***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

IMPLEMENTASI ALGORITMA RIVEST CODE 4 (RC4) UNTUK PENYANDIAN SMS PADA TELEPON SELULAR

Hafiz Irsyad [1] **, Akhsani Taqwiym** [2] **, Novan Wijaya** [3]

[1] Teknik Informatika, Universitas Multi Data Palembang, Jalan Rajawali No.14 Palembang
[2] Sistem Informasi, Universitas Multi Data Palembang, Jalan Rajawali No.14 Palembang
[3] Manajemen Informatika, Universitas Multi Data Palembang, Jalan Rajawali No.14 Palembang
email : hafizirsyad@mdp.ac.id [1], akhsani.taqwiym@mdp.ac.id [2], novan.wijaya*@mdp.ac.id [3]*

Abstrak

Komunikasi SMS merupakan fitur dari telepon selular yang user friendly, useful, sangat standar dan sangat mudah digunakan dan banyak orang yang menggunakan media tersebut sebagai mengirimkan informasi baik secara rahasia atau terbuka untuk umum. Kondisi seperti inilah yang dimanfaatkan oleh intruder untuk mengambil informasi secara illegal dengan menggunakan informasi tersebut. Ada banyak cara untuk melakukan proses pengamanan informasi yang kita kirimkan tersebut, diantaranya menggunakan teknik kriptografi. Algoritma RC4 merupakan algoritma kriptografi yang cukup sederhana dan tidak telalu rumit. Teknik kriptografi yang cocok diimplementasikan pada telepon selular adalah teknik kriptografi dengan algoritma kriptografi yang sederhana dan tidak terlalu rumit. Telepon selular pada umumnya tidak memiliki processor yang cepat layaknya komputer, sehingga untuk menerapkan teknik kriptografi diperlukan pemilihan yang tepat. SMS adalah suatu layanan yang memungkinkan pengguna telepon selular mengirim atau menerima pesan-pesan singkat dengan cepat dan dengan biaya yang relatif murah. Penelitian yang diharapkan mampu melakukan proses enkripsi dari inforamsi sehingga tidak bisa diakses secara illegal.

Kata Kunci :

Kriptografi, RC4, Telepon Seluler, Keamanan Informasi

Abstract

SMS communication is a feature of cellular phones that is user friendly, useful, very standard and very easy to use and many people use this media to send information either confidentially or openly to the public. Conditions like this are used by intruders to take information illegally by using that information. There are many ways to carry out the process of securing the information that we send, including using cryptography techniques. The RC4 algorithm is a cryptographic algorithm that is quite simple and not too complicated. Cryptographic techniques that are suitable to be implemented on cellular phones are cryptographic techniques with simple and not too complicated cryptographic algorithms. Cellular phones in general do not have a fast processor like a computer, so to apply cryptographic techniques, proper selection is needed. SMS is a service that allows cellular phone users to send or receive short messages quickly and at a relatively low cost. The research is expected to be able to carry out the encryption process of information so that it cannot be accessed illegally.

Keywords :

Cryptography, RC4, Cell Phones, Information Security

1. PENDAHULUAN

Telepon selular adalah perangkat telekomunikasi elektronik yang memiliki kemampuan dasar yang sama dengan telepon *fixed line* konvensional, namun bersifat portable dan tidak perlu disambungkan ke jaringan telepon kabel karena menggunakan jaringan nirkabel. Pada dasarnya telepon selular berfungsi untuk melakukan panggilan dan menerima panggilan telepon, namun mengikuti perkembangan teknologi digital yang semakin pesat, kini telepon selular dilengkapi dengan berbagai pilihan fitur, seperti kamera digital, mp3 player, video, game, radio, televisi bahkan layanan internet (WAP, GPRS, 3G, 4G dan 5G). Dari berbagai fitur yang tersedia pada telepon selular saat ini, media komunikasi pesan singkat atau yang lebih dikenal dengan SMS

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

(*Short Message Service*) merupakan fitur yang paling sering digunakan oleh pengguna telepon selular [1].

SMS adalah suatu layanan yang memungkinkan pengguna telepon selular mengirim atau menerima pesan-pesan singkat dengan cepat dan dengan biaya yang relatif murah. Media Komunikasi SMS merupakan fitur dari telepon selular yang *user friendly*, *useful*, sangat standar dan sangat mudah digunakan [2]. Sehingga tidak jarang para pengguna telepon selular menggunakan fitur SMS ini untuk mengirimkan suatu pesan yang bersifat rahasia, padahal jalur komunikasi ini masih cukup rawan karena terdapat celah-celah yang memungkinkan pesan teks diserang ketika proses pengiriman [3].

Secara garis besar proses pengiriman SMS adalah pesan dikirim dari telepon selular pengirim, kemudian pesan terlebih dahulu disimpan di pusat pesan atau yang lebih dikenal dengan SMSC (*Short Message Service Center*) dan kemudian diteruskan ke telepon selular tujuan [4]. Salah satu kelebihan dari SMS adalah ketika tujuan sibuk, pesan tetap dapat dikirimkan karena pesan akan disimpan di SMSC terlebih dahulu, dan ketika tujuan tidak dalam keadaan sibuk, maka pesan akan langsung dikirimkan ke tujuan dari SMSC. Namun ternyata kelebihan dari SMS ini menjadi celah yang dapat dimanfaatkan oleh para penyerang dengan leluasa, dengan tersimpannya suatu pesan teks di SMSC, para penyerang dapat melakukan penyusupan ke SMSC dan mendapatkan pesan yg diinginkan. Selain penyerangan ke SMSC, terdapat model serangan lain yang langsung menyerang frekuensi radio ketika pesan baru dikirimkan dari suatu telepon selular, serangan ini dikenal dengan *Radio Frequency Jamming* [5].

