IMPLEMENTASI DAN ANALISA ALGORITMA WAKE DALAM PENYANDIAN DATA

Suziane[1], Suyanto[2], --[3]

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

Abstrak

Kerahasiaan data merupakan hal yang sangat diperlukan dalam komunikasi data. Untuk menjamin keamanan dan kerahasiaan data tersebut diperlukan teknik tertentu yang dapat menyandikan data. Teknik ini biasanya disebut dengan kriptografi. Ada banyak algoritma kriptografi seperti One Time Pad, RC4, RSA, dan sebagainya yang dianggap benar-benar mampu menjaga keamanan dan kerahasiaan data. Oleh karena itu para kriptografer berusaha menciptakan algoritma yang rumit untuk lebih menjamin keamanannya.
Algoritma WAKE (Word Auto Key Encryption) merupakan salah satu algoritma yang digunakan untuk menyandikan data. Penulis melakukan implementasi dan menganalisa algoritma ini. Yang dianalisa adalah kompleksitas algoritma, ukuran file, tingkat keamanan, dan perbandingan waktu eksekusi dengan algortima lainnya. Keamanan algoritma WAKE terletak pada jumlah putaran yang ditentukan oleh user. Semakin banyak putarannya, maka semakin acak kunci yang dihasilkan, dan semakin aman data tersebut.

Kata Kunci : kriptografi, WAKE, keamanan data

Abstract

Confidentiality of data is much needed in data communication. To ensure the security and confidentiality of the data required a technique that can encode data. This technique is usually called cryptography. There are many cryptography algorithms such as One Time Pad, RC4, RSA, and others that are considered fully capable of maintaining security and confidentiality of data. Therefore the cryptographer attempt to create a complex algorithm to ensure the better safety.
Algorithm WAKE (Word Auto Key Encryption) is one of the algorithm that is used to encode data. The author implementate and analyzes the algorithm. The author analyzed the complexity, the file size, security level, and the comparison of the execution time with the other cryptography algorithm.
WAKE security algorithm lies in the number of cycles specified by the user. If there are plentiful cycles, the generated key more random, and the data more secure.

Keywords : crypthography, WAKE, security of data

1 Pendahuluan

1.1 Latar belakang masalah

Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikannya. Cara pengamanan tersebut dapat dilakukan dengan penyandian data. Saat ini sudah banyak algoritma yang bisa digunakan untuk penyandian data. Salah satunya adalah algoritma WAKE.

Algoritma WAKE merupakan salah satu algoritma kriptografi yang telah digunakan secara komersial. WAKE merupakan singkatan dari *Word Auto Key Encryption*. Algoritma ini ditemukan oleh David Wheeler pada tahun 1993 dan merupakan salah satu algoritma *stream cipher* (*Cipher* aliran) yang cepat dalam implementasinya dalam perangkat lunak. Metode ini menggunakan kunci 128 bit, plaintext 32 bit dan sebuah tabel 256 x 32 bit. Dalam algoritmanya, metode ini menggunakan operasi XOR, AND, OR dan Shift Right. Metode WAKE ini telah digunakan pada program Dr. Solomon Anti Virus versi terbaru. Inti dari metode WAKE terletak pada proses pembentukan tabel *S-Box* (*Substitution Box*) dan proses pembentukan kunci. Tabel *S-Box* dari metode WAKE bersifat fleksibel dan berbeda-beda untuk setiap putaran. Keistimewaan dari metode ini adalah banyak putaran yang ditentukan oleh *user*, sedangkan algoritma yang lain jumlah putarannya sudah ditentukan.

Berikut tabel perbandingan algoritma kriptografi *stream cipher* : [12]

