PEMANFAATAN ALGORITMA CAESAR CIPHER DAN RC6 UNTUK PENGAMANAN SMS PADA SMARTPHONE BERBASIS ANDROID

Pipin Farida Ariyani[1)], Rifty Okky Darmawan Saputra[2)]

[1,2)]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
[1]pipin.faridaariyani@budiluhur.ac.id, [2]okky.saputra1092@gmail.com

ABSTRAK

Berbagai organisasi, perusahaan ataupun personal yang telah menggunakan teknologi dalam mengirim pesan perlu adanya keamanan dan kerahasiaan data. Hal ini juga menjadi masalah karena keamanan data yang bersifat penting dan rahasia masih rentan terhadap penyalahgunaan oleh pihak tertentu yang dapat menimbulkan kerugian yang sangat besar. Komunikasi melalu SMS masih menjadi pilihan dalam bertukar informasi. Hal ini dapat menjadi masalah bagi pengguna aplikasi SMS Android, khususnya bila aplikasi tersebut digunakan untuk berkomunikasi membahas kepentingan yang rahasia, dikarenakan pengamanan data SMS pada Android masih rentan terhadap penyadapan. Masalah semacam ini dapat dicegah dengan cara menggunakan metode enkripsi yang dimasukkan di proses pengiriman pesan pada aplikasi SMS. Dari sekian banyak metode enkripsi yang ada, algoritma enkripsi yang digunakan adalah caesar cipher dan RC6, sehingga pesan yang dikirimkan tidak akan tampil dalam bentuk sebenarnya dan perlu melakukan dekripsi agar pesan asli dapat terbaca oleh penerima. Pemilihan algoritma caesar cipher dan RC6 ini didasari karena algoritma enkripsi ini mudah dipelajari dan termasuk algoritma kandidat AES yang berarti sudah memiliki tingkat keamanan yang baik. Dengan demikian diharapkan pengguna aplikasi SMS Android dapat berkomunikasi dengan nyaman dan aman tanpa perlu kuatir isi pesan yang dikirimkan dapat disadap. Hasil akhir penelitian ini adalah aplikasi yang menampilkan isi pesan yang dibahas dan dikirim tidak akan dapat dimengerti oleh pihak lain selain penerima tujuan pesan.

Kata kunci: *SMS, Enkripsi, Caesar Cipher, RC6, Android*

I. PENDAHULUAN

Perkembangan teknologi komputer dan telekomunikasi saat ini telah mengalami pertumbuhan dan mengalami kemajuan yang sangat pesat dan menjadi suatu kebutuhan, karena banyak pekerjaan dapat diselesaikan dengan cepat, akurat, efisien dan aman. Salah satu dampak negatif dari perkembangan teknologi adalah banyaknya pencurian data, yang sangat ditakuti oleh sebagian besar pengguna mobile. Dengan adanya pencurian data maka aspek-aspek keamanan dan pertukaran informasi harus memiliki jalur transmisi yang aman khususnya dari penyadapan. Oleh karena itu pengguna mobile membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data SMS yang dikirimkan dan diterima. Dalam pemanfaatan teknologi maka kriptografi dapat digunakan untuk mengamankan pesan. Penerapan kriptografi pada penelitian ini difokuskan bagaimana algoritma yang diterapkan dapat mengamankan data SMS agar sampai kepada penerima pesan dengan aman.

Permasalahan yang timbul karena perkembangan teknologi dalam berkirim pesan dengan SMS melalui smartphone juga mendorong adanya kepentingan yang bisa merugikan pihak pengirim dan penerima SMS. Penyadapan SMS oleh beberapa pihak yang tidak bertanggung jawab bisa terjadi. Hal ini menyebabkan kurangnya privasi bagi pengirim dan penerima SMS jika data tidak terlindungi dengan enkripsi. Oleh karena itu timbul pertanyaan riset "Bagaimana mengamankan data SMS dari pencurian atau penyadapan oleh pihak lain yang tidak berhak?"

