IMPLEMENTASI ALGORITMA *ADVANCE ENCRYPTION STANDART* (AES) PADA KEAMANAN DATA TEKS DAN GAMBAR BERBASIS ANDROID

Dedy Armiady
Program Studi Teknik Informatika FIKOM Universitas Almuslim

ABSTRAK

Kriptografi adalah ilmu mengenai teknik enkripsi dimana "naskah asli" (plaintext) diacak menggunakan suatu kunci enkripsi menjadi "naskah acak yang sulit dibaca" (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Kriptografi adalah ilmu matematika yang berkaitan teknik enkripsi berupa"naskah asli" (plaintext) menggunakan kunci enkripsi "naskah sandi yang tidak bisa dibaca" (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. dengan transformasi keamanan data untuk membuat artinya tidak dapat dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Algoritma AES merupakan salah satudiantara banyak metode yang mempunyai keunggulan dalam melakukan enkripsi dan dekripsi, metode algoritma AES dengan melakukan 10 kali putaran dan jaringan Feistel serta menggunakan operasi subtitusi dan permutasi membuat tingkat pengacakan yang memiliki beberapa tahap putaran yaitu Byte Subtitution, Shipting Rows, Add Roundkey dan Inv Mix Columm. Ciphertextpesan yang dihasilkan dengan kriptografi ini mengalami pembengkakan data yang cukup besar yaitu antara 40% sampai 1200%. Semakin besar data plaintext maka pembengkakan data semakin besar pula.
Kata Kunci: Keamanan Data, Kriptografi, Aes, Android.

PENDAHULAAN

Komputer merupakan salah satu media keamanan dalam penyimpanan data teknologi jaringan komputer yang saat ini berkembang, memungkinkan satu komputer dapat terhubung dengan komputer lainnya di belahan dunia ini untuk saling berbagi data dan informasi, selain itu banyak pekerjaan yang dapat diselesaikan dengan cepat, akurat, dan efisien dengan komputer. Sejalan dengan perkembangan teknologi tersebut, semakin mengubah cara masyarakat dalam berkomunikasi, semenjak kehadiran internet pada kehidupan manusia, kontrol atas informasi bergerak dengan amat cepat, termasuk pula informasi-informasi yang harus mendapatkan "perhatian" khusus karena nilai informasi tersebut sangatlah penting. Dulu komunikasi jarak jauh misalnya saja, masih menggunakan cara yang konvensional, yaitu dengan cara saling mengirim surat, tetapi sekarang komunikasi jarak jauh dapat dilakukan dengan mudah dan cepat yaitu dengan adanya teknologi seperti *email*, SMS (*Short Messaging Service*), dan internet yang merupakan salah satu teknologi telekomunikasi yang paling banyak digunakan.

Di dalam dunia informasi, terdapat data-data yang tidak terlalu penting, jadi jika publik mengetahui data tersebut, pemilik data tidak terlalu dirugikan. Tetapi apabila pemilik data adalah pihak militer atau pihak pemerintah, keamanan dalam pertukaran informasi menjadi sangatlah penting karena data yang mereka kirim adalah data-data rahasia yang tidak boleh diketahui oleh publik.

Smart phone (Telepon Pintar), merupakan alat komunikasi yang umum digunakan oleh sebagian besar manusia di dunia saat ini. *Smart phone* juga menyediakan berbagai macam aplikasi yang dapat memudahkan penggunanya dalam berakselerasi menggunakan *smart phone* tersebut.

Berdasarkan uraian yang telah penulis bahas, maka dapat diangkat menjadi suatu pokok bahasan dengan judul "IMPLEMENTASIALGORITMA *Advance Encryption Standart* (AES) Pada keamanan data teks dan gambar berbasis android".

METODE PENELITIAN

Deskripsi Umum

Perancangan Aplikasi Kriptografi ini di rancang guna untuk dapat mengamankan data teks dan gambar dari ancaman orang-orang jahat yang tidak bertanggung jawab. Pengamanan gambar di lakukan dengan cara mengenkripsi, mengubah teks maupun gambar menjadi sesuatu yang tidak terlalu dimengerti oleh orang lain atau disandikan.

Enkripsi yaitu suatu proses pengamanan suatu data yang disembunyikan atau proses konversi data (*plaintext*) teks maupun gambar menjadi bentuk yang tidak dapat dibaca/dimengerti maupun tersandikan. Enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, namun, hanya organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi.

Analisis

Aplikasi Kriptografi ini digunakan untuk mengamankan data teks maupun gambar. Aplikasi Kriptografi ini akan mengenkripsi data teks maupun gambar yang akan diamankan menjadi *cipher text* dan Aplikasi Kriptografi ini juga akan mendeskripsi data teks maupun gambar berupa *cipher text* menjadi *plain text*. Dalam membangun Aplikasi Kriptografi ini, diperlukan batasan yang jelas sebagai tujuan utamanya agar tidak keluar dari rencana yang telah ditetapkan. Beberapa kebutuhan sistem yang akan didefinisikan antara lain:

1. Memiliki kemampuan untuk mengirimkan dan menerima data.
2. Memiliki kemampuan untuk mengenkripsi pesan dan memberikan header Kriptografi/gambar/teks pada pesan yang telah di enkripsi.
3. Memiliki kemampuan untuk mendekripsi data yang mengandung header Kriptografi/gambar/teks.
4. Menampilkan output berupa pesan asli yang telah di deskripsi.

