IMPLEMENTASI ALGORITMA CAESAR, CIPHER DISK, DAN SCYTALE PADA APLIKASI ENKRIPSI DAN DEKRIPSI PESAN SINGKAT, LumaSMS

Yusuf Triyuswoyo ST. [1]
Ferina Ferdianti ST. [2]
Donny Ajie Baskoro ST. [3]
Lia Ambarwati ST. [4]
Septiawan ST. [5]

[1,2,3,4,5] *Jurusan Manajemen Sistem Informasi, Universitas Gunadarma*
smti.2010@yahoo.co.id

Abstrak

Short Message Service (SMS) merupakan salah satu cara berkomunikasi yang banyak digunakan oleh pengguna telepon seluler. Namun banyaknya pengguna telepon seluler yang menggunakan layanan SMS, tidak diimbangi dengan faktor keamanan yang ada pada layanan tersebut. Banyak pengguna telepon seluler yang belum menyadari bahwa SMS tidak menjamin integritas dan keamanan pesan yang disampaikan. Ada beberapa risiko yang dapat mengancam keamanan pesan pada layanan SMS, diantaranya: SMS spoofing, SMS snooping, dan SMS interception. Untuk mengurangi risiko tersebut, maka dibutuhkan sebuah sistem keamanan pada layanan SMS yang mampu menjaga integritas dan keamanan isi pesan. Dimana tujuannya ialah untuk menutupi celah pada tingkat keamanan SMS. Salah satu penanggulangannya ialah dengan menerapkan algoritma kriptografi, yaitu kombinasi atas algoritma Cipher Disk, Caesar, dan Scytale pada pesan yang akan dikirim. Tujuan dari penulisan ini adalah membangun aplikasi LumaSMS, dengan menggunakan kombinasi ketiga algoritma kriptografi tersebut. Dengan adanya aplikasi ini diharapkan mampu mengurangi masalah keamanan dan integritas SMS.

Kata Kunci: *caesar, cipher disk, kriptografi, scytale, SMS.*

PENDAHULUAN

Telepon seluler merupakan salah satu hasil dari perkembangan teknologi komunikasi. Terdapat beberapa layanan komunikasi yang dapat digunakan pada telepon seluler, diantaranya: laynan telepon, *video call,* SMS, dan MMS. Short Message Service (SMS) atau pesan singkat merupakan fungsi komunikasi yang banyak digunakan oleh pengguna telepon seluler. Salah satu alasan layanan SMS menjadi salah satu layanan yang paling penting dan dibutuhkan dikarenakan SMS mudah digunakan dan biaya yang dikeluarkan untuk mengirim SMS relatif murah.

Namun banyaknya pengguna telepon seluler yang menggunakan layanan SMS ini tidak diimbangi dengan faktor keamanan yang ada pada layanan tersebut. Banyak pengguna telepon seluler yang belum menyadari bahwa SMS tidak menjamin integritas dan keamanan pesan yang disampaikan. Dalam berkomunikasi melalui SMS, pesan yang dikirim dapat dicuri informasinya oleh orang lain (Permana,

2014). Ada beberapa risiko yang dapat mengancam keamanan pesan pada layanan SMS, diantaranya: SMS *spoofing*, SMS *snooping*, dan SMS *interception* (Ardiyanto, 2011).

SMS *spoofing* merupakan pengiriman SMS di mana nomor pengirim yang tertera bukanlah nomor pengirim yang sebenarnya (Azannudin, 2013). Mekanisme SMS spoofing ini dimungkinkan karena lemahnya proteksi koneksi SMSC-*gateway* (Dwi, 2012). SMS *snooping* lebih sering terjadi karena kelalaian pengguna telepon seluler. Contohnya, ketika seseorang meminjamkan telepon selulernya pada orang lain, pada saat itu orang tersebut dengan sengaja atau tidak membuka isi pesan yang ada pada *inbox* SMS sehingga pesan yang seharusnya bersifat personal atau rahasia dapat dibaca dengan mudah oleh orang lain melalui cara ini. Sedangkan SMS *interception* merupakan pencurian data pesan SMS ketika pesan masih dalam transmisi dari pengirim ke penerima (Azannudin, 2013).

