APLIKASI ENKRIPSI MMS PADA PONSEL BERBASIS JAVA DENGAN MENGGUNAKAN ALGORITMA IDEA

Reza Dwi Noviawan[1], Yusuf Kurniawan[2], .[3]

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

Abstrak

Saat ini, Multimedia Messaging Service (MMS) sudah sering digunakan untuk berkomunikasi lewat ponsel. Pesan yang dikirimkan pun beragam, mulai dari teks, audio, image, hingga video. Pesan yang dikirimkan ada pula yang bersifat rahasia, padahal pesan tersebut bisa saja dibaca oleh orang yang tidak berhak.

Oleh karena itu, diperlukan adanya enkripsi agar pesan MMS dapat terjaga kerahasiaannya. Salah satu algoritma enkripsi yang terkenal dengan kehandalannya adalah International Data Encryption Algorithm (IDEA). Mode operasi enkripsi blok cipher yang digunakan adalah Cipher Block Chaining (CBC). Sedangkan untuk mengatasi keamanan dari sisi kunci, kunci di-hash-kan dengan fungsi hash MD5.

Pada tugas akhir ini, penulis membuat suatu aplikasi enkripsi MMS pada ponsel yang mendukung Java 2.0. Aplikasi enkripsi ini dianalisis dari waktu proses enkripsi dan dekripsi, ukuran pesan sebelum dan setelah enkripsi, memori yang terpakai pada proses enkripsi dan dekripsi, dan besar persentase avalanche effect.

Dari hasil percobaan, algoritma IDEA merupakan algoritma yang relatif kurang tepat untuk digunakan dalam proses enkripsi pada ponsel. Walaupun dilihat dari besar persentase avalanche effect yang dihasilkan memenuhi syarat sebagai algoritma yang baik, tetapi jika dilihat dari waktu yang digunakan untuk melakukan proses enkripsi dan dekripsi untuk pesan yang berukuran besar, seperti audio dan image, membutuhkan waktu yang lama.

Kata Kunci : MMS, enkripsi, IDEA, CBC, MD5, java

Abstract

Currently, the Multimedia Messaging Service (MMS) is often used to communicate via phone. The message sent was diverse, ranging from text, audio, image, until the video. The message that is sent there is secret, but the message can be read by people who are not eligible

Therefore, it is necessary to an MMS message encryption can be safe. One well-known encryption algorithm with reliability is the International Data Encryption Algorithm (IDEA). Operation mode block cipher encryption used is Cipher Block Chaining (CBC). Meanwhile, to overcome the security of the key, the key-hash of the MD5 hashes function

In this final task, the author makes an encryption application of MMS on the phone that supports Java 2.0. Encryption application is analyzed from time encryption and decryption process, the size of messages before and after encryption, the unused memory in the process of encryption and decryption, and a large percentage of the avalanche effect

From the results of the experiment, the algorithm is the IDEA algorithm is relatively less appropriate for use in the encryption process on the phone. Although viewed from a large percentage of the resulting avalanche effect qualifies as a good algorithm, but if viewed from the time used to perform encryption and decryption process for large messages, such as audio and image, take a long time

Keywords : MMS, encryption, IDEA, CBC, MD5, java

1. Pendahuluan

1.1 Latar belakang

Di era serba canggih dan mutakhir ini, teknologi informasi telah memasuki banyak aspek kehidupan. Dari aspek dalam dunia rumah tangga hingga dunia kerja, informasi dapat dikatakan sebagai kebutuhan penting yang datangnya bisa kapan saja dan darimana saja. Salah satu asal informasi tersebut adalah *mobile phones*, bisa berupa *ponsel*, PDA, atau PocketPC. Kehadiran ponsel tidak lepas dari adanya perkembangan teknologi informasi yang begitu cepat dan meluas. Keuntungan dari penggunaan teknologi informasi ini adalah dapat mempersingkat waktu dan biaya dalam penyampaian informasi yang notebene sangat berharga saat ini.

