Aplikasi Enkripsi dan Dekripsi untuk Keamanan Komunikasi Data pada SMS (*Short Message Service*) Berbasis Android Menggunakan Algoritma Blowfish

Ibrahim Mahardika Seno.[1], Anggi Puspita Sari[2], Wawan Gunawan[3]

Program Studi Teknik Informatika STMIK Nusa Mandiri Jakarta
Program Studi Sistem Informasi, Universitas Bina Sarana Informatika
Program Studi Teknik Informatika, Universitas Mercubuana

impandaseno@gmail.com[1], anggi.apr@bsi.ac.id [2], wawan.gunawan@mercubuana.ac.id[3]

Abstract - ***SMS become one of communication service most favored, because each mobile phone in circulation either expensie or cheap have the SMS servivce. SMS interception is the theft of the contents of the SMS messages when in the process of the transmission from the sender through the Short Message Service Center (SMSC) and toward the recipients. And SMS snooping occur more frequently due to the negligence of mobile phone users. For example when someone lend the phone to others, at that time the person can intentionally or not, open the message in the inbox. Therefore, by using cryptography provides guarantee security of data or information by means of encryption and decryption, by using one of the cryptographic algorithm is Blowfish algorithm. Blowfish is one of the algorithms that are strong enough to have a large key spaces and the length can be varied, so it is not vulnerable to attack on the key. The applications are developed in an Android Studio because it's easy in implementation of the blowfish algorithm.***

Keywords: SMS, Cryptography, Security, Blowfish Algorithm

Abstrak - SMS menjadi salah satu layanan komunikasi yang paling disukai, karena setiap telepon seluler yang beredar baik mahal maupun murah memiliki layanan SMS. Namun banyak celah keamanan pada pengiriman SMS seperti SMS *interception* dan SMS *Snooping*. SMS *interception* adalah pencurian isi pesan SMS ketika dalam proses transmisi dari pengirim melalui *Short Message Service Center* (SMSC) dan menuju ke penerima. Dan SMS *snooping* lebih sering terjadi karena kelalaian pengguna telepon seluler. Contohnya ketika seseorang meminjamkan telepon selulernya pada orang lain untuk digunakan telepon. Pada saat itu orang tersebut dapat dengan sengaja atau tidak membuka isi pesan yang ada pada *inbox* SMS. Oleh karena itu, dengan menggunakan kriptografi memberikan jaminan keamanan data atau informasi dengan cara enkripsi dan dekripsi menggunakan salah satu algoritma kriptografi yaitu Algoritma *Blowfish*. *Blowfish* merupakan salah satu algoritma yang cukup kuat memiliki ruang kunci yang besar dan panjangnya bisa beragam, sehingga tidak mudah diserang pada bagian kuncinya. Aplikasi yang dihasilkan dibuat dengan *Android Studio* karena mudah dalam pengimplementasian algorima *blowfish*.

I. PENDAHULUAN

Komunikasi telepon seluler memiliki banyak fitur diantaranya *Short message service* (SMS), *Multimedia Messaging Service* (MMS), *chatting*, *video call*, dan internet. Di antara beberapa layanan tersebut, SMS menjadi salah satu layanan komunikasi yang paling disukai, hal tesebut di karenakan setiap telepon seluler yang beredar baik mahal maupun murah memiliki layanan SMS.

Celah keamanan terbesar pada layanan SMS adalah pada saat SMS tersebut dikirim melalui jaringan telekomunikasi. SMS bekerja pada jaringan nirkabel yang memungkinkan terjadinya pencurian isi pesan SMS ketika dalam proses transmisi dari pengirim melalui Short Message Service Center (SMSC) dan menuju ke penerima, hal tersebut merupakan ancaman SMS interception. SMSC memiliki fungsi mencatat segala aktifitas komunikasi yang terjadi antara pengirim dan penerima. Ancaman SMS lainnya adalah SMS snooping, SMS snooping lebih sering terjadi karena kelalaian pengguna telepon seluler. Contohnya ketika seseorang meminjamkan telepon selulernya pada orang lain untuk menggunakan telepon selulernya. Pada saat itu orang tersebut dapat dengan sengaja atau tidak membuka isi pesan yang ada pada inbox SMS. Untuk itu dibutuhkan sebuah sistem keamanan pada layanan SMS yang mampu menjaga integritas dan keamanan isi pesan, agar isi pesan tersebut hanya bisa dibaca pengirim dan penerima.