Banyaknya celah pada fitur SMS akan berdampak pada banyaknya resiko yang akan bermunculan, sehingga diperlukan penanggulangan untuk setidaknya mengurangi resiko tersebut. Ada beberapa kasus pencurian data yang sering terjadi, misalnya mengirimkan SMS ke nomor penerima secara acak dan memaksa penerima membuka *link* atau pesan yang diterima yang secara tidak langsung akan membuka data pribadi kita. Bahkan saat ini, modus pencurian data melalui sms bisa mencuri dompet digital yang kita punya didalam perangkat tersebut. Salah satu cara yang dapat dilakukan adalah dengan menerapkan teknik kriptografi pada pesan teks yang akan dikirimkan. Saat ini banyak bermunculan telepon selular dengan media penyimpanan yang relatif besar, hal ini memungkinkan implementasi teknik kriptografi dapat dilakukan [6]. Dengan terenkripsinya pesan teks yang dikirimkan, maka penyerang yang berhasil mendapatkan pesan teks akan kesulitan untuk mengetahui isi dari pesan teks tersebut.

Telepon selular pada umumnya tidak memiliki *processor* yang cepat layaknya komputer, sehingga untuk menerapkan teknik kriptografi diperlukan pemilihan yang tepat. Teknik kriptografi yang cocok diimplementasikan pada telepon selular adalah teknik kriptografi dengan algoritma kriptografi yang sederhana dan tidak terlalu rumit [7]. Algoritma RC4 merupakan algoritma kriptografi yang cukup sederhana dan tidak telalu rumit. Algoritma RC4 memiliki proses enkripsi dan dekripsi yang cukup sederhana karena hanya melibatkan beberapa operasi saja per *bytenya* [8].

Banyak penelitian yang telah dilakukan mengenai topik ini, diantaranya implementasi algoritma RC6 untuk enkripsi SMS [9] tetapi untuk saat ini penulis mencoba dengan metode yang berbeda sebagai enkripsi SMS pada telepon selular menggunakan RC4 sehingga menjadi sebuah pembeda penelitan pada teknik kriptografi yang digunakan. Penulis membatasi

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

penelitian ini dengan algoritma kriptografi *Stream Cipher* RC4 untuk penyendian SMS pada telepon selular.

2. METODE / ALGORITMA

2.1 Struktur SMS

Struktur SMS terdiri dari dua bagian, yaitu *header* dan *message body*. Pada bagian *header* sebuah pesan terdiri dari instruksi-instruksi kepada komponen-komponen yang bekerja dalam jaringan SMS, sehingga apabila terjadi kerusakan data pada bagian header ini akan mengakibatkan kegagalan pengiriman pesan. Enkripsi SMS akan dilakukan pada bagian *message body* saja, hal ini dilakukan untuk menghindari perubahan data pada *header* SMS yang dapat mengakibatkan kegagalan pengiriman pesan. Sebagai contoh, nomor tujuan merupakan bagian dari *header* SMS, apabila nomor tujuan ini dienkripsi maka nomor tujuan dapat berubah atau tidak dikenali, sehingga terjadi kegagalan pengiriman pesan atau pesan terkirim pada tujuan yang tidak diinginkan [2].

2.2 Layanan Kriptografi

Pada bab sebelumnya dijelaskan mengenai jenis-jenis layanan kriptografi yang terdiri dari kerahasiaan, integritas data, otentikasi dan nirpenyangkalan. Salah satu jenis layanan kriptografi yang digunakan adalah kerahasiaan (*privacy*). Penyandian SMS bertujuan untuk menjaga kerahasiaan pesan yang dikirimkan agar pesan hanya dapat diakses oleh pengguna yang berhak, dengan kata lain hanya pengguna yang memiliki otoritas atau kunci rahasia yang dapat membuka isi SMS yang telah disandi.

Layanan kriptografi lainnya yang digunakan adalah otentikasi (*Authentication*). Jenis otentikasi yang digunakan adalah jenis otentikasi entitas berupa keaslian pengirim dan penerima pesan. Untuk menerapkan layanan ini, pada perangkat lunak yang dibangun akan digunakan fasilitas *login*. Diharapkan dengan adanya fasilitas ini keaslian pengirim dan penerima pesan dapat terjaga, karena sistem hanya dapat dibuka oleh pengguna yang mengetahui password login [1].

2.3 Algoritma Kriptografi

Algoritma kriptografi yang digunakan untuk penyandian SMS adalah algoritma kriptografi dengan jenis *stream cipher*. Pemilihan algoritma kriptografi jenis *stream cipher* dikarenakan jenis ini secara umum lebih cepat dibandingkan *block cipher*, serta tepat diimplementasikan pada aplikasi telelomunikasi [10]. Selain relatif lebih cepat, algoritma kriptografi jenis *stream cipher* memiliki baris koding program yang lebih singkat dibandingkan algoritma kriptografi jenis *block cipher*. Penggunaan baris program yang sedikit berdampak pada penggunaan memori yang sedikit pula, dengan kata lain algoritma jenis *stream cipher* lebih hemat memori dibandingkan jenis lainnya. Hal ini sangat cocok dengan kondisi telepon selular yang memiliki *space memori* yang tidak terlalu besar.