Salah satu teknologi informasi yang tertanam dalam ponsel adalah *Multimedia Messaging Service* (MMS). Pada suatu komunitas yang sangat aktif dan mementingkan pertukaran informasi dalam waktu yang singkat, MMS sangat dibutuhkan. Karena dengan MMS kita dapat mengirimkan pesan teks, gambar, suara, dan video dengan biaya yang relatif murah. Namun adakalanya MMS digunakan untuk mengirimkan data yang sifatnya rahasia, seperti nomor KTP, nomor rekening bank, password, foto rahasia, dan lain-lain. Akan tetapi dapatkah kita menjamin bahwa informasi yang kita sampaikan aman sampai tujuan. Otentifikasi dan *non-repudiation* dalam komunikasi MMS bisa didapatkan dengan mudah dari melihat pesan tersebut yang terdapat nomor pengirimnya.

Oleh karena itu, diperlukan suatu ilmu untuk memastikan bahwa pesan yang dikirim melalui MMS terjamin kerahasiaannya. Ilmu tersebut dinamakan dengan kriptografi, yaitu suatu bidang ilmu dan seni yang bertujuan untuk menjaga kerahasiaan suatu pesan yang berupa data-data dari akses oleh pihak lain yang tidak berhak sehingga tidak menimbulkan kerugian. Salah satu istilah dalam kriptografi adalah enkripsi, yaitu suatu cara untuk menjaga kerahasiaan suatu pesan dengan cara mengacak pesan sehingga pesan tersebut tidak dapat dikenali lagi. Seseorang hanya dapat melihat isi pesan asli (plainteks) apabila ia mempunyai kunci yang sesuai untuk mendekripsikannya.

Salah satu algoritma yang telah terbukti kehandalannya adalah algoritma IDEA (International Data Encryption Algorithm). IDEA adalah sebuah blok cipher yang didesain oleh James Massey dan Xuejia Lai dari ETH Zurich pada tahun 1992 dan mendukung panjang kunci 128 bit dan beroperasi pada blok plainteks 64 bit. Karena algoritma ini mempunyai panjang kunci 128 bit, maka algoritma ini tahan terhadap serangan *exhaustive key search*. Selain itu, algoritma ini pun menyediakan level keamanan tingkat tinggi yang lebih merahasiakan kunci daripada merahasiakan algoritmanya. Sehingga, algoritma IDEA dapat dengan bebas diterapkan dalam aplikasi selama aplikasi tersebut tidak memberikan keuntungan secara komersial. Hal ini dikarenakan nama IDEA dan algoritma IDEA telah mendapatkan hak paten di benua Eropa, Amerika, dan Jepang [11].

Sudah banyak sekali aplikasi enkripsi yang menggunakan algoritma IDEA karena hingga kini belum ditemukan cara pemecahan kode rahasianya. Tetapi

bagaimana menerapkan algoritma IDEA untuk aplikasi enkripsi MMS pada ponsel yang mempunyai jumlah memori yang terbatas. Untuk mengetahui performansi kecepatan IDEA dalam mengenkripsi dan mendekripsi pesan maka dilakukan pengukuran waktu yang dibutuhkan dalam melakukan proses enkripsi dan dekripsi dengan ukuran pesan (dalam bytes) yang beragam. Untuk mengetahui pengaruh proses enkripsi dan dekripsi terhadap penggunaan memori ponsel maka dilakukan pengukuran pemakaian memori ketika proses tersebut berlangsung. Sedangkan untuk mengetahui aman tidaknya algoritma IDEA dapat diketahui dengan menghitung persentase *avalanche effect*nya.

Saat ini sudah banyak ponsel yang mampu menjalankan aplikasi yang berbasis Java. Oleh karena itu, aplikasi ini akan dibangun dengan menggunakan teknologi Java. Selain karena bersifat *open source*, teknologi Java pun sudah terbukti kehandalannya.