Untuk mengurangi risiko pada layanan SMS maka dibutuhkan sebuah sistem keamanan pada layanan SMS yang mampu menjaga integritas dan keamanan isi pesan. Enkripsi dan dekripsi pesan dapat digunakan sebagai faktor keamanan tambahan pada layanan SMS (Satyanegara, 2012). Dengan menerapkan algoritma kriptografi pada pesan yang dikirim, maka isi SMS menjadi sulit untuk dibaca karena telah dienkripsi sehingga hanya dapat dibaca dengan menggunakan kunci enkripsi. Tujuan dari penelitian ini adalah mengembangakan aplikasi enkripsi SMS berbasis Android. Dengan adanya aplikasi ini, pengguna dapat mengamankan isi pesan yang dikirim maupun yang diterima sehingga integritas pesan yang sifatnyanya personal atau rahasia dapat terjaga.

METODE PENELITIAN

Metode yang digunakan dalam membuat aplikasi LumaSMS adalah model *waterfall*, yaitu sebuah metode pengemebangan perangkat lunak yang bersifat sekuensial dan terdiri dari 5 tahap saling terkait. Adapun metode yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Analisis Kebutuhan

Penelitian dimulai dengan membaca beberapa buku mengenai algoritma kriptografi, diantaranya: algoritma Caesar, Cipher Disk, dan Scytale, serta beberapa referensi jurnal yang membahas mengenai penelitian-penelitian enkripsi SMS yang telah dilakukan sebelumnya. Selain itu juga dilakukan pencarian pustaka melalui sumber internet.

Aplikasi LumaSMS ini digunakan untuk mengirim dan menerima pesan melalui SMS. Pesan yang akan dikirimkan melalui SMS dienkripsi dahulu dengan menggunakan algoritma kriptografi klasik yang terdiri dari: algoritma Caesar, Cipher Disk, dan Scytale. Proses enkripsi dilakukan secara seri atau bertahap dan menghasilkan *chippertext*. Kemudian *chippertext* tersebut dikirimkan ke penerima melalui SMS. Untuk dapat membaca isi makna dari pesan tersebut penerima harus mendekripsi *chippertext* dengan kunci yang sama.

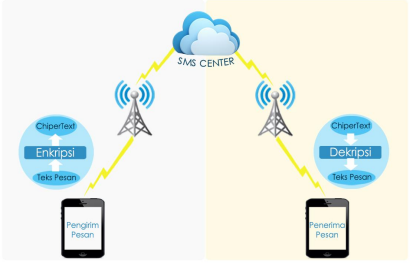
Dalam membangun aplikasi LumaSMS ini diperlukan batasan yang jelas agar aplikasi yang dibangun tidak keluar dari rencana awal. Berikut ini beberapa batasan dari aplikasi yang dibangun:

a. Proses enkripsi pesan dilakukan dengan mengkombinasikan 3 algoritma klasik, yaitu: Algoritma Cipher Disk, Caesar, dan Scytale

secara seri pada saat pesan dikirim oleh pengirim SMS.

b. Ketika pesan diterima oleh penerima SMS, pesan didekripsi dengan mengkombinasikan 3 algoritma yaitu: Algoritma Scytale, Caesar, dan Cipher Disk secara seri.
c. Aplikasi dapat berjalan pada telepon seluler atau tablet PC berbasis Android.
d. Jenis karakter yang dapat digunakan pada aplikasi LumaSMS ini dalam proses pengiriman pesan adalah angka 0 sampai dengan 9, huruf a sampai dengan z, dan simbol special karakter.
e. Jenis karakter yang digunakan tidak dibedakan berdasarkan huruf besar atau kecil (tidak case sensitive).
f. Format pesan yang diterima hanya menggunakan huruf kecil (lower case).