Tidak semua telepon selular dapat menjalankan aplikasi Kriptografi ini.

Berikut spesifikasi dari telepon selular agar dapat menjalankan aplikasi Kriptografi ini:

1. Mempunyai Sistem Operasi Android *Kitkat* ke atas.
2. Mempunyai *Micro Edition-profile* MIDP 2.0.
3. Mempunyai *Micro Edition-configuration* CLDC 1.0.

Analisis Kebutuhan Perangkat Keras

Dalam menjalankan aplikasi Kriptografi ini diperlukan yaitu: 1 Unit Hp yang memiliki Sistem Operasi Android versi 5.0 ke bawah.

Analisis Kebutuhan Perangkat Lunak

Dalam membangun aplikasi Kriptografi ini diperlukan beberapa kebutuhan sistem perangkat lunak yaitu: Microsoft Windows, Eclipse Mars, ADT dan Java.

Perancangan Proses

Perancangan proses akan menjelaskan bagaimana sistem bekerja untuk mengolah data *input* menjadi data *output* dengan fungsi yang telah direncanakan. Sistem ini akan digunakan oleh 1 *user* yaitu *user* umum sebagai pengguna pada sebuah perangkat. Adapun rancangan prosesnya adalah: *Flowchart* Enkripsi dan Deskripsi Gambar Aes, *Flowchart* Enkripsi dan Deskripsi Teks Aes dan Tahapan Proses Enkripsi dan Deskripsi Aes.

HASIL DAN BAHASAN

Implementasi Sistem

Implementasi merupakan tahap akhir yang dilakukan setelah proses pengembangan perangkat lunak selesai dikerjakan. Implementasi dimaksudkan untuk pengujian ataupun penjelasan mengenai langkah-langkah yang dilakukan untuk mengaplikasikan sebuah sistem yang telah dibuat melalui tampilan dari aplikasi yang telah dijalankan. Agar proses implementasi dari perangkat lunak dapat bekerja secara sempurna, maka, terlebih dahulu perangkat lunak tersebut harus diuji untuk mengetahui kelemahan dan kesalahan yang ada untuk kemudian dievaluasi.

Tampilan Sistem

Tampilan sistem berupa aplikasi android yang diinstall pada smartphone android. Berikut ini tampilan-tampilan systemnya.

Tampilan Halaman *Encrypt* Gambar

Halaman *encrypt* gambar merupakan halaman awal yang ditampilkan ketika program pertama kali dijalankan. Pada halaman *encrypt* gambar tersebut terdapat 2 tab yaitu tab gambar dan tab text, tab gambar digunakan untuk *encrypt* gambar dan tab text digunakan untuk *encrypt*text. Hasil dari implementasi halaman utama, seperti diperlihatkan pada. gambar 1. berikut ini.

Gambar 1. Tampilan Halaman Utama

Untuk proses *encrypt* gambar, caranya dengan memilih tombol “Pilih Gambar” maka aplikasi akan menampilkan halaman pemilihan direktori di mana lokasi gambar berada. Tampilan tersebut seperti diperlihatkan gambar 2. berikut.

Gambar 2. Tampilan Halaman Pilih Gambar

PENUTUP

Simpulan

Dari hasil implementasi perangkat lunak yang telah dilakukan, dapat diambil beberapa kesimpulan antara lain:

1. Aplikasi enkripsi dan deskripsi kriptografi pada telepon genggam berbasis android dapat diimplementasikan.

2. *Cipher text* pesan yang dihasilkan dengan kriptografi ini mengalami pembengkakan data yang cukup besar yaitu antara 40% sampai 1200%. Semakin besar data *plain text* maka pembengkakan data semakin besar pula.

Saran-Saran

Saran yang dapat peneliti berikan setelah penelitian ini adalah sebagai berikut :

1. Agar dapat mengurangi pembengkakan data, maka dibutuhkan kompresi sebelum data dikirim.
2. Agar keamanan data dapat lebih ditingkatkan perlu diterapkan algoritma enkripsi kunci asimetris.

DAFTAR PUSTAKA

RickRogers, John Lombardo, ZigurdMednicks, Blake Meike. 2009. *ation Development.* Sebastopol: O'Reilly Media Inc.

Nazaruddin, Safaat H. 2011. *Pemograman Android Mobile SmartPhone dan Tablet Pc BerbasisAndroid*. Bandung.

Setiawan, Wawan dan Munir. 2006. *Pengantar Teknologi Informasi: Basis Data*. Bandung: Universitas Pendidikan Indonesia.

Yusuf kurniawan, 2004. Kriptografi Keamanan Internet dan Jaringan Komunikasi. Penerbit Informatika Bandung.

Munir, 2006. S*usunan alphabet,* Bandung: Universitas Pendidikan Indonesia.