Algoritma kriptografi jenis *stream cipher* diantaranya adalah algoritma A5, SEAL, RC4 dan HC-256. Algoritma-algoritma ini memiliki karakteristik, kelemahan dan kelebihan masing-masing apabila diimplementasikan pada telepon selular. Algoritma A5 merupakan algoritma kriptografi jenis stream cipher yang digunakan di Amerika dan Eropa untuk mengenkripsi telepon selular GSM (*Group Special Mobile*) [11]. algoritma ini dirancang agar lebih efisien

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

untuk hardware, sehingga implementasi pada *software* membuat kecepatan enkripsi menjadi agak lambat. Algoritma *stream cipher* lainnya adalah SEAL, algoritma ini sangat efisien untuk implementasi pada *software* [10]. Algoritma SEAL memproses kunci enkripsi dan deskripsi menggunakan suatu tabel kunci internal. Penggunaan tabel kunci internal ini untuk mempercepat proses enkripsi dan dekripsi. Algoritma SEAL tidak cocok dimplementasikan pada media yg memiliki memori terbatas, karena untuk menerapkan algoritma ini dibutuhkan space memori khusus untuk menyimpan tabel kunci internal.

Algoritma kriptografi *stream cipher* yang paling banyak digunakan untuk *software* adalah algoritma RC4. Algoritma ini merupakan algoritma yang cepat, sederhana dan memiliki baris koding program yang singkat sehingga hemat dalam penggunaan memori [11]. Dalam hal lisensi, algortima ini bukan merupakan perdagangan rahasia, sehingga siapapun dapat menggunakannya.

Berdasarkan uraian diatas, akan digunakan algortima RC4 untuk penyandian SMS pada telepon selular. Pemilihan algortima RC4 berdasarkan pertimbangan, diantaranya algoritma RC4 merupakan algoritma yang cocok untuk diimplementasikan pada software. Algortima RC4 merupakan *algoritma stream cipher* yang memiliki baris koding program yang relatif singkat, sehingga sederhana dan hemat dalam penggunaan memori. Hal ini sangat cocok dengan space memori pada telepon selular yang tidak terlalu besar. Dan algoritma RC4 merupakan algoritma yang bebas digunakan untuk tujuan produk non-komersil. Apabila digunakan pada produk yang bertujuan untuk komersilpun, harga lisensi dari algoritma RC4 relatif lebih murah dibandingkan algoritma lainnya [12].

2.4 Implementasi Algoritma RC4 Untuk Penyandian SMS

Implementasi algoritma RC4 tidak membutuhkan penanganan khusus, beberapa hal yang perlu diperhatikan dalam mengimplementasikan algoritma RC4 untuk penyandian SMS pada telepon selular adalah menghindari pemakaian memori yang berlebihan dan melakukan penyesuaian aplikasi SMS terhadap algoritma RC4.

Aplikasi yang dibangun merupakan aplikasi pengiriman dan penerimaan SMS yang tidak terintegrasi dengan aplikasi SMS standar. Aplikasi dibangun berdiri sendiri dengan pertimbangan aplikasi SMS standar tiap jenis telepon selular tidaklah sama, panjang sebuah karakter dapat beragam (7 bit, 8 bit atau 16 bit) dan kemampuan konkatinasi SMS tidak dimiliki oleh semua jenis telepon selular. Dalam penjelasan sebelumnya mengenai penggunaan nomor port pada suatu aplikasi SMS yang digunakan sebagai pengenal antara dua atau lebih aplikasi penerimaan SMS. Sehingga untuk membangun suatu aplikasi SMS yang berdiri sendiri, diperlukan nomor port yang berbeda dengan aplikasi SMS standar pada telepon selular. Nomor port yang digunakan pada aplikasi SMS yang akan dibangun tentunya adalah nomor-nomor port yang belum digunakan oleh aplikasi-aplikasi SMS standar pada telepon selular, hal ini dilakukan untuk menghindari *crash* antara kedua aplikasi.

Pembangunan aplikasi SMS yang berdiri sendiri mengakibatkan aplikasi SMS hanya dapat diterapkan pada telepon selular GSM. Namun apabila aplikasi yang dibangun tidak berdiri sendiri melainkan terintegrasi dengan aplikasi standar SMS pada telepon selular, maka kompabilitas aplikasi akan lebih terbatas karena harus menyesuaikan dengan kemampuan dari

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

aplikasi SMS standar tiap telepon selular. Atas dasar pertimbangan tersebut, aplikasi yang akan dibangun adalah aplikasi SMS untuk telepon selular GSM yang berdiri sendiri [4].

2.5 Dampak Perangkat Lunak Terhadap Sistem Telepon Selular

Perangkat lunak yang dibangun adalah perangkat lunak yang berdiri sendiri, oleh karena itu perangkat lunak tidak melakukan interaksi dengan aplikasi lainnya yang terdapat pada telepon selular. Pada dasarnya, sebuah telepon selular hanya memiliki satu saluran pengiriman SMS [13], oleh karena itu ketika perangkat lunak yang dibangun melakukan proses pengiriman SMS, maka aplikasi SMS lainnya tidak dapat melakukan proses pengiriman SMS, begitupun sebaliknya. Hal yang sama juga terjadi pada proses penerimaan SMS.

Perangkat lunak yang akan dibangun memiliki tempat penyimpanan sendiri, sehingga tidak akan mempengaruhi penyimpanan data yang digunakan aplikasi lain pada telepon selular. Selain itu perangkat lunak ini menempati sebuah *port*, adapun *port* yang akan digunakan adalah *port* yang jarang digunakan sehingga tidak menganggu *port* yang telah digunakan oleh aplikasi lainnya pada telepon selular.