Cara kerja sistem ini akan dibagi ke dalam beberapa proses utama seperti yang ditunjukkan pada Gambar 1.



Gambar 1. Arsitektur Sistem

Dilihat dari gambar 1 di atas, dapat diketahui bahwa alur proses aplikasi yang ini cukup sederhana. Dimana pengirim pesan akan memasukkan isi pesan lalu aplikasi akan memroses enkripsi isi pesan tersebut ke dalam bentuk *chippertext*. Bentuk dari *chippertext* tersebut yang diterima oleh penerima pesan dan kemudian proses dekripsi dari isi pesan tersebut dilakukan pada aplikasi yang sama, agar isi pesan yang sebenarnya dapat dibaca oleh penerima pesan.

2. Perancangan Sistem

Perancangan sistem dilakukan dengan menggunakan diagram *flowchart*. Untuk proses enkripsi dapat dilihat pada gambar 2 dan untuk proses dekripsi dapat dilihat pada gambar 3.

Error! Not a valid link.
Gambar 2. *Flowchart* proses enkripsi

Error! Not a valid link.
Gambar 3. *Flowchart* proses dekripsi

3. Penulisan Kode Program

Penulisan barisan kode program untuk aplikasi LumaSMS menggunakan Eclipse, yaitu alat bantu yang digunakan untuk membuat aplikasi pada perangkat Android. Penulis juga menggunakan XML sebagai kode program untuk mengatur posisi antar muka pada perangkat Android.
Pada bagian penulisan baris program algoritma yang digunakan, yakni Caesar, Cipher Disk dan Scytale, menggunakan bahasa pemrograman Java.

4. Implementasi

Setelah melakukan perancangan sistem dan penulisan program maka dilakukan instalasi aplikasi pada perangkat telepon genggam berbasis Android untuk menguji apakah terdapat kesalahan atau tidak pada aplikasi yang telah dibuat.

HASIL DAN PEMBAHASAN

1. Skema Algoritma

Dalam penelitian ini, menggunakan 3 algoritma enkripsi dan dekripsi, yaitu: algoritma Caesar, Chiper Disk, dan Scitale. Ketiga algoritma ini disusun menjadi 3 tahapan algoritma secara seri, dengan logika yakni hasil dari enkripsi algoritma yang pertama menjadi masukan (*plaintext*) untuk algoritma yang kedua dan hasil dari algoritma

yang kedua menjadi masukan untuk algoritma yang ketiga. Hasil dari enkripsi ketiga inilah yang dikirimkan sebagai isi pesan singkat kepada penerima pesan. Berikut ini adalah penjelasan dari masing-masing algoritma yang digunakan, berdasarkan urutan tahapan enkripsi yang dilakukan.

1. Algoritma Caesar

Merupakan metode enkripsi paling pertama, ditemukan dan digunakan oleh Julius Caesar dan tentaranya pada saat terjadi perang Gaul di tahun 50 SM. Cara kerja dari algoritma ini, semua karakter alfabet digeser sebanyak n-karakter. Contohnya:

Untuk pergeseran n = 1, maka :

abcdefghijklmnopqrstuvwxyz

Akan bergeser menjadi :

BCDEFGHIJKLMNOPQRSTUVWXYZA

Untuk pergeseran n = 5, maka :

abcdefghijklmnopqrstuvwxyz

Akan bergeser menjadi :

FGHIJKLMNOPQRSTUVWXYZABCDE

Jumlah pergeseran n-karakter harus diketahui oleh pengirim dan juga penerima pesan tersebut.

2. Algoritma Cipher Disk (Vigenere)

Pengembangan dari algoritma Ceasar ialah algoritma Cipher Disk yang menggunakan disk sebagai media enkripsi dan dekripsi, dan juga dikenal sebagai Vigenere yang sama seperti Cipher Disk namun menggunakan tabel. Algoritma ini diciptakan pada abad ke-17, oleh Giovan Battista Bellaso.