Berdasar dari pertanyaan riset tersebut, penelitian dilakukan bertujuan untuk merancang suatu aplikasi yang bisa mengamankan data SMS dari pencurian atau penyadapan oleh pihak lain yang tidak berhak. Aplikasi yang dirancang pada *smartphone* berbasis android mampu melakukan proses enkripsi dan deskripsi dengan algoritma Caesar Cipher dan RC6. Dengan aplikasi ini diharapkan data SMS berupa teks bisa dilindungi agar tidak bisa dibaca oleh pihak lain selain penerima pesan.

II. KRIPTOGRAFI

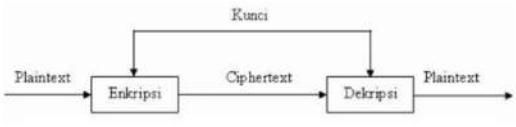
2.1. Pengertian Kriptografi

Kriptografi merupakan ilmu merumuskan metode yang memungkinkan informasi yang akan dikirimkan dibuat sedemikian rupa sehingga menjadi dalam kondisi atau bentuk yang aman, dan orang yang mampu mengambil informasi tersebut hanyalah penerima yang ditujukan informasi dikirimkan [1]. Pada kriptografi terdapat proses enkripsi dan deskripsi. Proses enkripsi yaitu suatu proses melakukan perubahan bentuk pesan dari yang bisa dimengerti menjadi tidak bisa dimengerti oleh manusia. Sedangkan proses dekripsi adalah suatu proses mengembalikan bentuk pesan

yang sudah terenkripsi kedalam bentuk aslinya sehingga dapat dimengerti kembali.

2.2. Algoritma Simetris

Algoritma ini disebut juga algoritma konvensional yaitu algoritma kriptografi simetris adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya [2]. Algoritma simetris dibagi menjadi 2 (dua) kategori yaitu, algoritma aliran (*Stream Cipher*) dan algoritma blok (*Block Cipher*). Pada algoritma aliran, proses penyandiannya bekerja pada satu *bit* atau *byte data*. Sementara algoritma blok, bekerja pada sekumpulan *bit* atau *byte data* (per blok) [3].



Gambar 1: Proses algoritma simetris

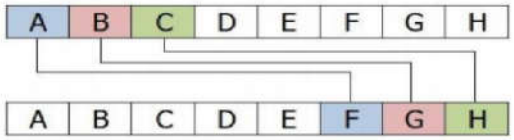
2.3. Algoritma Asimetris

Algoritma asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Pada algoritma ini menggunakan kunci umum (*public key*) dan kunci pribadi (*private key*). penggunaan kunci umum sebagai proses enkrip boleh saja diketahui oleh setiap orang, tetapi kunci pribadi sebagai proses dekrip hanya boleh diketahui oleh pihak yang berhak untuk mengetahui isi pesan tersebut [3]. Proses kriptografi algoritma asimetris dapat dilihat pada gambar berikut:

Gambar 2: Proses algoritma asimetris

2.4. Algoritma Caesar Cipher

Subtitusi kode yang pertama dalam dunia penyandian dikenal dengan kode Caesar, karena penyandian ini digunakan oleh Julius Caesar. *Caesar cipher* merupakan salah satu *cipher* subtitusi yang membentuk *cipher* dengan cara melakukan penukaran satu karakter diganti dengan karakter yang berada di sejumlah digit sebelah kanan atau kirinya, tergantung arah pergeserannya. Caesar cipher merupakan salah satu jenis cipher subtitusi yang membentuk cipher dengan cara melakukan pergeseran satu karakter tergantung angka pergeserannya. Teknik seperti ini disebut juga *cipher* abjad tunggal. *Caesar cipher* adalah dasar enkripsi yang sangat baik untuk dipahami sebelum membahas enkripsi lainnya yang lebih rumit. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter yang ada di *plaintext* dengan nilai pergeseran yang sama. Contohnya jika diketahui bahwa pergeseran sebanyak lima, maka huruf A akan digantikan oleh huruf F, huruf B akan digantikan dengan huruf G, dan seterusnya.[4]