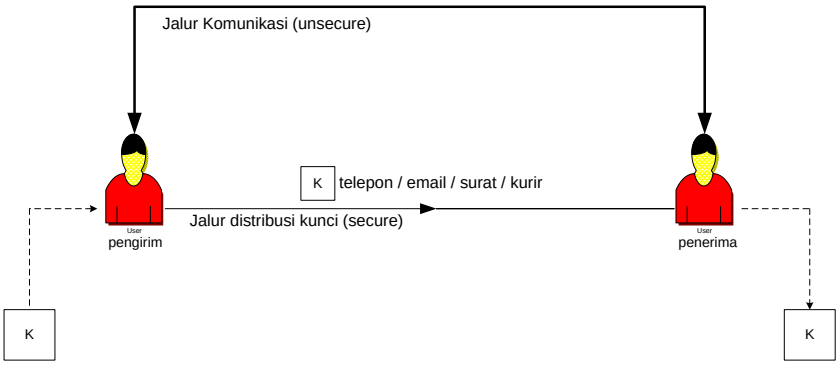
2.6 Perbandingan Terhadap Aplikasi SMS Standar

Perangkat lunak yang akan dibangun memilki kelebihan disisi keamanan dibandingkan dengan aplikasi SMS standar pada telepon selular. Namun perangkat lunak yang akan dibangun memilki kelemahan yaitu pesan yang dienskripsi akan cenderung membesar, sebuah pesan dapat berubah menjadi dua pesan setelah proses enkripsi.

2.7 Keamanan Pesan

Proses enkripsi pada aplikasi yang akan dibangun dilakukan sebelum proses pengiriman pesan, dengan kata lain pesan yang dikirimkan berupa *cipherteks* atau pesan yang telah disandikan. Enkripsi SMS sebelum pengiriman dapat mencegah serangan pasif dan menghindari jenis serangan aktif berupa *sniffing* [9]. Pesan SMS yang dikirimkan akan berhenti sesaat pada SMSC, pada saat inilah penyerang melakukan aksinya dengan "mengendus" isi dari pesan yang diburu. Namun dengan dienkripsinya pesan, kerahasiaan tetap terjaga karena tanpa kunci yang benar pesan tidak akan terbaca oleh penyerang.

2.8 Manajemen Kunci



Gambar 2.1 Skema Distribusi Kunci

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

Penyandian SMS pada perangkat lunak yang akan dibangun menggunakan algoritma RC4 yang merupakan algoritma kunci simetri. Kendala komunikasi menggunakan algoritma kunci simetri adalah rumitnya manajemen kunci, terutama pada jalur distribusi kunci. Kendala yang timbul adalah bagaimana mendistribusikan kunci yang digunakan pengirim pesan kepada penerima pesan. Distribusi kunci tidak dapat dilakukan pada saluran yang akan digunakan untuk komunikasi, pada kasus ini jalur komunikasi tersebut adalah jalur SMS. Sehingga dibutuhkan media khusus selain jalur SMS untuk distribusi kunci, seperti jalur telepon, surat, email atau kurir. Distribusi kunci pada perangkat lunak yang akan dibangun diilustrasikan pada Gambar 2.1.

Pada gambar 2.1 dijelaskan bahwa distribusi kunci dilakukan pada jalur selain jalur komunikasi (jalur SMS), yang berarti pendistribusian kunci tidak dilakukan pada sistem yang akan dibangun. Dengan kata lain pada perangkat lunak yang akan dibangun tidak tersedia fitur pengiriman kunci.

3. HASIL DAN PEMBAHASAN

3.1 Kebutuhan Sistem

Perangkat lunak yang akan dibangun adalah perangkat lunak yang mampu melakukan enkripsi terhadap pesan SMS sebelum proses pengiriman dan mampu mendekripsi pesan SMS yang diterima dari perangkat lunak sejenis. Selain itu, perangkat lunak ini harus dapat melakukan pengiriman dan penerimaan pesan yang terenkripsi maupun tidak terenkripsi. Perangkat lunak yang akan dibangun merupakan perangkat lunak yang digunakan sebagai alat komunikasi. Oleh karena itu, perangkat lunak akan ditanamkan pada pengirim dan penerima. Pengguna menggunakan *keypad* yang tersedia pada telepon selular sebagai piranti masukan. Sedangkan media interaksi antara pengguna dan perangkat lunak adalah *user interface* yang disediakan oleh perangkat lunak itu sendiri. Kemudian pesan yang telah diinputkan kirimkan melalui jaringan SMS. Secara umum, arsitektur global perangkat lunak dapat dilihat pada Gambar 3.1.

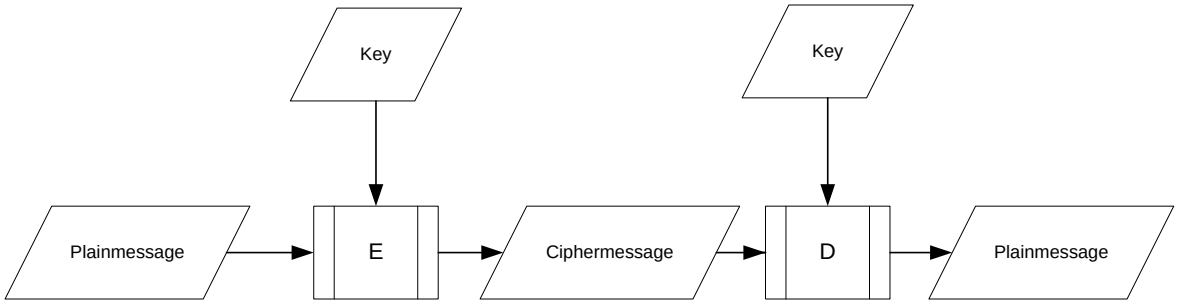
Gambar 3.1 Arsitektur Global Sistem

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

Data-data yang bekerja pada perangkat lunak yang akan dibangun, diantaranya adalah :

1. *Password Login* merupakan sandi yang yang digunakan pengguna untuk masuk ke sistem.
2. *Plain message* merupakan pesan SMS asli yang yang memiliki pengertian (makna).
3. *Cipher message* merupakan pesan SMS yang diacak atau disamarkan.
4. *Key* merupakan data yang digunakan untuk mentransformasi *plain message* ke *cipher message*, serta data yang digunakan untuk mendapatkan kembali *plain message* dari *cipher message*.