1.2 Perumusan masalah

Berdasarkan latar belakang masalah yang dikemukakan di atas maka penulis merumuskan bahwa masalah-masalah yang akan diselesaikan dengan riset tugas akhir ini adalah sebagai berikut :

1. Bagaimana MMS yang dikirimkan dapat dienkripsikan dengan benar menggunakan algoritma IDEA sesuai dengan format MMS.
2. Bagaimana cara kinerja algoritma IDEA dalam mengenkripsikan teks, gambar, dan audio pada ponsel yang mendukung teknologi Java.
3. Bagaimana MMS yang telah dienkripsikan dapat didekripsikan sesuai dengan pesan asli.
4. Analisis yang dilakukan penulis melibatkan kecepatan enkripsi dan dekripsi, peningkatan ukuran pesan setelah enkripsi, penggunaan memori ketika menjalankan proses enkripsi dan dekripsi pada ponsel, dan besar persentase *avalanche* effect. Oleh karena itu, penulis merumuskan masalah seberapa cepat waktu yang dibutuhkan untuk mengenkripsi dan mendekripsi, seberapa besar peningkatan ukuran data pesan sesudah enkripsi dibanding dengan sebelum enkripsi, seberapa besar memori yang dibutuhkan ketika menjalankan aplikasi, serta seberapa acak keterikatan informasi antara plainteks dengan cipherteks dengan menghitung persentase *avalanche effect*.

Adapula beberapa batasan masalah sebagai berikut:

1. Masukan bagi perangkat lunak yang dirancang adalah teks, image dengan format jpg dan audio dengan format amr.
2. Algoritma kriptografi yang digunakan adalah algoritma private key dengan kunci simetrik yaitu algoritma IDEA mode operasi blok cipher CBC.
3. Fungsi *hash* yang digunakan adalah fungsi *hash* satu arah MD-5.
4. Spesifikasi mobile phone yang digunakan untuk perancangan adalah Samsung Star.
5. MMS yang dikirimkan dan diterima disimpan dalam database aplikasi atau *Record Management Store* (RMS).
6. MMS hanya dapat dikirimkan ke nomor ponsel, tidak dapat mengirimkan ke email.

7. Pengenkripsian dan pendekripsian hanya bisa dilakukan jika aplikasi sedang dijalankan pada ponsel.

1.3 Tujuan

Berdasarkan rumusan masalah penulis menetapkan tujuan riset tugas akhir ini adalah :

1. Membuat suatu aplikasi MMS pada ponsel yang dapat mengirim dan menerima pesan dalam bentuk teks, gambar dan audio dengan menggunakan algoritma IDEA
2. Menganalisis performansi dilihat dari waktu yang dibutuhkan untuk mengenkripsi dan mendekripsi pesan, ukuran data pesan sesudah enkripsi, pemakaian memori yang digunakan untuk melakukan proses enkripsi dan dekripsi, serta besarnya *avalanche effect*.

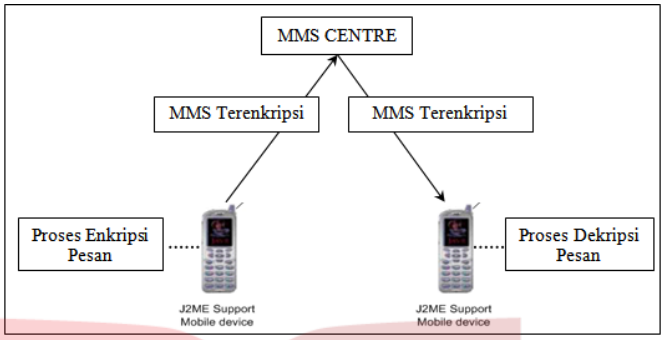
Hipotesa awal untuk penelitian riset tugas akhir ini adalah :

Waktu yang dibutuhkan untuk mendekripsi pesan MMS lebih lama dibandingkan dengan waktu untuk mengenkripsi. Adanya peningkatan ukuran pesan sesudah enkripsi dibandingkan sebelum enkripsi. Algoritma IDEA mampu memenuhi syarat *avalanche effect* yang baik.