Salah satu solusinya adalah menerapkan suatu algoritma kriptografi dengan terenkripsinya pesan yang akan dikirimkan. Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah data (plaintext) menjadi data yang

tersembunyi (ciphertext). Ciphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah. Salah satu algoritma yang terkenal untuk mengamankan isi pesan adalah Algoritma Blowfish. Karena Blowfish merupakan salah satu algoritma yang cukup kuat memiliki ruang kunci yang besar dan panjangnya bisa beragam, sehingga tidak mudah diserang pada bagian kuncinya. Diharapkan hasil akhir dari aplikasi ini dapat bermanfaat bagi semua pengguna SMS yang menginginkan keamanan yang lebih.

II. LANDASAN TEORI DAN METODE

Metode penelitian memegang peranan penting dalam memberikan pondasi atau landasan terhadap tindak dan keputusan dalam membangun suatu bidang terutama dalam sebuah penelitian. Adapun metode penelitian yang penulis gunakan untuk menyelesaikan berbagai masalah yang terjadi adalah:

Teknik Pengumpulan Data

1. *Observasi*
   Penulis melakukan *observasi* terhadap algoritma *blowfish* untuk mengetahui bagaimana cara pengimplementasian enkripsi dan dekripsi pesan singkat dengan *key* kedalam aplikasi berbasis android.

2. Studi Pustaka
   Dalam pengumpulan data, penulis mendapatkan sumber yang mendukung seperti jurnal, buku, dan e-book. Serta sumber dari internet untuk pembuatan langkah-langkah pembangunan aplikasi ini.

Metode Pengembangan Sistem

1. Analisa Kebutuhan
   Berdasarkan hasil analisis permasalahan mengenai pembuatan aplikasi ini diharapkan dapat mengatasi permasalahan yang dapat menghalangi proses maupun kinerja dari pihak terkait. Perancangan aplikasi ini penulis menggunakan software Android Studio V.1.5 sebagai pendukung.
2. Desain
   Desain yang akan penulis buat terdiri dari tampilan yang sesuai dengan kebutuhan aplikasi. Agar para pengguna dapat mengoperasikan aplikasi ini dengan mudah penulis menggunakan software Android Studio V.1.5, serta mendesain input dan output program untuk interaksi antara program dengan pengguna.
3. Testing
   Selanjutnya tahap Testing (pengujian system). Testing disini dilakukan agar diketahui beberapa aspek-aspek kesalahan pada pengujian aplikasi dan pengujian menggunakan white box testing dan black box testing.
4. Implementasi
   Implementasi menggunakan software Android Studio V.1.5 aplikasi enkripsi dan dekripsi SMS akan dijalankan di Android V.2.3 Gingerbread ke atas, kemudian data pesan singkat akan di enkripsi untuk menjaga informasi di dalamnya.

SMS (Short Message Service)

SMS adalah kependekan dari *Short Messages Services*. Ini merupakan sebuah teknologi yang menyediakan pelayanan pengiriman dan penerimaan pesan antar *mobile phone*. Seperti namanya"Short Message Services", data yang mampu ditampung juga terbatas. Satu SMS hanya dapat menampung maksimal 140 *bytes* data, jadi satu SMS dapat menampung:

1. 160 karakter : karakter latin
2. 70 karakter : non latin karakter

Ketika SMS dikirim ke suatu nomor tertentu, SMS yang dikirimkan tidak langsung dikirim ke nomor tersebut, namun akan masuk terlebih dahulu ke SMS Center (SMSC) operator telepon yang digunakan. SMS Center sendiri dapat diartikan sebagai sebuah server yang bertanggung jawab pada proses pengiriman SMS dalam suatu operator. SMS yang dikirimkan dari suatu ponsel akan masuk ke SMSC ini, kemudian diteruskan ke nomor tujuan SMS tersebut. Bila nomor yang dituju ternyata sedang mati/offline, SMSC ini akan menyimpan SMS tersebut untuk sementara, hingga nomor tujuan hidup kembali. Lamanya waktu penyimpanan SMS, sangat tergantung dari lamanya waktu yang telah ditetapkan oleh operator untuk menyimpan SMS tersebut. Nomor yang telah menerima SMS akan mengirimkan laporan ke SMSC bahwa SMS telah diterima. Laporan tersebut kemudian akan diteruskan kembali ke nomor pengirim SMS