Stream Cipher	Creation Date	Speed (cycles per byte)	(bits)			Attack	
			Effective Key-Length	Initialization vector	Internal State	Best Known	Computational Complexity
A5/1	1989	Voice (WHW)	54	114	64	Active KPA OR KPA Time-Memory Tradeoff	~2 seconds OR $2^{39.91}$
A5/2	1989	Voice (WHW)	54	114	64?	Active	4.6 milliseconds
FISH	1993	Quite Fast (WSW)	Huge	?	?	Known-plaintext attack	2^{11}
Grain	Pre-2004	Fast	80	64	160	Key-Derivation	2^{43}
HC-256	Pre-2004	4 (WPE)	256	256	65536	?	?
ISAAC	1996	2.375 (W64-bit) - 4.6875 (W32-bit)	8-8288 usually 40-256	N/A	8288	(2006) First-round Weak-Internal-State-Derivation	4.67×10^{1240} (2001)
MUGI	1998-2002	?	128	128	1216	N/A (2002)	$\sim 2^{82}$
PANAMA	1998	2	256	128?	1216?	Hash Collisions (2001)	2^{82}
Phelix	Pre-2004	up to 8 (W86)	256 + a 128-bit Nonce	128?	?	Differential (2006)	2^{37}
Pike	1994	0.9 x FISH (WSW)	Huge	?	?	N/A (2004)	N/A (2004)
Py	Pre-2004	2.6	8-2048? usually 40-256?	64	8320	Cryptanalytic Theory (2006)	2^{75}
Rabbit	2003-Feb	3.7(WPE)-9.7(WARM7)	128	64	512	N/A (2006)	N/A (2006)
RC4	1987	Impressive	8-2048 usually 40-256	8	2064	Shamir Initial-Bytes Key-Derivation OR KPA	2^{13} OR 2^{33}
Salsa20	Pre-2004	4.24 (WG4) - 11.84 (WPE)	128 + a 64-bit Nonce	512	512 + 384 (key+IV+index)	Differential (2005)	N/A (2005)
Scream	2002	4 - 5 (WSW)	128 + a 128-bit Nonce	32?	64-bit round function	?	?
SEAL	1997	Very Fast (W32-bit)	?	32?	?	?	?
SNOW	Pre-2003	Very Good (W32-bit)	128 OR 256	32	?	?	?
SOBER-128	2003	?	up to 128	?	?	Message Forge	2^{-6}
SOSEMANUK	Pre-2004	Very Good (W32-bit)	128	128	?	?	?
Trivium	Pre-2004	4 (W86) - 8 (WLG)	80	80	288	Brute force attack (2006)	2^{135}
Turing	2000-2003	5.5 (W86)	?	160	?	?	?
VEST	2005	42 (WASIC) - 64 (WFPGA)	Variable usually 80-256	Variable usually 80-256	256 - 800	N/A (2006)	N/A (2006)
WAKE	1993	Fast	?	?	8192	CPA & CCA	Vulnerable
Stream Cipher	Creation Date	Speed (cycles per byte)	(bits)			Attack	
			Effective Key-Length	Initialization vector	Internal State	Best Known	Computational Complexity

Gambar 1-1 : Perbandingan Metode WAKE dengan metode stream cipher lainnya

Berdasarkan uraian di atas maka penulis ingin membuat tugas akhir dengan judul ”Implementasi dan Analisa Algoritma WAKE dalam Penyandian Data”.

1.2 Perumusan masalah

Yang menjadi permasalahan dalam menyusun tugas akhir ini adalah :

1. Bagaimana cara meng-implementasikan algoritma WAKE pada suatu program.
2. Bagaimana performansi algoritma WAKE dalam penyandian data.

Batasan masalah dalam pembuatan tugas akhir ini adalah :

1. Input data berupa karakter (string).
2. Tahap-tahap perhitungan ditampilkan dalam bentuk biner dan desimal.

1.3 Tujuan

Tujuan penyusunan tugas akhir ini adalah :

1. Mengimplementasikan algoritma WAKE pada program simulasi.
2. Menganalisa performansi algoritma WAKE, yaitu :
    a. Kompleksitas Algoritma.
    b. Ukuran file sebelum dan sesudah di enkripsi.
    c. Tingkat keamanan algoritma WAKE dilihat dari proses pengacakan kuncinya.
    d. Waktu komputasi yang dibutuhkan. Output yang dihasilkan berupa angka perbandingan.

1.4 Hipotesa awal

Hipotesa awal yang diambil dari proses penyandian data dengan menggunakan algoritma WAKE adalah :

1. Memiliki kompleksitas waktu yang besar karena banyak langkah yang harus dieksekusi.
2. Ukuran file setelah dienkripsi lebih kecil atau sama dengan ukuran file sebelum dienkripsi.
3. Memiliki kerumitan kunci yang tinggi, sehingga keamanannya lebih tinggi.
4. Algoritma WAKE memiliki waktu komputasi yang lebih cepat dibandingkan RC4 dan *One Time Pad*.

1.5 Metodologi penyelesaian masalah

Langkah-langkah yang dilakukan oleh penulis dalam pembuatan tugas akhir ini adalah :

1. Membaca dan mempelajari buku-buku kriptografi dan literatur yang berhubungan dengan metode kriptografi WAKE.
2. Membaca dan mempelajari buku-buku pemrograman dasar dengan menggunakan Microsoft Visual Basic 6.0
3. Mempelajari cara kerja dari metode kriptografi WAKE.
4. Melakukan pemodelan terhadap algoritma kriptografi WAKE.
5. Merancang sistem yang mengaplikasi metode kriptografi WAKE.