1.4 Metodologi penyelesaian masalah

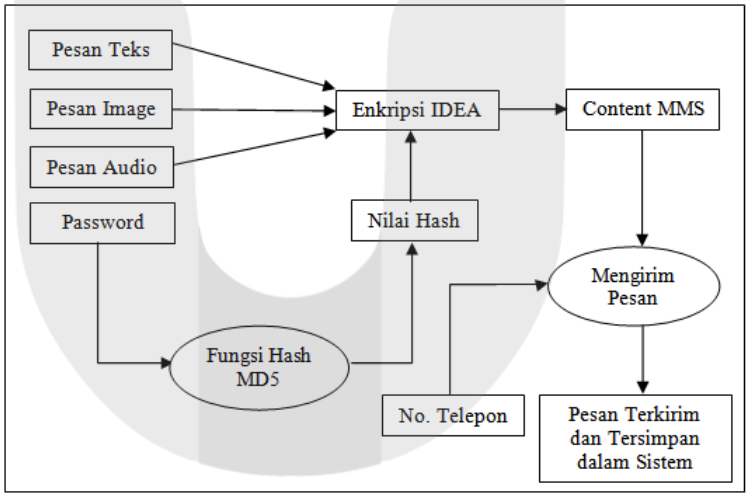
Metodologi penyelesaian masalah yang digunakan dalam penelitian tugas akhir ini adalah:

1. Studi literatur
   - Pencarian referensi
     Mencari referensi dari sumber-sumber yang layak. Seperti informasi-informasi yang tersedia di internet yang berhubungan dengan materi dari kriptografi, algoritma IDEA, MMS, JavaME, dan JavaSE.
   - Pendalaman materi
     Mendalami materi kriptografi, algoritma IDEA, MMS, JavaME, dan JavaSE yang dijadikan referensi.
2. Analisis kebutuhan sistem
   Tahapan ini meliputi analisis kebutuhan dari sistem perangkat lunak yang akan dibangun, yaitu menganalisis permasalahan pembangunan aplikasi kriptografi dengan menggunakan algoritma IDEA pada teknologi MMS yang akan diimplementasikan pada ponsel yang support Java.
3. Perancangan
   Sistem yang akan dibangun akan melibatkan dua buah ponsel yang berperan sebagai alat untuk mengirim dan menerima pesan. Pesan yang akan dikirim akan dienkripsi terlebih dahulu kemudian melalui MMS Center akan diterima di ponsel penerima. Pesan yang diterima masih dalam keadaan terenkripsi. Di ponsel penerima inilah pesan tersebut akan didekripsi menjadi pesan asli.



Gambar 1-1: Arsitektur Umum Sistem

Dalam mengirim MMS, user akan diminta untuk memasukkan nomor tujuan, pesan, dan password. Tipe media yang dapat dimasukkan ke dalam pesan yaitu teks, gambar, dan audio. Password tersebut akan dihashkan dengan menggunakan fungsi hash MD5 menjadi sebuah kunci algoritma IDEA yang berukuran 64 bit. Setelah pesan telah dienkripsi maka pesan selanjutnya akan dikirimkan ke nomor tujuan.



Gambar 1-2: Blok Diagram Mengirim MMS

4. Implementasi sistem
   Pada tahap ini akan dilakukan implementasi metode pada perangkat lunak sesuai dengan analisis perancangan yang telah dilakukan dengan menggunakan bahasa pemrograman Java.
5. Evaluasi
   Melakukan proses evaluasi terhadap hasil implementasi, apakah aplikasi yang telah dibuat dapat mendekripsikan pesan MMS sesuai dengan aslinya.
6. Analisis hasil implementasi
   Melakukan proses analisis terhadap hasil implementasi, yaitu dengan melakukan analisis terhadap hasil pengukuran performansi dan *avalanche effect*.
7. Penyusunan laporan tugas akhir
   Penyusunan hasil laporan terhadap penelitian yang telah dilakukan, dan membuat kesimpulan dari hasil penelitian tersebut.

persentase masih berkisar 45-60%, akan sulit untuk menemukan kejadian seperti disebutkan di atas untuk beberapa kali percobaan yang dilakukan.