Kriptografi

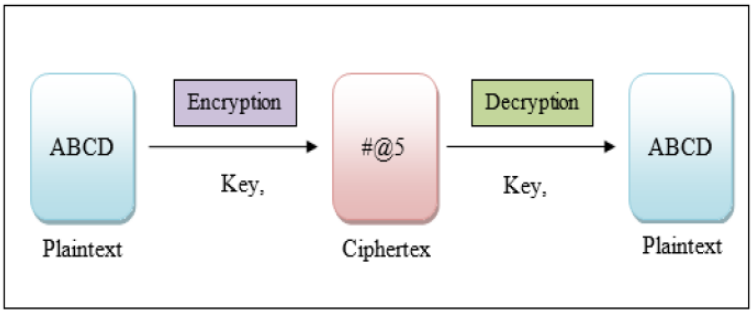
Kriptografi merupakan ilmu dan seni dalam memproteksikan informasi dengan mengubahnya ke dalam bentuk himpunan karakter acak yang tidak dapat dibaca. Kriptografi adalah sebuah cara yang efektif dalam mengamankan informasi penting baik yang tersimpan dalam media penyimpanan atau melalui jaringan komunikasi.

Terminology kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Pada prinsipnya, kriptogarfi memiliki 4 komponen utama yaitu:

1. Plaintext, yaitu pesan yang dapat dibaca secara langsung.
2. Ciphertext, yaitu pesan yang disandikan.
3. Key, yaitu kunci untuk melakukan enkripsi atau dekripsi.

4. Algoritma, yaitu metode yang digunakan untuk melakukan enkripsi atau dekripsi.

Enkripsi (*encryption*) adalah sebuah proses menjadikan pesan yang dapat dibaca (*plaintext*) menjadi pesan acak yang tidak dapat dibaca (*ciphertext*). Sedangkan dekripsi (*decryption*) merupakan proses kebalikan dari enkripsi dimana proses ini mengubah *ciphertext* menjadi *plaintext.*



Sumber:Jurnal Coding Sistem Komputer Untan
Gambar 1. Ilustrasi Enkripsi dan Dekripsi

Algoritma Blowfish

Blowfish alias "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem.* Diciptakan oleh seorang *Cryptanalyst* bernama Bruce Schneier Presiden perusahaan *Counterpane Internet Security, Inc* (Perusahaan konsultan tentang kriptografi dan keamanan Komputer) dan dipublikasikan tahun 1994. Sejak saat itu telah dilakukan berbagai macam analisis, dan perlahan - lahan mulai mendapat penerimaan sebagai algoritma enkripsi yang kuat.

Blowfish adalah algoritma yang tidak dipatenkan dan *license free*, dan tersedia secara gratis untuk berbagai macam kegunaan. *Blowfish* dirancang dan diharapkan mempunyai kriteria perancangan yang diiginkan sebagai berikut :

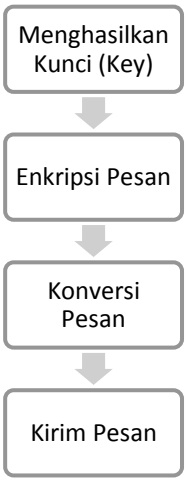
1. Cepat, Blowfish melakukan enkripsi data pada microprocessor 32-bit dengan rate 26 clock cycles per byte.
2. Compact, Blowfish dapat dijalankan pada memory kurang dari 5K.
3. Sederhana, Blowfish hanya menggunakan operasi – operasi sederhana, Blowfish hanya menggunakan operasi – operasi sederhana, seperti : penambahan, XOR, dan lookup tabel pada operan32-bit.
4. Memiliki tingkat keamanan yang bervariasi, panjang kunci yang digunakan oleh Blowfish dapat bervariasi dan bisa sampai sepanjang minimal 32-bit, maksimal 448 -bit, Multiple 8 bit, defalut 128 bit.

