

Aplikasi Enkripsi Pesan Teks Dengan Metode *Advanced Encryption Standard* Pada Ponsel Berbasis Android

Saefudin¹, Syamsudin²,

^{1,2} Program Studi Sistem Informasi Fakultas Teknologi Informasi

Universitas Serang Raya

¹saefudin12@gmail.com, ²Syamsudin@gmail.com

Abstrak - Android adalah salah satu sistem operasi ponsel pintar yang saat ini banyak digunakan oleh masyarakat luas, android memiliki berbagai fasilitas dan salah satu fasilitas yang paling banyak digunakan adalah fasilitas lama yaitu layanan pesan singkat atau sering kita sebut dengan istilah sms, namun dengan fasilitas sms yang ada saat ini, timbul pertanyaan mengenai keamanan informasi jika seseorang mengirim pesan yang bersifat rahasia melalui fasilitas sms, ditambah lagi pendistribusian informasi yang saat ini semakin rentan terhadap serangan dan gangguan.

Dengan melakukan enkripsi pada pesan teks sms, maka keamanan informasi dari pesan tersebut dapat ditingkatkan, dan dari berbagai teknik enkripsi, enkripsi AES (*Advanced Encryption Standard*) adalah teknik yang saat ini dianggap sebagai teknik enkripsi yang paling kuat. Dengan menggunakan teknik AES untuk mengenkripsi pesan maka pesan yang kita kirim tidak akan dapat dibaca oleh orang lain yang tidak berhak.

Kata Kunci : SMS, *Advanced Encryption Standard*, Enkripsi, Dekripsi.

I. PENDAHULUAN

Dewasa ini perkembangan Smartphone dan Tablet PC berbasis android telah berkembang sangat pesat, hal ini terbukti dari banyaknya vendor-vendor smartphone yang sudah memproduksi smartphone berbasis android. Antusiasnya vendor smartphone memproduksi smartphone berbasis android dikarenakan android adalah sistem operasi mobile yang open platform karena android sendiri adalah sistem operasi untuk perangkat mobile berbasis linux yang mencakup sistem operasi, middleware dan aplikasi.

Pemanfaatan SMS untuk mengirim pesan rahasia telah lebih dulu dikembangkan. Misalnya di Inggris sebuah perusahaan operator telepon selular, *stallium* UK, mengeluarkan layanan bernama "stealth text" yang dapat digunakan untuk mengirim pesan dengan aman, yaitu dengan cara menghapus pesan secara otomatis segera setelah 40 detik pesan dibaca atau yang dikenal dengan nama self-destruct text message. Ada juga pengamanan sms dengan menggunakan kriptografi sms yang memanfaatkan kunci untuk mendekripsikan sms yang telah di enkripsi.

Salah satu cara pengamanan dalam penyampaian informasi adalah dengan melakukan pengkodean terhadap informasi tersebut. Teknik pengkodean ini dikenal dengan nama kriptografi. Kriptografi merupakan seni dan ilmu untuk

menjaga kerahasiaan berita. Dan dalam teknik pengkodean dikenal dua istilah yaitu enkripsi dan dekripsi, enkripsi adalah proses dimana teks asli dirubah menjadi teks rahasia dengan menggunakan kata kunci dan algoritma tertentu, sedangkan dekripsi adalah proses dimana teks rahasia dirubah kembali menjadi teks asli dengan kata kunci dan algoritma yang sama dengan kata kunci dan algoritma yang digunakan pada proses enkripsi.

Tujuan penelitian ini untuk membuat sebuah aplikasi yang dapat mengamankan pesan teks dengan menggunakan algoritma kriptografi AES (*Advanced Encryption Standard*) sebagai teknik untuk menenkripsi data sehingga pertukaran data menjadi lebih aman.

II. METODE PENELITIAN

2.1 Android

Android adalah sistem operasi berbasis Linux yang digunakan untuk perangkat mobile seperti Mobile Phone (HP), Ipad ataupun PC Tablet. Android merupakan software berbasis kode komputer yang bisa didistribusikan secara terbuka (open source) sehingga programmer bisa membuat aplikasi baru didalamnya. Terdapat Android Market yang menyediakan ribuan aplikasi baik yg gratis maupun berbayar,

serta memiliki aplikasi native Google yang terintegrasi, seperti push email GMail, Google Maps, dan GoogleCalendar.

2.2 Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu kriptos dan graphia. Kriptos berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut temoniloginya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain.

2.3 Algoritma Kriptografi

Menurut Dony Ariyus dan Rum Andri (2011), Ditinjau dari asal-usul kata, algoritma mempunyai sejarah yang menarik, kata ini muncul di dalam kamus Webster. Sampai akhir tahun 1957 hanya ditemukan kata algorism yang mempunyai arti proses perhitungan dengan bahasa Arab. Algoritma berasal dari nama penulis buku Arab yang terkenal yaitu Abu Ja'far Muhammad ibnu Musa al-Khwarizmi (al-Khwarizmi dibaca oleh orang Barat menjadi algorism). Kata algorism lama-lama berubah menjadi algorithm.