Gambar 3: Pergeseran caesar cipher

2.5. Algoritma Rivest Code 6

Algoritma RC6 adalah algoritma yang menggunakan kunci simetris. Dirancang oleh Ronald Linn Rivest, Matt J.B Robshaw, Ray Sydney, dan Yuqin Lisa Yin dari laboratorium RSA. RC sendiri adalah singkaan dari "Rivest Code" sedangkan angka 6 (enam) berarti algoritma ini pengembangan dari algoritma sebelumnya, RC5. Letak perbedaan yang mendasar dari RC6 dari varian sebelumnya adalah langkah transformasi dan perbedaan banyak register. Register diperlukan untuk penempatan blok data yang diolah pada algoritma mengolah data pada tiap register yang ada. Algoritma RC5 membagi plaintext ke dalam 2 (dua) register, lain halnya dengan RC6 yang membagi plaintext ke dalam 4 (empat) register. Sedangkan algoritma RC4 adalah algoritma stream cipher bukanlah algoritma block cipher seperti RC5 dan RC6.[5]

III. ANALISIS DAN DESAIN

3.1. Analisis Masalah

Permasalahan yang dihadapi oleh pengguna SMS saat ini adalah kurang terjaminnya kerahasiaan sebuah pesan yang dikirimkan. Selama perjalan pesan dari pengirim ke penerima, SMS tersebut sangat rentan terhadap penyadapan pihak lain. Seseorang dapat membaca atau bahkan mengubah SMS yang dikirimkan pada saat SMS tersebut dalam perjalanan.

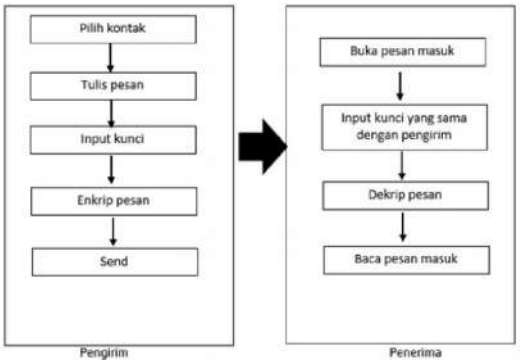
3.2. Penyelesaian Masalah

Untuk memecahkan masalah yang timbul, maka dibuatlah suatu aplikasi yang dapat melakukan proses enkripsi dan dekripsi SMS pada *smartphone* berbasis android, agar setiap SMS yang dikirimkan dapat terjaga kerahasiaan dan integritasnya. Pembuatan aplikasi ini diharapkan dapat menjadi solusi untuk menjaminnya kerahasiaan suatu pesan yang dikirimkan melalui media SMS.

3.3. Perancangan Aplikasi

Tahap perancangan aplikasi dilakukan untuk mencari bentuk yang optimal dari aplikasi yang akan dibuat dengan mempertimbangkan faktor permasalahan dan kebutuhan yang telah dijelaskan sebelumnya. Upaya yang dilakukan adalah dengan berusaha mencari kombinasi penggunaan teknologi hardware, dan software yang tepat sehingga didapatkan hasil yang optimal dan mudah untuk diimplementasikan. Berdasarkan analisis yang telah dilakukan, berikut ini akan

dibahas mengenai solusi perancangan pada aplikasi enkripsi SMS yang akan dibuat.



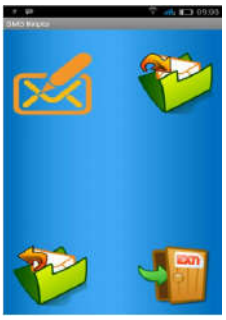
Gambar 4: Sistem yang diajukan untuk enkripsi SMS

3.4. Rancangan Layar

Rancangan layar yang akan dibangun terdiri dari beberapa modul *Form* yaitu *Form* menu utama, *Form* tulis pesan baru, *Form* pesan masuk, *Form* pesan keluar, *Form* list pesan.

a. Rancangan layar menu utama

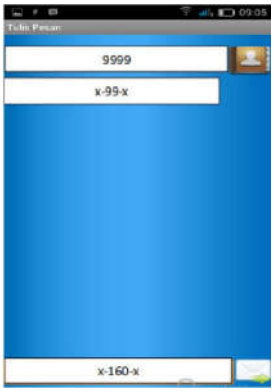
Menu utama merupakan tampikan awal pada aplikasi yang akan diterapkan. Pada rancangan layar menu utama terdapat beberapa *Form* menu seperti *Form* tulis pesan, *Form* pesan masuk, *Form* pesan keluar, dan keluar. Form menu utama ini merupakan modul utama yang menghubungkan ke modul-modul lainnya. Rancangan bisa dilihat pada gambar 5 (lima).