Skema proses enkripsi dan dekripsi pada algoritma *Blowfish*

1. Proses Pengiriman dan Penerimaan Pesan dengan Algoritma Blowfish

   Proses dalam pembuatan aplikasi dapat dibagi ke dalam dua tahapan yaitu tahap pengiriman pesan dan tahap penerimaan pesan. Berikut adalah ilustrasi mengenai tahap pengiriman pesan:

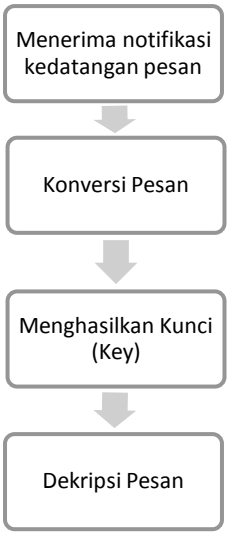
a. Tahap Pengiriman Pesan Singkat dengan Algoritma *Blowfish*



Gambar 2. Proses Pengiriman Pesan Enkripsi

Pertama, pengguna memasukan kunci yang berukuran 32-448 bit sesuai dengan spesifikasi pada algoritma Blowfish. Kunci inilah yang akan digunakan untuk melakukan enkripsi dan dekripsi pesan. Selanjutnya pesan akan dienkripsi dengan melakukan operasi pada struktur jaringan *Feistel* pada *Blowfish* dengan menggunakan kunci dan upakunci yang dihasilkan. Setelah itu, pesan akan dikonversi ke dalam representasi *hexadecimal* sebelum dikirimkan. Selanjutnya, pesan dikirimkan dalam bentuk *string hexadecimal* menuju alamat tujuan.

b. Tahap Penerimaan Pesan Singkat dengan Algoritma Blowfish



Gambar 3. Proses Dekripsi Penerimaan Pesan

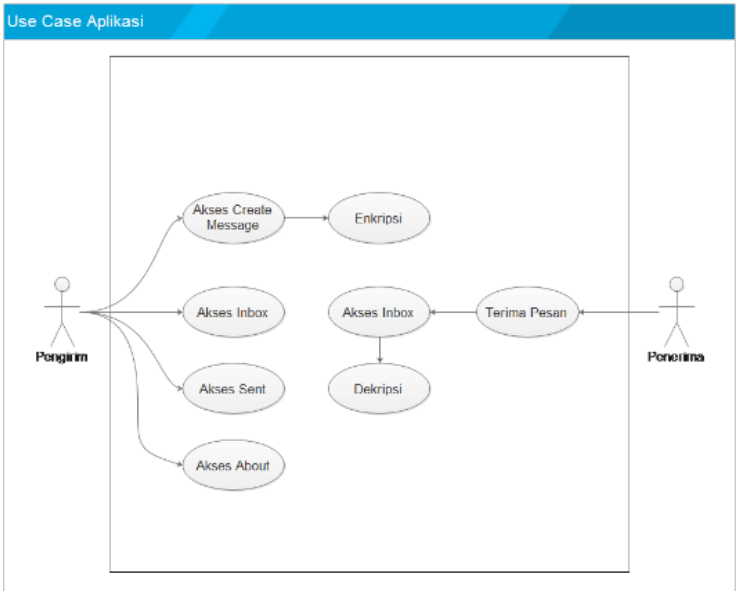
Aplikasi akan mendapatkan notifikasi dari sistem operasi Android mengenai kedatangan pesan singkat (SMS). Selanjutnya, aplikasi akan melakukan konversi pesan dari representasi string hexadecimal ke dalam representasi array of byte. Setelah konversi dilakukan, aplikasi akan meminta pengguna untuk memasukan kunci (key) yang akan digunakan untuk melakukan dekripsi progam. Berikutnya, aplikasi akan melakukan dekripsi pesan.

III. PEKERJAAN DAN DISKUSI HASIL

Berdasarkan hasil analisa tentang kebutuhan-kebutuhan yang diperlukan, maka dapat diidentifikasikan serta diimplementasikan melalui rancangan sistem, serta rancangan layar.