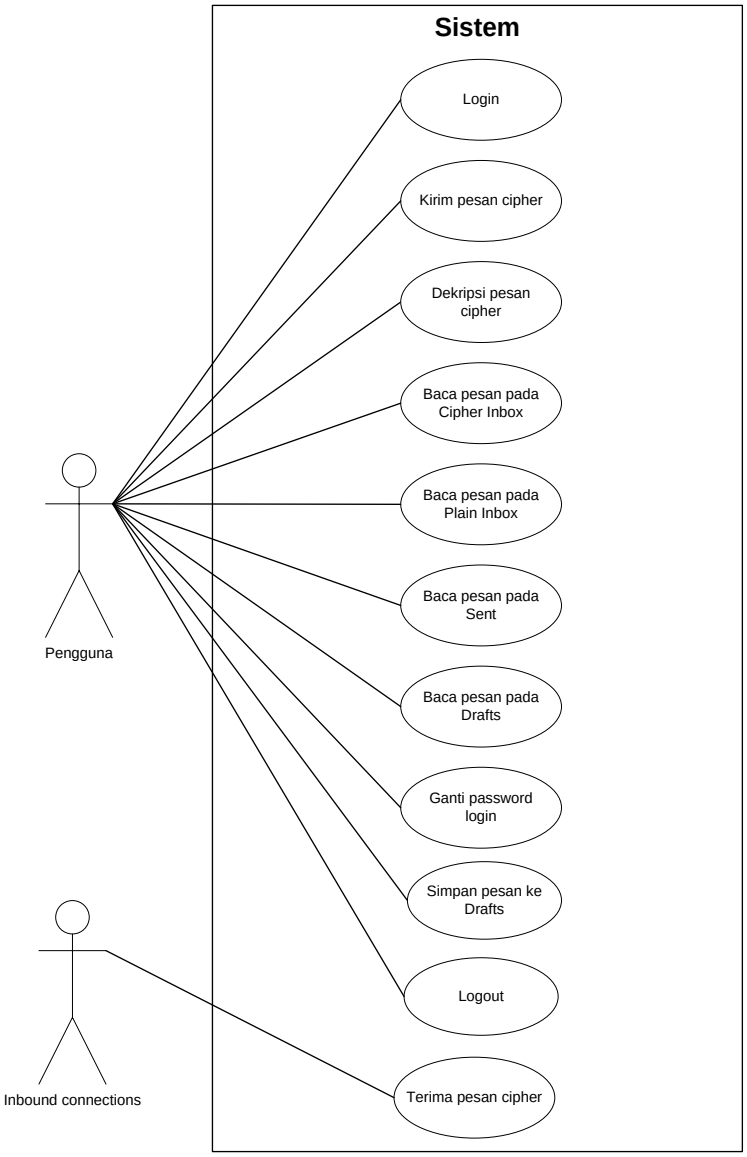
Data password login bekerja diluar proses penyandian SMS, data ini berfungsi sebagai alat otentikasi pengguna. Sedangkan tiga data berikutnya bekerja didalam proses penyandian SMS, bagaimana ketiga data tersebut bekerja dalam perangkat lunak yang akan dibangun, diilustrasikan dengan skema pada Gambar 3.2.



Gambar 3.2 Skema Kriptografi SMS

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

3.2 *Use Case*

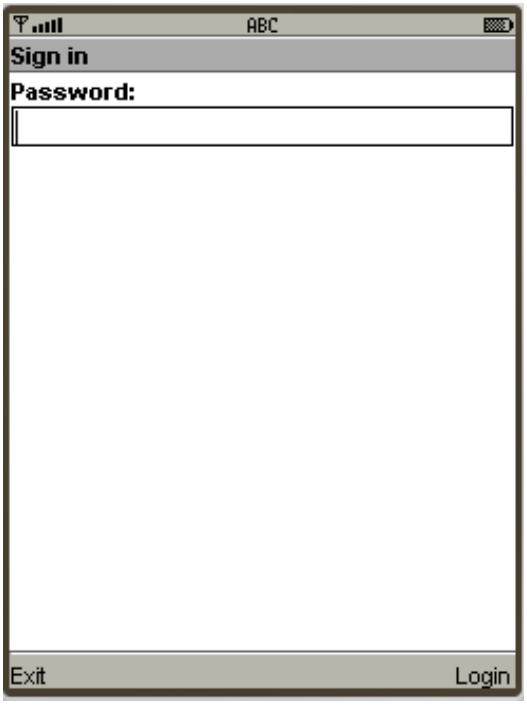


Gambar 3.3 Use Case

3.3 Perancangan Antar Muka

Rancangan antar muka dari perangkat lunak yang akan dibangun. Antar muka pertama yang tampil adalah antar muka yang berfungsi untuk mengotentikasi pengguna perangkat lunak, yaitu antar muka login. Adapun rancangannya tergambar pada gambar 3.4. Rancangan antar muka login.