6. Melakukan proses pengujian dan pengecekan kesalahan (error) terhadap program yang telah dirancang.
7. Menganalisa performansi algoritma kriptografi WAKE dengan cara membandingkannya dengan salah satu algoritma *stream cipher* lainnya.
8. Membuat laporan tugas akhir yang telah dibuat.

5 KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah selesai menyusun tugas akhir ini, penulis dapat mengambil kesimpulan bahwa :

1. Program aplikasi yang dibuat oleh penulis, dapat menampilkan langkah demi langkah dalam proses penyandian data. Sehingga *user* dapat lebih memahami cara kerja dan algoritma kriptografi WAKE.
2. Proses penyandian data dalam kriptografi WAKE terbagi atas 4 proses, yaitu :
    a. Proses pembentukan table S-Box.
    b. Proses pembangkitan kunci (*keystream*).
    c. Proses Enkripsi.
    d. Proses deskripsi.
3. Besar kompleksitas algoritma dilihat berdasarkan waktu adalah T(n) = O (n log n).
4. Ukuran file antara sebelum dan sesudah proses penyandian data adalah sama, karena dilakukan proses XOR antara plainteks dengan kunci, dan tidak dilakukan *padding*.
5. Algoritma WAKE memiliki tingkat keamanan yang baik dilihat dari proses pengacakan kuncinya, di mana semakin banyak putaran yang dilakukan pada proses pembentukan *keystream*, semakin acak kunci yang dihasilkan.
6. Bila dibandingkan dengan metode *stream cipher* lainnya, algoritma WAKE membutuhkan waktu lebih lama dalam mengeksekusi, atau dapat disimpulkan bahwa algoritma WAKE tidak semangkus dibandingkan dengan metode *One Time Pad* dan RC4. Tetapi kemangkusan suatu algoritma tidak menjamin tingkat keamanan dari algoritma tersebut. Biasanya waktu berbanding terbalik dengan keamanan. Semakin banyak proses yang dilakukan, semakin lama waktu yang dibutuhkan untuk mengeksekusinya, dan semakin acak *keystream* yang dihasilkan.

5.2 Saran

Penulis ingin memberikan beberapa saran yang mungkin dapat membantu dalam pengembangan metode kriptografi WAKE, yaitu :

1. Metode WAKE dapat dimodifikasi untuk mempertangguh keamanan dari metode tersebut seperti mengganti operasi-operasi logika dalam metode WAKE dengan metode rancangan sendiri.
2. Program aplikasi ini dapat dikembangkan untuk menampilkan proses enkripsi dan dekripsi untuk tipe data lainnya.

DAFTAR PUSTAKA

[1] Http://eprint.iacr.org/2001/065.pdf, tanggal 5 Maret 2009.

[2] Http://www.cix.co.uk/~klockstone/hereward.htm, tanggal 5 Maret 2009.

[3] Http://www.cix.co.uk/~klockstone/wake.htm, tanggal 5 Maret 2009.

[4] K. Jusuf Ir, M.T., Kriptografi, **Keamanan Internet dan Jaringan Komunikasi**, Penerbit Informatika Bandung, 2002.

[5] Menezes, Oorcshot, and Vanstone, *Handbook of Applied Cryptography*, CRC Press, Inc. USA, 1996.

[6] Munir, Rinaldi, Ir., M.T, Diktat Kuliah Kriptografi IF-5054, Informatika-ITB, Bandung, 2007.

[7] Munir, Rinaldi, Ir., M.T, Diktat Kuliah Matematika IF 2151 Matematika Diskrit, Informatika-ITB, Bandung, 2004.

[8] S. Ario, ***Microsoft Visual Basic 6.0***, PT. Elex Media Komputindo, 2001.

[9] S. Bruce, ***Applied Crytography***, Second Edition, John Wiley & Sons, Inc, 2007.

[10] Sodhi, Jag, ***Software Engineering Methods, Management, and CASE Tools, TAB Professional dan Reference Books***, Amerika, 1991.

[11] http://www.cdrummond.qc.ca/cegep/informat/Professeurs/Alain/files/asc ii.htm, tanggal 20 Maret 2009

[12] Matt J. B. Robshaw, Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories, 1995