang lebih panjang.

4 SARAN

Adapun saran-saran terkait pengembangan penelitian selanjutnya adalah:

1. Algoritma ini nantinya dapat diterapkan kedalam metode *web service* yang lain.
2. Pengembang selanjutnya untuk dapat menggunakan parameter yang berbeda selain waktu, seperti dari sisi keamanan.

DAFTAR PUSTAKA

[1] Utama, Yadi. "Teknik Pemrograman Web Service PHP Dengan Menggunakan SOAP dan WSDL". Yogyakarta

[2] Lucky. 2008. "*XML Web services: Aplikasi Desktop, Internet & Handphone*". Jakarta: Jasakom

[3] http://isaninside.net/2011/06/tentang-web-service-dan-aplikasinya-di-wsns-latar-belakang-tesis.htm, diakses pada tanggal: 3 September 2014

[4] Sutanta, Edhy dan Khabib Mustofa. 2012. "Kebutuhan Web Service Untuk Sinkronisasi Data Antar Sistem Informasi dalam e-Gov Pemkab Bantul Yogyakarta". Jurnal TIK edisi Mei STMIK Bandung. Bandung

[5] http://csrc.nist.gov/encryption/aes/, diakses pada tanggal 30 Oktober 2014

[6] Ariyana, Yoki. "Advanced Encryption Standard". PPPPTK IPA BANDUNG

[7] Adi, Bayu Nugroho. "Proteksi Dokumen Office Menggunakan Xml Web Service Dengan Algoritma Elliptic Curve Cryptography (Ecc) Berbasis Web". Institute Teknologi Sepuluh November

[8] Marta, Revi Fajar. "Implementasi Kriptografi Pada E-Commerce". Institut Teknologi Bandung

[9] Triwinarko, Andy. "Elliptic Curve Digital Signature Algorithm (ECDSA) Departemen Teknik Informatika ITB". Institut Teknologi Bandung

[10] Fadli, Hadyan Ghaziani. "Studi dan Implementasi Algoritma Rijndael Untuk

Enkripsi Halaman Web HTML". Institut Teknologi Bandung

[11] Cahyani, Era, Elly Kristania, Ferry Hirawan. "Penerapan Metode Enkripsi Rijndael pada Sistem Pendaftaran Mahasiswa Secara Online". Universitas Bina Nusantara

[12] Hidayat, Akik. "Enkripsi Dan Dekripsi Data Dengan Algoritma 3 Des (Triple Data Encryption Standard)". Universitas Padjajaran