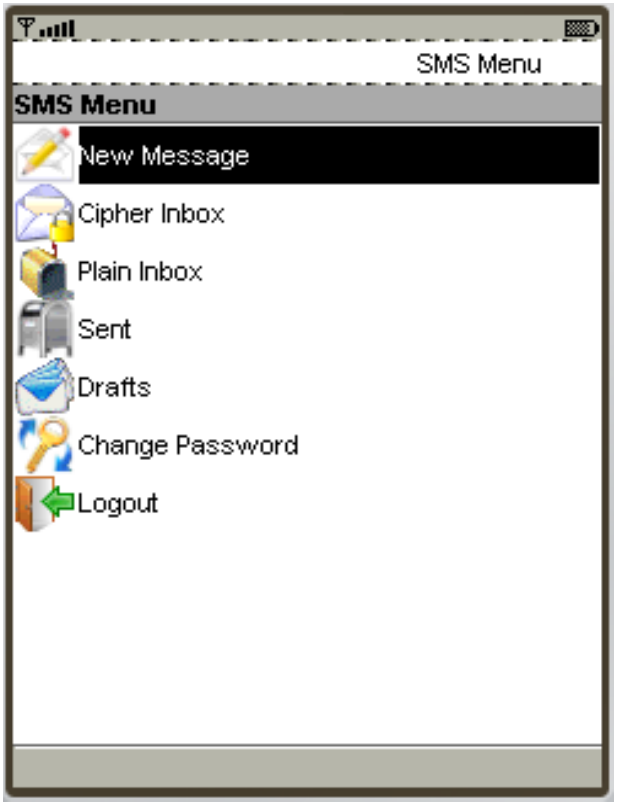
***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal



Gambar 3.4 Rancangan Antar Muka Login

Jika sukses melakukan proses otentikasi, maka antar muka yang tampil berikutnya adalah antar muka menu utama atau dapat disebut juga antar muka *home*. Antar muka menu utama berisi menu-menu atau fitur-fitur utama yang dimiliki oleh perangkat lunak seperti menu menulis pesan, membaca pesan yang diterima, membaca pesan hasil dekripsi, membaca pesan terkirim, membaca pesan yang disimpan, lalu menu mengganti password login serta menu logout. Rancangan dari antar muka menu utama tergambar pada gambar 3.5 rancangan antar muka menu utama:

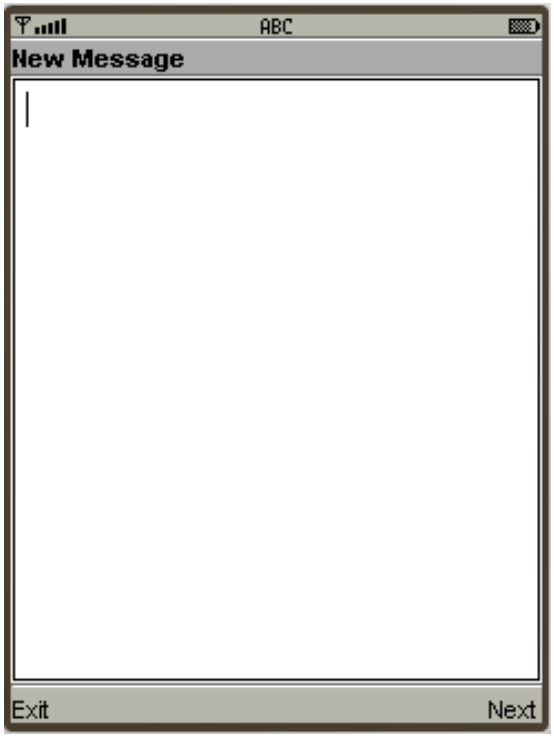
***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal



Gambar 3.5 Rancangan Antar Muka Menu Utama

Rancangan antar muka berikutnya adalah antar muka untuk menulis pesan, antar muka untuk menginput kunci enkripsi maupun dekripsi, antar muka yang menampilkan isi pesan yang diterima, didekripsi, terkirim maupun disimpan, dan antar muka untuk menginput nomor telepon tujuan pada saat pengiriman pesan. Rancangan-rancangan antar muka tersebut akan dirancang dengan pola atau *template* yang sama yaitu dengan pola *text box*, pola rancangan dari antar muka untuk menu-menu atau fitur-fitur tergambar pada gambar 3.6. Rancangan antar muka pola text box.

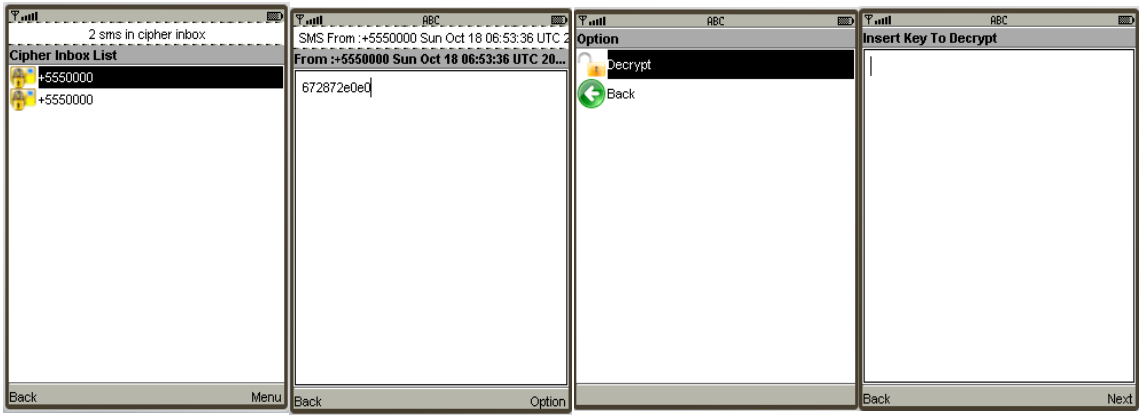
***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal



Gambar 3.6 Rancangan Antar Muka Pola Text Box

Rancangan antar muka selanjutnya adalah rancangan antar muka untuk menampilkan list SMS yang disimpan oleh perangkat lunak. Terdapat empat media penyimpanan SMS dalam perangkat lunak ini, yaitu *Cipher Inbox* untuk menyimpan pesan *cipher* yang diterima, lalu *Plain Inbox* untuk menyimpan pesan hasil dekripsi, kemudian *Sent* untuk menyimpan pesan terkirim, serta *Drafts* untuk menyimpan pesan tanpa mengirimkannya. Pesan-pesan pada *Cipher Inbox*, *Plain Inbox* dan *Sent* akan ditampilkan dengan pola yang sama, yaitu pola list nomor telepon. Adapun pola *list* nomor telepon yang dimaksud diilustrasikan dengan gambar 3.7.

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

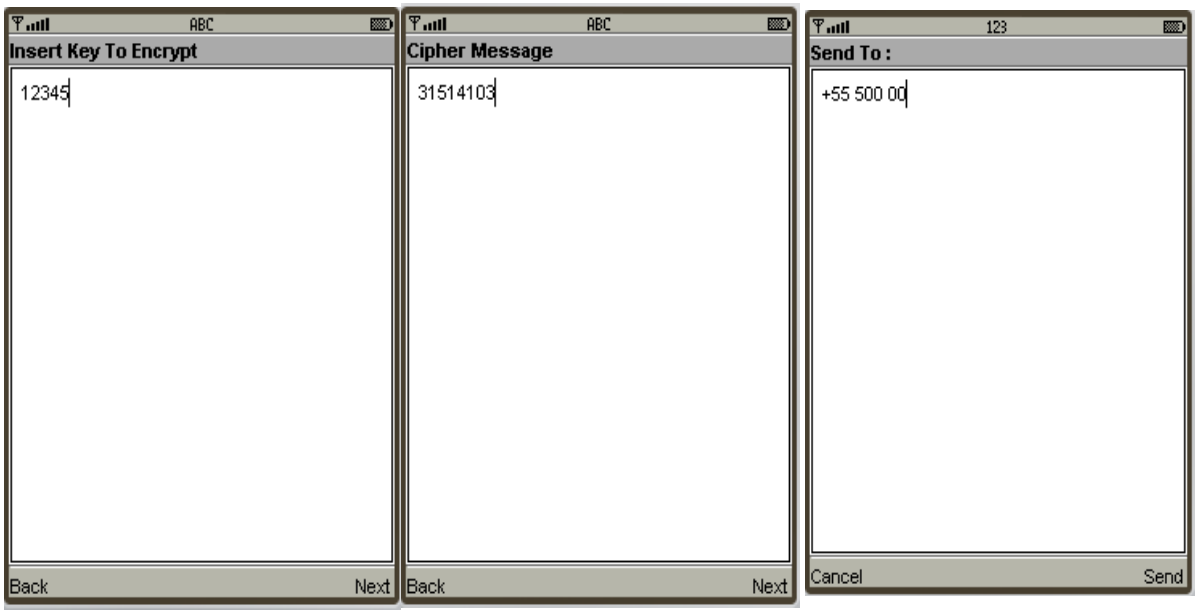


Gambar 3.7 Antar Muka Antar Muka List Cipher Inbox, Isi Pesan Pada Cipher Inbox, Menu Dekripsi, List Plain Inbox, dan Isi Pesan Pada Plain Inbox

Sedangkan untuk media penyimpanan *Drafts*, list yang ditampilkan berbeda dari ketiga media penyimpanan lainnya. Apabila *Cipher Inbox*, *Plain inbox* dan *Sent* menggunakan nomor telepon pada list yang ditampilkan pada anatr muka, maka pada *Drafts list* yang akan ditampilkan adalah list isi pesan bukan list nomor telepon. Hal ini dikarenakan pesan pada Drafts tidak menyimpan informasi mengenai nomor telepon, informasi yang disimpan hanya isi pesan.

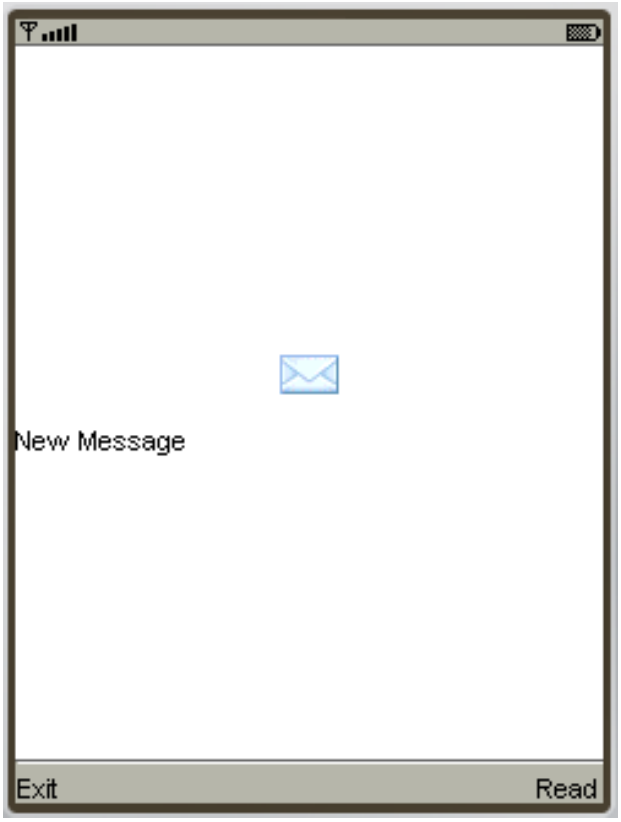
Rancangan antar muka berikutnya berupa tampilan dalam melakukan proses enkripsi data. Dimana akan melakukan proses *input* data enkripsi sehingga pesan yang dikirmkan bisa dibukan dan diterima di telepon seluler yang diminta.