Gambar 5: Tampilan layar menu utama

b. Rancangan layar tulis pesan

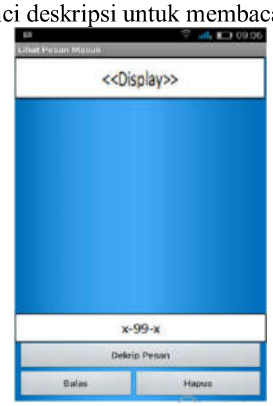
Rancangan layar pada gambar 6 (enam) di bawah ini menampilkan *Form* tulis pesan untuk menginput nomor tujuan, kunci enkripsi dan pesan yang akan dikirim. Pada form tulis pesan ini pengirim pesan bisa melakukan konfigurasi untuk mengirim SMS.



Gambar 6: Tampilan layar tulis pesan

c. Rancangan layar pesan masuk

Rancangan layar pada gambar 7 (tujuh) di bawah ini menampilkan isi pesan masuk ke *smartphone.* Pengguna bisa melihat dan membaca pesan yang telah diterima. Pesan yang diterima masih dalam bentuk cipher teks. Pengguna harus memasukkan kunci deskripsi untuk membaca SMS.



Gambar 7: Tampilan layar pesan masuk

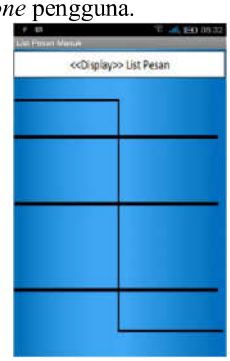
d. Rancangan layar pesan keluar

Rancangan layar ini menampilkan pesan yang telah terkirim dari *smartphone* pengguna. Pesan yang ditampilkan masih berupa teks cipher. Pengguna harus memasukkan kunci deskripsi untuk membaca SMS.

Gambar 8: Tampilan layar pesan keluar

e. Rancangan layar list pesan masuk

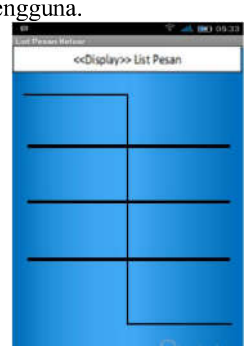
Rancangan layar ini menampilkan pesan-pesan yang masuk ke *smartphone* pengguna.



Gambar 9: Tampilan layar list pesan masuk

f. Rancangan layar list pesan keluar

Rancangan layar ini berisi list pesan-pesan yang pernah dikirimkan oleh pengguna.



Gambar 10: Tampilan layar list pesan keluar

IV. IMPLEMENTASI DESAIN

4.1. Kebutuhan Aplikasi

Sebelum memasuki tahapan pemasangan Aplikasi pada *Smartphone* yang akan dijadikan *server,* ada beberapa kebutuhan perangkat keras dan perangkat lunak yang harus dipenuhi untuk dapat menggunakan aplikasi tersebut.

a. Implementasi Kebutuhan Perangkat Keras

Sebelum memasuki tahapan pemasangan aplikasi pada *smartphone* android ada beberapa kebutuhan perangkat keras yang digunakan dalam pengembangan aplikasi enkripsi SMS menggunakan algoritma Caesar cipher dan RC6, yaitu:

1) Notebook
2) Prosesor: Intel(R) Core(TM) 2 Duo
3) Ram: 2084MB LPDDR2
4) LCD: 14" TFT LCD (1366 x 768)
5) Penyimpanan: 500GB
6) Mouse & Keyboard
7) Smartphone
8) Prosesor: MTK6592
9) Ram: 1024MB LPDDR3
10) LCD: 4.7" (1280 x 720)
11) Penyimpanan: 16GB
12) Android 4.4.2 Kitkat