Kesimpulan dan Saran

5.1 Kesimpulan

1. Algoritma IDEA kurang tepat jika digunakan dalam proses enkripsi-dekripsi pesan pada ponsel. Hal ini dikarenakan waktu yang digunakan untuk melakukan proses enkripsi-dekripsi pesan berukuran besar, seperti gambar dan audio, membutuhkan waktu yang relatif lama.
2. IDEA merupakan algoritma pengenkripsian data yang kecepatan dekripsinya lebih lama dibandingkan kecepatan enkripsinya. Hal ini dikarenakan adanya peningkatan ukuran pesan dan tidak efisiennya program yang dibuat.
3. Ukuran pesan setelah enkripsi lebih besar daripada ukuran pesan sebelum enkripsi karena adanya penambahan bit *padding* dan juga 8 bytes Initial Vektor (IV).
4. Memori ponsel yang digunakan untuk proses enkripsi lebih besar dibandingkan dengan memori yang digunakan untuk proses dekripsi. Walau demikian, perbedaannya tidak terlalu signifikan.
5. Algoritma IDEA memenuhi syarat *avalanche effect* (AE) yang baik, dimana persentasenya mencapai 50,01% untuk perubahan 1 bit pada plainteks dan 49,95% untuk perubahan 1 bit pada key. Dengan terpenuhinya syarat AE, maka IDEA dapat dikatakan aman.

5.2 Saran

1. Untuk aplikasi enkripsi MMS selanjutnya diharapkan dapat mengimpor kontak yang dikehendaki, dan memberikan password untuk masing-masing kontak. Jadi, ketika akan mengirim pesan tidak perlu melakukan input password lagi karena sudah diinputkan sebelumnya.
2. Menambahkan menu ”Drafts” untuk menyimpan pesan yang belum sempat dikirim.
3. Program yang dibuat hendaknya memperhatikan keterbatasan-keterbatasan yang terdapat pada ponsel, sehingga program nantinya dapat berjalan lebih efisien dan optimal.

Referensi

[1] A. Menezes, P. Van Oorschot, S. Vanstone. 1996. "Handbook of Applied Cryptography". CRC Press: Kanada.

[2] Cobb, Chey. 2004. "Cryptography for Dummies". John Wiley & Sons.

[3] Forum Nokia. MIDP: Wireless Messaging API 2.0 Developer's Guide. http://www.forum.nokia.com/documentation/MIDP_Wireless_Messaging_API_2_0_Dev_Guide_v2_0_en.zip, didownload pada tanggal 28 Januari 2009.

[4] JSR 120 Expert Group. 2002. "Wireless Messaging Api (WMA) for Java™ 2 Micro Edition". http://docs.sun.com, didownload pada tanggal 28 Januari 2009.

[5] Knudsen, B. Jonathan. 1998. "Java Cryptography". O'Reilly.

[6] Kurniawan, Yusuf. 2007. "Kriptografi Keamanan Internet dan Jaringan Komunikasi". Informatika: Bandung.

[7] Munir, Rinaldi. 2006. "Kriptografi". Informatika: Bandung.

[8] Raharjo, Budi, Imam Heryanto, Arif haryono. 2007. "Tuntunan Pemrograman Java Untuk Handphone". Informatika : Bandung.

[9] Ralph, Daniel, Paul Graham. 2004. "MMS Technologies, Usage and Business Models". John Wiley & Son, Inc.

[10] Riggs, Roger, Antero Taivalsaari, 2003. "Programming Wireless Devices with the Java™ 2 Platform, Micro Edition, Second Edition". Addison Wesley.

[11] Rodiah. 2004. "Algoritma IDEA". http://www.gunadarma.ac.id, didownload pada tanggal 7 Juli 2008.

[12] Shalahudin, M.dan A. S., Rosa. 2006. "Pemrograman J2ME: Belajar Cepat Pemrograman Perangkat Telekomunikasi Mobile". Informatika: Bandung.

[13] Wobst, Reinhard, 2007. "Cryptology Unlocked". John Wiley & Son, Ltd: Inggris.

[14] Young Rhee, Man. 2003. "Internet Security, Cryptographic Principles,