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal



Gambar 3.8 Antar Muka Menu Enkripsi, Input Kunci Enkripsi, Hasil Enkripsi, dan Input Nomor Telepon

Rancangan antar muka berikutnya adalah rancangan antar muka terima pesan untuk pengguna dan rancangan antar muka mengganti *password login.* Rancangan antar muka tergambar pada gambar 3.9.



Gambar 3.9 Rancangan Antar Muka Terima Pesan

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

Gambar 3.10 Rancangan Antar Muka Ganti Password Login

4. KESIMPULAN

Algoritma RC4 dapat diimplementasikan pada telepon selular dengan spesifikasi MIDP 2.0 dan CLDC 1.1. Penyandian pesan SMS dengan algoritma RC4 membuat pesan yang dikirimkan menjadi lebih panjang, yaitu dua kali lipat dari pesan aslinya. Agar penelitian ini menjadi lebih baik dan untuk pengembangan lebih lanjut dari penelitian ini diantaranya, penggunaan algoritma kriptografi kunci asimetri untuk memperbaiki manajemen kunci pada sistem penyandian SMS yang telah dibangun menggunakan algoritma kriptografi kunci simetri, sehingga sistem kriptografi akan menjadi hybrid cryptosystem. Penambahan layanan kriptografi yang belum diterapkan pada penelitian ini, seperti otentikasi pesan, integritas data atau nir-penolakan.

5. REFERENSI

[1] S. Subhan, S. Amini, and P. F. Ariyani, "IMPLEMENTASI PENGAMANAN DATA ENKRIPSI SMS DENGAN ALGORITMA RC4 BERBASIS ANDROID," in *Prosiding SENIATI 2017*, 2017, pp. A29-1.

[2] A. Wicaksono, "LAYANAN REFERENSI MELALUI SMS: STUDI LITERATUR," *Media Pustak.*, vol. 24, no. 1, pp. 1–8, 2017, doi: 10.37014/medpus.v24i1.154.

[3] D. Adhar, "Implementasi Algoritma DES (Data Encryption Standard) Pada Enkripsi Dan Deskripsi SMS Berbasis Android," *JTIK (Jurnal Tek. Inform. Kaputama)*, vol. 3, no. 2, pp. 53–60, 2019.

[4] M. Pineng, "Analisa Performansi Pengiriman Short Message Service (SMS) Pada Jaringan CDMA," *J. Dyn. Saint*, vol. 3, no. 1, pp. 405–416, 2017, doi: 10.47178/dynamicsaint.v3i1.266.

[5] Z. Qin, J. Sun, B. Wahaballa, W. Zheng, H. Xiong, and Z. Qin, "A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing," *Comput. Stand. Interfaces*, vol. 54, no. 1, pp. 55–60, 2017, doi: 10.1016/j.csi.2016.11.012.

***e-issn :* 2615-6474**
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

[6] F. Fredianto, A. Kusyanti, and K. Amron, "Analisis Perbandingan Algoritma Advanced Encryption Standard Untuk Enkripsi Short Message Service (SMS) Pada Android," *urnal Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 10, pp. 4281–4289, 2018.

[7] R. Sahara, H. Prastiawan, and A. Rohman, "Implementasi Keamanan SMS Dengan Algoritma RSA Pada Smartphone Android," *J. Ilm. FIFO*, vol. IX, no. 2, pp. 112–118, 2017.

[8] M. Diana and T. Zebua, "OPTIMALISASI BEAUFORT CIPHER MENGGUNAKAN PEMBANGKIT KUNCI RC4 DALAM PENYANDIAN SMS," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 2, no. 1, pp. 12–22, 2018, doi: 10.30645/j-sakti.v2i1.52.

[9] K. M. A. Hakim, "RANCANG BANGUN APLIKASI ENKRIPSI-DEKRIPSI SMS PADA ANDROID DENGAN METODE RC6," *J. Tera*, vol. 1, no. 2, pp. 241–252, 2021.

[10] F. A. Syahputra, "SIMULASI PENGAMANAN TEXT DALAM PROSES ENKRIPSI DAN DESKRIPSI METODE VIGENERE CIPHER," *Kumpul. Karya Ilm. Mhs. Fak. sains dan Tekhnologi*, vol. 1, no. 1, pp. 176–176, 2019.

[11] D. Arius, *Komunikasi Data*. Yogyakarta: Andi Offset, 2008.

[12] M. D. Wulandari and D. Kusumaningsih, "APLIKASI PENGAMANAN DATABASE BERBASIS DESKTOP DENGAN ALGORITMA AES-128 DAN RIVEST CODE (RC4)," *SKANIKA*, vol. 1, no. 1, pp. 373–379, 2018.

[13] R. C. Wardani and A. Joewono, "Alat Pemantau Aliran Listrik Melalui Koneksi Wireless dengan Informasi Menggunakan SMS," *Widya Tek.*, vol. 12, no. 1, pp. 36–46, 2017.