Logika dari algoritma ini mengikuti algoritma Ceasar untuk perpindahannya, tetapi menggunakan sebuah kunci yang merupakan gabungan alfabet untuk menentukan n-karakter pergeserannya. Contohnya adalah sebagai berikut :

Diasumsikan kuncinya adalah "***CHARLIE***" dan isi pesannya adalah "***tutorials at dic***", maka dituliskan proses enkripsinya sebagai berikut:

CHARLIECHARLIECH

tutorials at dic

Maka logika proses enkripsi sebagai berikut:

- untuk huruf pertama digeser sejauh karakter C, maka karakter T pada pesan akan berganti menjadi V.
- untuk huruf pertama digeser sejauh karakter H, maka karakter U pada pesan akan berganti menjadi A.
- untuk huruf pertama digeser sejauh karakter A, maka karakter T pada pesan akan tetap menjadi T.

dan seterusnya.

3. Algoritma Scytale

Merupakan salah satu algoritma tradisional, yang menggunakan media perkamen atau kain yang dililitkan ke sebuah batang atau stik kayu. Digunakan untuk mengirimkan pesan yang terenkripsi. Harus diketahui besarnya keliling dari batang atau stik kayu yang menjadi media penulisan untuk dijadikan acuan proses enkripsi. Proses enkripsi dimulai dengan melilitkan media tulis pada batang, dan kemudian menuliskan pesan asli baris demi baris secara mendatar. Ketika lilitan media tulis dilepaskan dari batang, maka akan didapatkan hasil enkripsi. Contohnya:

Isi pesan : *saya mahasiswa gunadarma*

Penulisan pada batang :

S A Y A M A H A
S I S W A G U N
A D A R M A X X

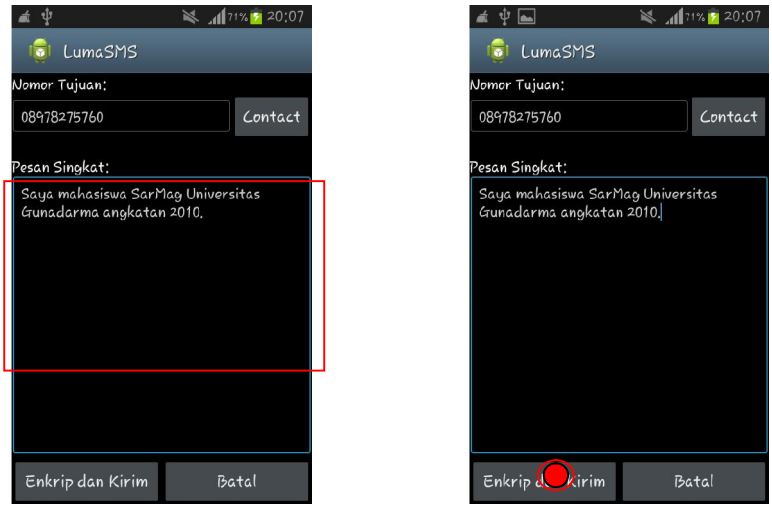
Hasil enkripsi menjadi :

