SIMULASI DAN ANALISIS KRIPTOGRAFI ALGORITMA F8 DAN F9

Dita Agustiono[1], Iwan Iwut Tritoasmoro[2], Sofia Naning Hertiana[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

UMTS (Universal Mobile Telecomunication System) merupakan sistem komunikasi nirkabel generasi ketiga yang merupakan hasil pengembangan dari GSM (Global System for Mobile Communication). Dengan semakin pesatnya perkembangan teknologi seluler (nirkabel) ini, sistem keamanannya juga semakin mendapat perhatian untuk menghindari adanya pencurian informasi oleh pihak atau badan yang tidak bertanggung jawab.

Sistem keamanan pada jaringan UMTS menggunakan kriptografi algoritma f8 dan f9 untuk menjaga kerahasiaan dan integritas data antara User Equipment (UE) dan Radio Network Controller (RNC). Algoritma f8 merupakan algoritma untuk proses enkripsi-dekripsi untuk menjaga kerahasiaan data. Sedangkan algoritma f9 adalah algoritma untuk menghasilkan kode yang ditambahkan ke data yang akan dikirim untuk menjaga integritas data. Algoritma f8 dan f9 dibuat berdasarkan algoritma block cipher KASUMI yang merupakan jenis algoritma simetri dimana kunci yang dipakai untuk proses enkripsi dan dekripsi sama dengan inputan 64-bit dan ukuran kunci 128-bit menghasilkan outputan 64-bit. Tugas akhir ini secara khusus membahas simulasi kriptografi algoritma f8 dan f9 pada UMTS dengan menggunakan Matlab 2007a. Kemudian membuktikan kemampuan sistem algoritma f8 dan f9 dengan cara menganalisa waktu dan performansi proses, serta menganalisa tingkat distribusi keacakan atau perubahan bitnya dan avalanche effect pada algoritma f8. Dan mengukur kehandalan algoritma f8 dan f9 dari Brute Force Attack.

Dari hasil pengujian dapat disimpulkan perubahan bit input dan output algoritma f8 dari beberapa kali percobaan untuk teks =53,5125%, suara=51,254%, dan gambar=49,81162%. Waktu dan performansi algoritma f8 dan f9 hampir sama. Nilai avalanche effect algoritma f8 berdasarkan perubahan 1 bit kunci mencapai 50,23202% sedangkan berdasarkan perubahan 1 bit plaintext atau ciphertext hanya 3,125%. Sedangkan waktu untuk melakukan brute forced attack pada algoritma f8 dan f9 ialah 1,618 x 1040 tahun.

Kata Kunci : UMTS, Algoritma f8, f9, KASUMI, brute force attack dan avalanche effect

Abstract

UMTS (Universal Mobile Telecomunication System) is a third generation wireless communication system which is the increasing of GSM (Global System for Mobile Communication). Because of the increase in cellular technology (wireless), the safety system get more attention to avoid the information robbing by the others side or groups who are not responsible.

Safety system of UMTS link use f8 and f9 cryptography algorithm to keep the confidentiality and integrity of data between User Equipment (UE) and Radio Network Controller (RNC). f8 algorithm is algorithm for encryption and decryption process to protect data confidentiality and f9 algorithm is algorithm to produce code attached to data for protect integrity. f8 and f9 algorithm is made according to KASUMI block cipher algorithm, a kind of simetry algorithm, where the key which is used to encryption and decription procces is 64-bit input and the 128-bit key will produce 64-bit output. This thesis specially discuss about cryptography f8 and f9 algorithm simulation using Mathlab 2007a. It also try to prove the ability of f8 and f9 algorithm system by analizing time and performance process, then analizing random distribution level or the changing of the bit and avalanche effect from f8 algorithm. And measure ability the f8 and f9 algorithm of brute force attack.

From the result of some test, it can be concluded that the f8 algorithm input and output bit changging for text =53,5125%, voice=51,254%, dan picture=49,81162%. Time and Performance process for f8 and f9 is almost the same. Avalanche effect value of f8 algorithm for one bit key changing is 50,23202% while for one bit plaintext or ciphertext is about 3,125%. Otherwise, the delay to do brute forced attack for f8 and f9 algorithm is 1,618 x 1040 years.

Keywords : UMTS, f8 and f9 Algorithm, KASUMI, brute force attack dan avalanche effect

BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini, komunikasi *mobile* sudah menyebar ke seluruh dunia dengan sangat cepat, dengan perkembangan teknologi yang tidak kalah cepat pula. Teknologi komunikasi *mobile* telah mencapai generasi ketiga (3G) dimana telah dapat melakukan transfer data suara dan data lainnya secara bersamaan. Dengan semakin pesatnya perkembangan teknologi seluler (nirkabel) ini, perhatian pada tingkat-tingkat keamanannya juga semakin mendapat perhatian. UMTS (Universal Mobile Telecomunication System) adalah sebuah standar internasional untuk sistem komunikasi *mobile* 3G yang menggunakan metode kriptografi untuk menjaga kerahasiaan informasi yang ditransmisikan antara UE (User Equipment) dan RNC (Radio Network Controller)