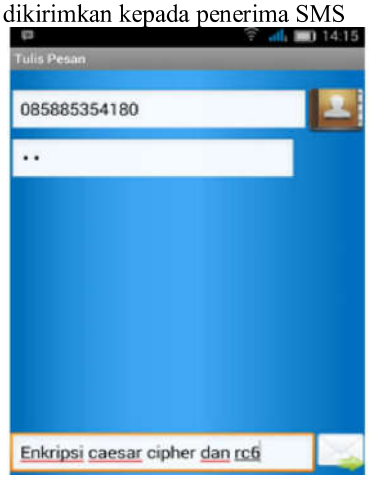
b. Implementasi Kebutuhan Perangkat Lunak

Perangkat lunak yang digunakan dalam pengembangan aplikasi enkripsi SMS menggunakan algoritma Caesar cipher dan RC6 pada *smartphone* android adalah sebagai berikut:

1) Microsoft Windows 7
2) Android Studio 1.1.0
3) Java Android
4) Microsoft Office Word 2010
5) Microsoft Paint
6) Android Virtual Device
7) Android Developer Tools
8) Android SDK
9) Red Koda

c. Implementasi Aplikasi

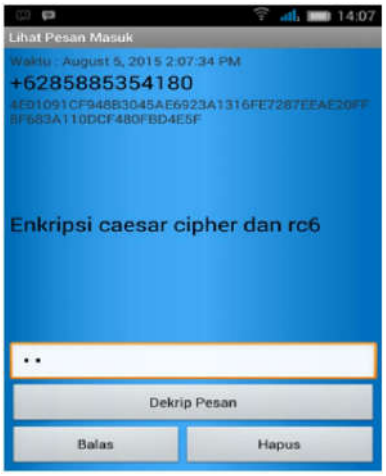
Gambar 11 adalah contoh pesan teks yang akan di enkripsi dan dikirimkan kepada penerima SMS



Gambar 11: Contoh pesan yang akan dienkripsi

Gambar 12: Contoh pesan yang sudah terenkripsi

Gambar 12 adalah pesan terenkripsi yang diterima oleh pengguna, untuk membaca isi pesan asli cukup memasukan kunci yang sama dengan kunci untuk enkripsi pesan seperti contoh pada gambar 13.



Gambar 13: Contoh pesan yang sudah terdekripsi

4.2. Uji Coba Aplikasi

Untuk melihat apakah aplikasi yang dirancang bisa memecahkan masalah yang terjadi, dilakukan uji coba aplikasi. Pengujicobaan dilakukan dengan membuat tabel enkripsi dan tabel deskripsi yang berisi data pada saat pemakaian SMS. Pada tabel ekripsi diperlihatkan data mengenai teks cipher yang dihasilkan dan pajang karakter hasil enkripsi. Pada tabel deskripsi diperlihatkan data mengenai teks plain pada pemakaian kunci yang benar dan salah. Dari uji coba, bisa digunakan untuk mengetahui kelebihan dan kekurangan aplikasi yang dirancang.

Table 1: Tabel hasil enkripsi

No	Plaintext	Ciphertext Caesar	Ciphertext RC6	Panjang Karakter Hasil Enkripsi
1	Budi luhur	Cvej Mvivs	F21FF05432ED7EFBCD8889A8DC8F43CB	32 Karakter
2	Ke kampus jam 11	Lf ibnqvt kbn 11	FE451A71231071F82370C561FF656CE4E2672E887BC73EB10C51D52F307D30FD	64 Karakter
3	Ini pesan rahasia	Joj qftbo sbibtjb	897B1E4E0633B469DD25B7FA0B643CF9D6D1F89F9E32F922C77E4E27191C8E90	64 Karakter
4	Kuncinya adalah GO	Lvodjozb bebmbi HP	F59CA5DCA7715CD054E28E9D16E927053F258727B500CE54C6B4A3D7D29D7B9	63 Karakter