SSAAIDYSAAWRMAMAGAHUXANX

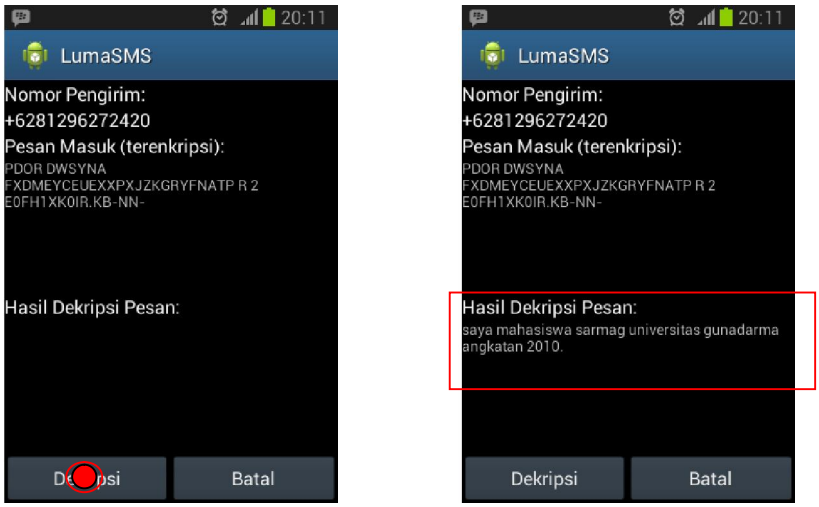
2. Penggunaan Aplikasi

Langkah pertama yang harus dilakukan pengguna untuk bisa

menggunakan aplikasi ini ialah melakukan proses instalasi. Selanjutnya, pengguna diharuskan untuk memasukkan nomor tujuan dan isi dari pesan yang akan dienkripsi lalu dikirim kepada penerima pesan. Lalu, pesan akan masuk ke dalam perangkat telepon penerima. Kemudian penerima pesan dapat melakukan proses dekripsi agar bisa mengetahui isi pesan sebenarnya. Untuk lebih jelasnya, dapat dilihat pada gambar di bawah ini.



Gambar 4. Proses enkripsi dan pengiriman pesan



Gambar 5. Proses penerimaan dan dekripsi pesan

SIMPULAN DAN SARAN

Aplikasi keamanan pesan singkat dengan menggunakan tiga algoritma kriptografi klasik, yaitu: Caesar, Cipher

Disk (Vigenere) dan Scytale telah berhasil dibuat dan hasil dari proses enkripsi dan dekripsi pesan singkat telah sesuai dengan hasil tahapan setiap algoritma apabila dilakukan pemrosesan secara manual. Dari hasil uji tes tingkat keamanan, aplikasi ini mampu melindungi tingkat kerahasiaan dari isi pesan singkat yang dikirimkan melalui jaringan operator seluler.

Berdasarkan hasil penelitian, aplikasi ini telah memenuhi kebutuhan awal dari penelitian, Namun untuk penelitian selanjutnya diharapkan adanya penambahan fitur seperti pemanggilan fungsi SMS manager, dimana pengguna dapat mengatur sesuka hati pesan masuk dan keluar. Dari ketiga algortima yang digunakan, diharapkan adanya pengembangan algoritma yang dapat lebih menyempurnakan aplikasi LumaSMS, khususnya dalam menghasilkan parameter-parameter dari masing-masing algoritma, dimana dalam kondisi saat ini kunci (*key*) dari masing-masing algoritma dihasilkan secara tetap pada baris kode program untuk menghindari adanya celah pada tingkat keamanan.

DAFTAR PUSTAKA

Ardiyanto 2011 *Implementasi Algoritma Kriptografi Caesar Cipher Pada Aplikasi SMS Telepon Seluler Berbasis J2ME* Teknik Informatika STIMIK AMIKOM Yogyakarta.

Azanuddin 2013 "Penyandian Short Message Service (SMS) Pada Telepon Seluler Dengan Menggunakan Algoritma Gronsfeld" Pelita Informatika Budo Darma, vol:IV, no:1.hal:47-59.

Dwi, Andi K P 2011 "Penerapan Algoritma Vigenere Cipher pada Aplikasi SMS Android" Makalah IF3058 Kriptografi.

Permana, Tatang F 2014 *Application Encryption and Decryption SMS (Short Message Service) Use RC6 Algorithm Based on Android Mobile Phone* Sistem Informasi Universitas Gunadarma Jakarta.

Satyanegara, Biyan 2012 "Penerapan Kriptografi dalam Sistem Keamanan SMS Banking" Makalah IF3058 Kriptografi.