Sistem keamanan pada jaringan UMTS menggunakan kriptografi algoritma f8 dan f9 untuk menjaga kerahasiaan dan integritas data antara UE dan RNC. Algoritma f8 merupakan algoritma untuk proses enkripsi-dekripsi untuk menjaga kerahasiaan data. Sedangkan algoritma f9 adalah algoritma untuk menghasilkan kode yang ditambahkan ke data yang akan dikirim untuk menjaga integritas data. Algoritma f8 dan f9 dibuat berdasarkan algoritma block cipher KASUMI yang merupakan jenis algoritma simetri dimana kunci yang dipakai untuk proses enkripsi dan dekripsi sama dengan inputan 64-bit dan ukuran kunci 128-bit menghasilkan outputan 64-bit.

Tugas akhir ini secara khusus membahas simulasi kriptografi algoritma f8 dan f9 dengan menggunakan Matlab 2007a. Kemudian membuktikan kemampuan sistem algoritma f8 dan f9 dengan cara menganalisa waktu dan performansi proses, serta menganalisa tingkat distribusi keacakan atau perubahan bitnya dan *avalanche effect* pada algoritma f8. Dan mengukur kehandalan algoritma f8 dan f9 dari *Brute Force Attack*

1.2 Tujuan Tugas Akhir

Tujuan dari tugas akhir ini adalah :

1. Membuat aplikasi simulasi algoritma f8 dan f9.
2. Membuktikan kemampuan sistem algoritma f8 dari tingkat distribusi keacakan atau perubahan bitnya, waktu dan performansi proses dan *avalanche effect*

3. Membuktikan kemampuan sistem algoritma f9 dari waktu dan performansi proses
4. Mengukur kehandalan algoritma f8 dan f9 terhadap *Brute Force Attack*.

1.3 Rumusan Masalah

Dalam Tugas akhir ini akan dibahas kriptografi algoritma f8 dan f9.

Parameter-parameter yang akan dilakukan penganalisaan dan pensimulasian :

1. Bagaimana memodelkan kriptografi algoritma f8 dan f9
2. Bagaimana perubahan bit-bit setelah proses pengenkripsian dan pendeskripsian suatu inputan data pada algoritma f8.
3. Bagaimana lamanya waktu pemrosesan dan performansi pada algoritma f8 dan f9. Serta tingkat avalanche effect akibat perubahan bit plaintext maupun kunci pada algoritma f8.
4. Bagaimana tingkat kehandalan algoritma f8 dan f9 terhadap *Brute Force Attack*

1.4 Batasan Masalah

Tugas akhir ini dibatasi pada ruang lingkup algoritma f8 dan f9. Pembahasan hanya difokuskan pada penganalisaan simulasi dengan melakukan percobaan-percobaan. Berikut batasan-batasan yang dipakai :

- Pembahasan hanya akan difokuskan pada analisis dan simulasi menggunakan kriptografi algoritma f8 dan f9
- Proses enkripsi atau dekripsi *plaintext* atau *ciphertext* menjadi *ciphertext* atau *plaintext* pada algoritma f8.
- Proses menghasilkan kode Message Authentication Code-Integrity(MAC)/XMAC-I pada algoritma f9.
- Analisis hasil enkripsi atau dekripsi algoritma f8 dengan parameter : perubahan bit, lama proses, performansi, dan *avalanche effect.*
- Analisis hasil MAC-I/XMAC-I algoritma f9 dengan parameter: lama proses dan performansi
- Tidak memperhatikan skema modulasi hingga demodulasi, kanal, dan faktor-faktor propagasi lainnya

- Tidak memperhatikan di bagian perangkat antara User Equipment (UE) pelanggan dan sentral operator UMTS baik itu dari segi *hardware* maupun *software*nya

1.5 Metode Penelitian

Dalam menyelesaikan Tugas Akhir ini penulis akan melakukan metode :

1. Study Literatur dan survey dengan mengumpulkan data melalui buku-buku, jurnal ilmiah yang berkaitan dengan algoritma f8, f9 dan kriptografi algoritma KASUMI
2. Percobaan pada simulasi algoritma f8 dan f9 dengan menjalankan program pada komputer untuk mendapatkan data nilai dari analisa berupa lamanya pemrosesan dan ukuran ataupun kondisi data setelah dilakukan enkripsi yang dibandingkan dengan data sebelum dienkripsi .
3. Metode penghitungan nilai *avalanche effect*nya dan tingkat distribusi keacakan ciphertextnya dengan cara membandingkan besarnya perubahan bit antara inputan dan outputan dari hasil enkripsi dan dekripsi pada simulasi algoritma f8.
4. Analisa pengujian kehandalan algoritma f8 dan f9 terhadap *attack*/serangan.
5. Penyusunan laporan tugas akhir dan kesimpulan akhir

1.6 Sistematika Penulisan

Tugas Akhir ini ditulis dengan sistematika :

BAB I PENDAHULUAN

Berisi tentang Latar Belakang, Perumusan Masalah, Pembatasan Masalah, Metodologi Penyelesaian Masalah serta Sistematika Penulisan.