Table 2: Tabel hasil dekripsi

No	Ciphertext	Hasil Dekripsi Bila Kunci Salah	Ciphertext Caesar	Plaintext
1	F21FF05432ED7EFBCD8889A8DC8F43CB	Ð♦#@Ð♦♦♦♦♦	Cvej Mvivs	Budi luhur
2	FE451A71231071F82370C561FF656CE4E2672E887BC73EB10C51D52F307D30FD	♦♦♦♦a0♦♦Ð♦♦	Lf ibnqvt kbn 11	Ke kampus jam 11
3	897B1E4E0633B469DD25B7FA0B643CF9D6D1F89F9E32F922C77E4E27191C8E90	@0@♦♦♦♦♦♦	Joj qftbo sbibtjb	Ini pesan rahasia
4	F59CA5DCA7715CD054E28E9D16E927053F258727B500CE54C6B4A3D7D29D7B9	♦♦♦♦0$Ŕ♦♦♦♦	Lvodjozb bebmbi HP	Kuncinya adalah GO

4.3. Kelebihan Aplikasi

a. Faktor keamanan pada pengiriman SMS dengan smartphone android lebih terjamin kerahasiaannya.
b. Aplikasi mudah untuk digunakan sama hal-nya seperti aplikasi pengirim SMS lainnya.
c. Enkripsi dengan kunci yang salah akan membuat pesan semakin tidak bisa terbaca.
d. Penggunaan dua buah algoritma menambah tingkat keamanan, karena pesan akan melalui dua tahap enkripsi.

4.4. Kekurangan Aplikasi

a. Semakin panjang isi pesan maka semakin panjang pula hasil enkripsinya.
b. Aplikasi tidak memiliki fitur untuk melakukan manajemen kunci, sehingga harus meng*input key* yang berbeda jika ingin berpesan.
c. SMS tidak terintegrasi dengan kontak, berbeda dengan aplikasi SMS default android.
d. Aplikasi belum bisa mengirim dan menerima file gambar ataupun audio (MMS) terenkripsi.

V. HASIL PEMBAHASAN

5.1. Kesimpulan

Setelah beberapa melewati tahap perancangan dan uji coba aplikasi enkripsi SMS dengan algoritma caesar cipher dan RC6, ada beberapa kesimpulan yang dapat diambil. Sehingga dalam penggunaan apliakasi ini diharapkan dapat membantu untuk memberikan solusi dari masalah yang ada dengan pertimbangan sebagai berikut:

a. Pengamanan pesan sangat diperlukan untuk menjaga kerahasiaan pesan.
b. Menggunakan dua buah algoritma menambah keamanan sistem kriptografi.
c. Panjang hasil enkripsi RC6 bisa lebih panjang dari teks aslinya.

5.2. Saran

Aplikasi enkripsi SMS ini masih jauh dari sempurna dan masih sangat diperlukan pengembangan dan bermacam perbaikan yang ditujukan untuk dapat memberikan kemudahan bagi penggunanya. Beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut dengan beberapa perkembangan lagi, antara lain :

a. Aplikasi ini belum ada fitur untuk melakukan sharing kunci antar pengirim dan penerima, dan fitur ini diharapkan ada pada pengembangan selanjutnya.
b. Penambahan fitur *inbox* dan *outbox* menjadi satu yang terintegrasi dengan kontak, sehingga lebih memudahkan pengguna dalam mengirim dan menerima pesan.

Penambahan steganografi untuk mengirim dan menerima pesan gambar atau *audio* terenkripsi.

DAFTAR PUSTAKA

[1] Kromodimoeljo, Sentot, 2009. *Teori dan Aplikasi Kriptografi*. Penerbit SPK IT Consulting.
[2] Sadikin, Rafki, 2012. *Kriptografi untuk Keamanan Jaringan*. Penerbit Andi Publisher
[3] Munir, Rinaldi, 2006. *Kriptografi*. Penerbit Informatika.
[4] Fahrianto, F. et all, 2013. *Encrypted SMS Aplication on Android with Combination of Caesar Cipher and Vigenere Algorithm*, UIN Syarif Hidayatullah Jakarta.
[5] Dewi, Niluh Kadek Kurnia, 2013. *Implementasi Algoritma RC6 Untuk Proteksi File MP3*. Universitas Brawijaya.