2.4 ADT (Android Development Tools)

Android Development Tools (ADT) adalah plugin yang didesain untuk IDE Eclipse yang memberikan kita kemudahan dalam mengembangkan aplikasi Android dengan menggunakan IDE Eclipse. Dengan menggunakan ADT untuk Eclipse akan memudahkan kita dalam membuat aplikasi project Android, membuat GUI aplikasi, dan menambahkan komponen-komponen yang lainnya, begitu juga kita dapat melakukan running aplikasi menggunakan Android SDK melalui Eclipse. Dengan ADT juga kita dapat melakukan pembuatan package Android (.apk) yang digunakan untuk distribusi aplikasi Android yang kita rancang.

2.5 SMS (Short Message Service)

SMS (*Short Message Service*) Layanan pesan singkat atau surat masa singkat adalah sebuah layanan yang dilaksanakan dengan sebuah telepon genggam untuk mengirim atau menerima pesan-pesan pendek (Gupta, 2000).

2.6 Eclipse

Eclipse adalah sebuah IDE untuk mengembangkan perangkat lunak dan dapat dijalankan di semua platform (platform-independent). Berikut ini adalah sifat dari Eclipse:

1. Multi-platform Target sistem operasi Eclipse adalah Microsoft Windows, Linux, Solaris, AIX, HP-UX dan Mac OS X.
2. Multi-language Eclipse dikembangkan dengan bahasa pemrograman Java, akan tetapi Eclipse mendukung pengembangan aplikasi berbasis bahasa pemrograman lainnya, seperti C/C++, Cobol, Python, Perl, PHP, dan lain sebagainya.

3. Multi-role Selain sebagai IDE untuk pengembangan aplikasi, Eclipse pun bisa digunakan untuk aktivitas dalam siklus pengembangan perangkat lunak, seperti dokumentasi, tes perangkat lunak, pengembangan web, dan lain sebagainya.

2.7 Analisa Masalah

Pengembangan sistem pengamanan data SMS saat ini sangat dibutuhkan mengingat pendistribusian informasi yang saat ini rentan dengan serangan dan gangguan. Fasilitas SMS pada ponsel yang saat ini berfungsi untuk mengirim pesan yang bersifat plain text menimbulkan banyak pertanyaan mengenai keamanan data pesannya.

Pada penelitian ini, penulis melakukan penelitian guna membangun sebuah sistem pengamanan data SMS, baik SMS yang dikirim dan diterima agar tidak dapat dibaca oleh orang yang tidak berhak.

2.8 Analisa Kebutuhan Perangkat Keras (Hardware)

Pembuatan aplikasi dimulai dari perancangan, coding, sampai implementasi membutuhkan perangkat keras (hardware). Berikut daftar perangkat keras (hardware) yang digunakan untuk pembuatan aplikasi enkripsi pesan teks dengan metode advanced encryption standard pada ponsel berbasis Android ini.

Tabel 3.1 Spesifikasi hardware

Hardware	Spesifikasi
Processor	Intel Core 2 Quad Q8200 @ 2.33GHz
Mainboard	Motherboard Intel Socket LGA1155
Memory	Kingston DDR2 PC-6400 (2048 MB x 2)
Hardisk	Seagate Barracuda SATA2 160 GB
VGA	AMD Radeon HD4650, 512MB 64-Bit
Monitor	LG IPS236V (1920x1080)
Keyboard	Logitech K260
Mouse	Logitech M210

2.9 Analisa Kebutuhan Perangkat Lunak (Software)

Pembuatan aplikasi ini membutuhkan perangkat lunak (software) untuk pembuatan program dan pengimplementasiannya. Berikut daftar perangkat lunak (software) yang digunakan untuk pembuatan aplikasi enkripsi pesan teks dengan metode advanced encryption standard pada ponsel berbasis Android.

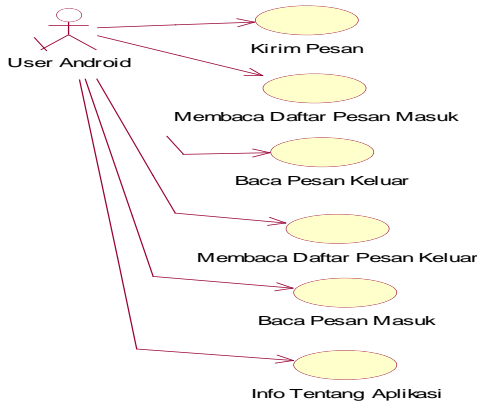
Tabel 3.2 Spesifikasi software

Software	Spesifikasi
Sistem Operasi	Windows 8 Enterprise v6.2 (Build 9200)
Design	Adobe Photoshop CS3
	CorelDRAW X6 (64-Bit) v16.1.0.843
UML	IBM Rational Rose v7.0.0.0
	The ObjectAid UML Explorer for Eclipse
Database	SQLite Database Browser v2.0b1
Eclipse	Android Developer Tools Build: v22.2.1-833290