BAB II DASAR TEORI

Membahas dasar teori yang berhubumgan dengan sistem keamanan UMTS (Universal Mobile Telecommunication System) menggunakan algoritma f8 dan f9. Teori dasar ini difokuskan pada teori-teori dasar pada mekanisme, kriptografi, algoritma KASUMI, algoritma f8 dan f9 itu sendiri.

BAB III PERANCANGAN SIMULASI ALGORITMA f8 DAN f9

Bab ini akan membahas proses perancangan implementasi software algoritma f8 dan f9.

BAB IV HASIL DAN ANALISA

Membahas tentang analisis dari hasil pengujian ataupun percobaan pada simulasi algoritma f8 dan f9.

BAB V KESIMPULAN DAN SARAN

Pada bab ini akan menjelaskan kesimpulan dan saran sebagai hasil dari analisa dan simulasi Tugas Akhir.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil percobaan simulasi algoritma f8 dan f9 dapat ditarik kesimpulan sebagai berikut:

1. Perubahan bit input dan output algoritma f8 dari beberapa kali percobaan untuk teks =53,5125 %, suara=51,254%, dan gambar=49,81162%. Dari hasil ini dapat disimpulkan bahwa algoritma f8 memiliki tingkat pengacakan yang baik.
2. Tingkat pengacakan oleh algoritma f8 dipengaruhi sebagian besar oleh kunci (CK)
3. Waktu proses untuk proses enkripsi-dekripsi algoritma f8 dan proses MAC-I-/XMAC-I algoritma f9 tergantung dari besar data. Semakin besar data semakin lama waktu prosesnya.
4. Waktu dan performansi untuk proses enkripsi-dekripsi algoritma f8 dan proses MAC-I/XMAC-I algoritma f9 hampir sama.
5. Nilai rata-rata avalanche effect untuk perubahan satu bit plaintext dari beberapa kali percobaan pada algoritma f8 sangat kecil, yaitu 3,125% hal ini dikarenakan bit plaintext tidak mengalami pengacakan oleh algoritma f8, sehingga jika ada perubahan satu bit pada plaintext, ciphertextnya tidak mengalami perubahan yang signifikan.
6. Nilai rata-rata avalanche effect untuk perubahan satu bit kunci dari beberapa kali percobaan yaitu 50,23202% mendekati nilai 50%. Ini berarti algoritma f8 menghasilkan *ciphertext* yang sangat acak.
7. Algoritma f8 dan f9 mempunyai ketahanan terhadap *brute forced attack* atau *exhaustive key search* yang baik, yaitu selama 1,618 x 10^{40} tahun dikarenakan kedua algoritma tersebut menggunakan panjang kunci yang sama yaitu 128-bit.

5.2 Saran

1. Menggunakan bahasa pemrograman yang lain. Hal tersebut dikarenakan waktu proses yang lama pada Matlab dikarenakan meng-compile kembali bahasanya kedalam java, c++, dan fortran.
2. Dapat diimplementasikan dengan hardware.

DAFTAR PUSTAKA

[1] 3GPP TS 33.102 V4.4.0 (2002-06). *3G Security; Security Architecture.Release 4*.2002

[2] 3GPP TS 35.201 V7.0.0 Release 7. *f8&f9 specification*.2007

[3] 3GPP TS 35.206 V7.0.0 Release 7.*f1, f2, f3, f4, f5 algorithm specification*.2007

[4] Donnie, 2006. *Studi Algoritma KASUMI(A5/3) Block Cipher*. Institut Teknologi Bandung. Bandung.

[5] Gilbert, Henry. 2001. *Design and Analysis of Cryptographic Algorithms for Mobile Communication Systems*. Orange group.

[6] Howard, Peter, 2006.*GSM and UMTS Security*.University of London. Inggris

[7] Jaaskelainen, Jukka, 2003. *Performance evaluation of software ciphering in UMTS radio network controller*. Nokia. Finlandia

[8] Kasera Sumit, Nishit Narang.2004.*3G Mobile Networks*.McGaw-Hill.India

[9] Kurniawan, Yusuf, 2004.*Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*. Informatika. Bandung

[10] Masigi, Jepri Rinaldi, 2006. *Simulation And Analysis Cryptography A5/2 Algorithm For GSM Security*, Jurusan Teknik Informatika. Bandung

[11] Nyberg, Kaisa, 2004. *CRYPTOGRAPHIC ALGORITHMS FOR* UMTS. Finlandia.

[12] Pütz Stefan, Roland Schmitz, Tobias Martin.2001.*Security Mechanisms in UMTS*

[13] Wicaksono, Sulistyo Unggul , 2006. *Kajian Sistem Keamanan Jaringan CDMA*, Institut Teknologi Bandung. Bandung.

[14] Wikipedia. http://id.wikipedia.org/wiki/bruteforceattack

[15] Wikipedia. http://id.wikipedia.org/wiki/Kriptografi