

**APLIKASI METODA ENKRIPSI SUBSTITUSI
UNTUK *SHORT MESSAGE SERVICE*
MENGUNAKAN *JAVA2 MICRO EDITION***

TUGAS AKHIR

Diajukan sebagai salah satu syarat untuk mendapatkan gelar Ahli Madya
pada Jurusan Teknologi Informasi Program Studi Teknik Komputer

Oleh :

AYU LIDIA PUTRI
BP. 06092023



**PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK UNIVERSITAS ANDALAS
PADANG**

2009



ABSTRAK

APLIKASI METODA ENKRIPSI SUBSTITUSI UNTUK *SHORT MESSAGE SERVICE* MENGUNAKAN *JAVA2 MICRO EDITION*

Aplikasi SMSMIDlet merupakan sebuah aplikasi yang dirancang dengan menggunakan salah satu perangkat lunak *mobile* yaitu *Java2 Micro Edition* (J2ME).

Aplikasi ini digunakan untuk proses pengiriman dan penerimaan pesan singkat atau *Short Message Service* (SMS) dengan menggunakan teknik substitusi enkripsi dan dekripsi, sehingga tidak dapat dibaca oleh pihak lain. Algoritma yang digunakan adalah *vigenere cipher*.

Aplikasi ini telah diimplementasikan dengan melakukan uji coba pada perangkat ponsel jenis Sony Erricson dengan tipe yang berbeda.

Kata Kunci : SMS, enkripsi, dekripsi, dan J2ME

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring dengan kemajuan teknologi dewasa ini, bidang komunikasi menjadi aspek utama dalam perkembangan dunia Ilmu Pengetahuan dan Teknologi. Salah satunya adalah telepon selular (ponsel). Sejauh ini penggunaan ponsel tidak hanya terbatas untuk berbicara dan mengirim pesan saja, akan tetapi ponsel juga dapat berfungsi sebagai multimedia, *multiplayer games*, *transfer data*, *video streaming* dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponselpun bermunculan, diantaranya yang cukup dikenal luas adalah *Java 2 Micro Edition (J2ME)*.

J2ME adalah lingkungan pengembangan yang didesain untuk meletakkan perangkat lunak Java pada barang elektronik beserta perangkat pendukungnya. J2ME biasa digunakan pada ponsel, *pager*, *personal digital assistants (PDA's)* dan sejenisnya.

Salah satu fasilitas yang disediakan oleh ponsel adalah proses pengiriman data berupa pesan singkat, atau yang biasa disebut dengan *Short Message Service (SMS)*. Saat ini SMS sudah banyak digunakan oleh masyarakat sebagai alat komunikasi untuk menyampaikan informasi. Namun dengan kesederhanaan yang dimiliki oleh layanan SMS, timbul pertanyaan mengenai keamanan suatu informasi jika SMS digunakan untuk mengirim pesan rahasia yang tidak sembarang orang boleh mengetahui isi pesan tersebut. Memang biasanya SMS tidak digunakan untuk mengirim pesan yang bersifat rahasia. Namun, hal ini cukup disayangkan jika mengingat mudahnya penggunaan SMS.

Kini dengan memanfaatkan *Wireless Messaging API (WMA)* dari J2ME, para pembuat program Java dapat mengembangkan sendiri sebuah aplikasi pengiriman pesan singkat atau SMS yang dapat dimodifikasi untuk mengamankan pesan, salah satunya adalah dengan metode enkripsi kriptografi.

Enkripsi merupakan hal yang sangat penting dalam kriptografi yang merupakan proses mengamankan informasi dengan membuat informasi tersebut tidak dapat terbaca tanpa bantuan alat khusus. Sedangkan kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Berdasarkan jenis kunci yang digunakan untuk enkripsi dan dekripsi, algoritma kriptografi dapat dibedakan lagi menjadi dua yaitu : algoritma kriptografi simetris / *private key algorithm* dan algoritma kriptografi asimetris / *public key algorithm*. Pada sistem kriptografi kunci simetri, kunci untuk enkripsi sama dengan kunci untuk dekripsi. Jika kunci untuk enkripsi tidak sama dengan kunci untuk dekripsi, maka dinamakan sistem kriptografi asimetri.

Disebut sebagai algoritma simetris, karena dalam proses enkripsi dan dekripsinya menggunakan kunci yang sama. Algoritma enkripsi dan deskripsi bisa merupakan algoritma yang sudah umum diketahui, namun kunci yang dipakai harus terjaga kerahasiaanya, dan hanya diketahui oleh pihak pengirim dan penerima saja. Kunci ini disebut sebagai *private key*. Sebelum berkomunikasi kedua pihak harus bersepakat lebih dahulu tentang kunci yang dipergunakan.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan yang telah dilakukan pada bab-bab sebelumnya, maka dapat ditarik kesimpulan :

- a. Dengan memanfaatkan *Wireless Messaging System* dapat dikembangkan kemampuan aplikasi J2ME untuk proses pengiriman dan penerimaan pesan.
- b. Aplikasi SMSMIDlet ini disimulasikan dengan menjalankan dua *emulator* sekaligus, *emulator* pertama untuk proses pengiriman pesan dan *emulator* kedua untuk proses penerimaan pesan.
- c. Aplikasi SMSMIDlet ini merupakan aplikasi untuk mengamankan pesan. Untuk menjaga kerahasiaan dari pesan tersebut digunakan algoritma enkripsi, sehingga yang dapat membaca pesan tersebut, hanya penerima yang mengetahui kunci enkripsinya.

5.2 Saran

Sejauh pembahasan yang telah dilakukan oleh penulis mengenai tugas akhir ini, ada beberapa hal yang disarankan:

- a. Diharapkan untuk kedepannya, aplikasi ini dapat dikembangkan tepatnya pada penggunaan algoritma yang tingkat keamanannya lebih terjamin.

DAFTAR PUSTAKA

- Ariyus, Doni. **Kriptografi Keamanan Data dan Komunikasi**. Yogyakarta : Graha Ilmu, 2006.
- Ariyus, Doni. **Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi**. Yogyakarta: Andi Offset, 2008
- Purnama, Rangsang. **Pemrograman J2ME Tingkat Dasar**. Surabaya: Gitamedia Press, 2008.
- Sbalahuddin, M. **Pemrograman J2ME** . Bandung : Informatika, 2008.
- Supardi, Yuniar. **Pemrograman Handphone dengan J2ME**. Jakarta: Elex Media Komputindo, 2008.