JDK	Java Development Kit v7 Update 40
-----	-----------------------------------

2.10 PERANCANGAN

Untuk mengenal proses dari suatu sistem digunakan Use Case Diagram. Dengan Use Case Diagram ini dapat diketahui proses yang terjadi pada aplikasi enkripsi sms. Gambar use case diagram dapat dilihat pada gambar di bawah ini:



Gambar 3.1 Use Case Diagram

III. HASIL DAN PEMBAHASAN

3.1 Implementasi Sistem

Pembahasan dari perancangan implementasi yang telah penulis buat pada pemaparan sebelumnya dapat dilihat dalam bentuk screenshot di bawah ini:

3.2 Implementasi Main Menu

Main menu dirancang sebagai tampilan utama pada aplikasi enkripsi sms ini, Main menu berperan sebagai tampilan awal sekaligus pusat dari aplikasi sms enkripsi ini.



Gambar 4.1 Main menu

3.3 Implementasi Kirim Pesan

Tampilan kirim pesan merupakan tampilan saat user ingin mengirim pesan, berisikan kolom inputan nomor tujuan, isi pesan, kunci untuk enkripsi, keterangan panjang kunci dan kolom hasil enkripsi pesan, pada halaman ini akan muncul pilihan panjang kunci untuk enkripsi saat user menekan tombol pilihan pada ponsel.



Gambar 4.2 Kirim Pesan

3.4 Implementasi Daftar Pesan

Tampilan daftar pesan pada aplikasi enkripsi ini untuk daftar pesan masuk dan pesan keluar secara garis besar tampilannya sama, pada tampilan ini user dapat memilih pesan mana yang ingin user baca.



Gambar 4.3 Daftar Pesan

IV. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Kesimpulan yang didapat dari pembuatan aplikasi enkripsi pesan teks dengan metode advanced encryption standard pada ponsel berbasis android ini adalah sebagai berikut:

1. Aplikasi enkripsi pesan teks yang telah dibangun dapat berjalan pada ponsel dengan sistem operasi minimal gingerbread.
2. Pesan yang telah dienkripsi oleh aplikasi enkripsi ini dapat kembali didekripsi oleh aplikasi dengan proses enkripsi dan dekripsi yang cukup singkat.
3. Aplikasi enkripsi pesan teks yang telah dibangun berjalan dengan baik pada kedua sisi user.

4.2 Saran

Penulis ingin memberikan beberapa masukan untuk pengembangan aplikasi enkripsi pesan teks dengan metode advanced encryption standard pada ponsel berbasis android kedepannya, dengan harapan semakin semakin baiknya sistem menjadi lebih efisien dan bagus.

1. Pada form kirim pesan harusnya pesan yang diinput dapat dienkripsi lebih dari satu kali untuk tingkat keamanan yang lebih baik.
2. Pada form pesan masuk harusnya ada fitur untuk membalas pesan.
3. Aplikasi enkripsi pesan teks ini masih jauh dari sempurna. Untuk itu sistem ini dapat dikembangkan menjadi sistem yg jauh lebih baik lagi.

REFERENCES

- (1) Al-qdah, Majdi.Lin, Yi.(2012). *Simple Encryption/Decryption Application*. International Journal of Computer Science and Security.1 (1).
- (2) A.S, Rosa dan Salahudin,M, 2001. *Rekayasa Perangkat Lunak*. Bandung : Modula
- (3) Fajar,Dyah.(2012). *Android Programming Modul Indonesian Language*. http://www.academia.edu/1809022/Android_Programming_Modul_Indonesian_Language_.
- (4) Irawan.(2012). *Membuat Aplikasi Android Untuk Orang Awam*. Palembang: Maxikom.
- (5) Irawan.(2013). *Perancangan Aplikasi Sms (Short Message Service) Dengan Enkripsi Teks Menggunakan Algoritma Block Cipher Aes (Advanced Encryption Standard) Berbasis Mobile Pada Platform Android*, Jurnal Sistem Dan Teknologi Informasi.1(1).
- (6) National Institute of Standard and Technology (NIST).2001.Fips-pub 197, *Announcing the Advanced Encryption Standard (AES)*, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- (7) Veronica, Lusiana.(2011).Implementasi Kriptografi pada File Dokumen Menggunakan Algoritma Aes-128.Jurnal Dynamika Informatika.3(2).
- (8) Yuniata, Voni. Gani, Indriyanta, dan Antonius, Rachmat. (2009). Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jenis File. Jurnal Informatika.5(1).