Rancangan Sistem

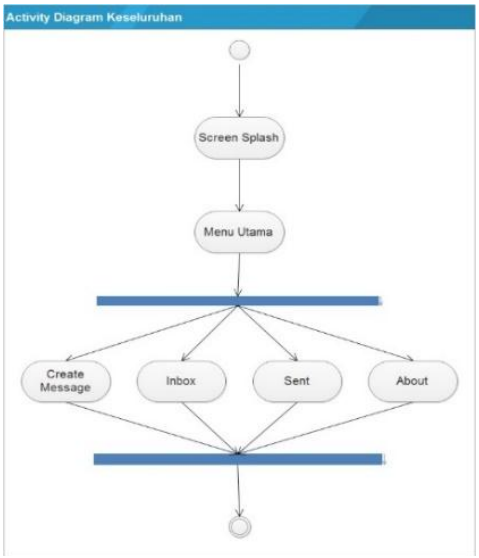
1. Use Case Diagram



Sumber: Hasil Penelitian

Gambar 4. *Use Case* Diagram

2. Activity Diagram Aplikasi

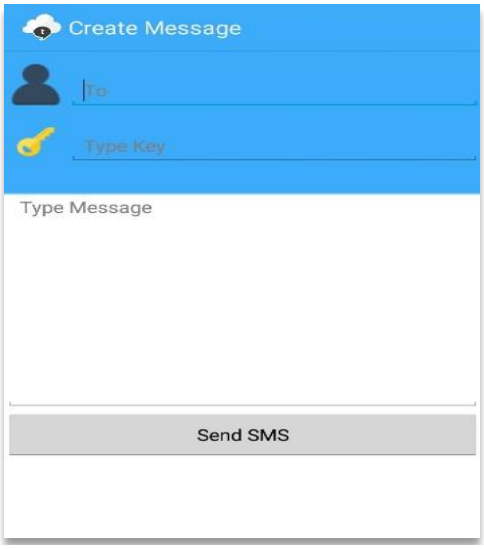


Sumber: Hasil Penelitian
Gambar 5. Activity Diagram Aplikasi

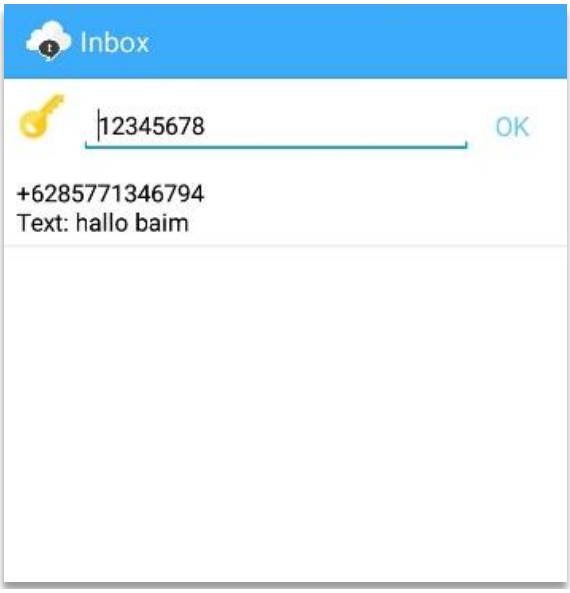
3. Rancangan Layar

Sumber: Hasil Penelitian
Gambar 6. *User Interface Screen Splash*

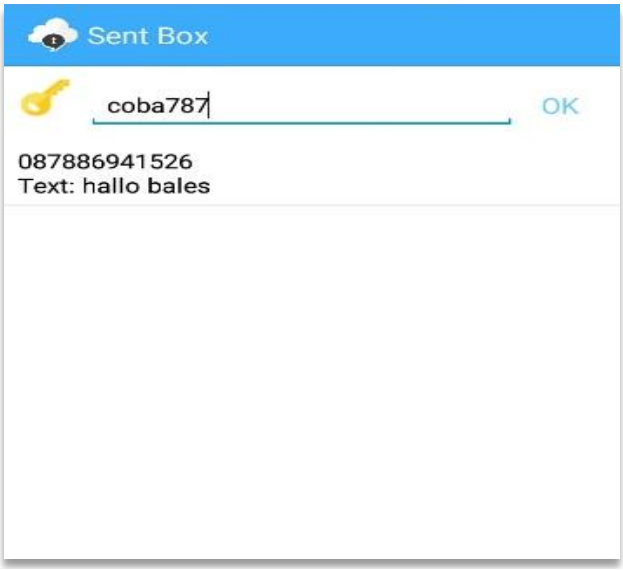
Sumber: Hasil Penelitian
Gambar 7. User Interface Menu Utama



Sumber: Hasil Penelitian
Gambar 8. User Interface Create Message



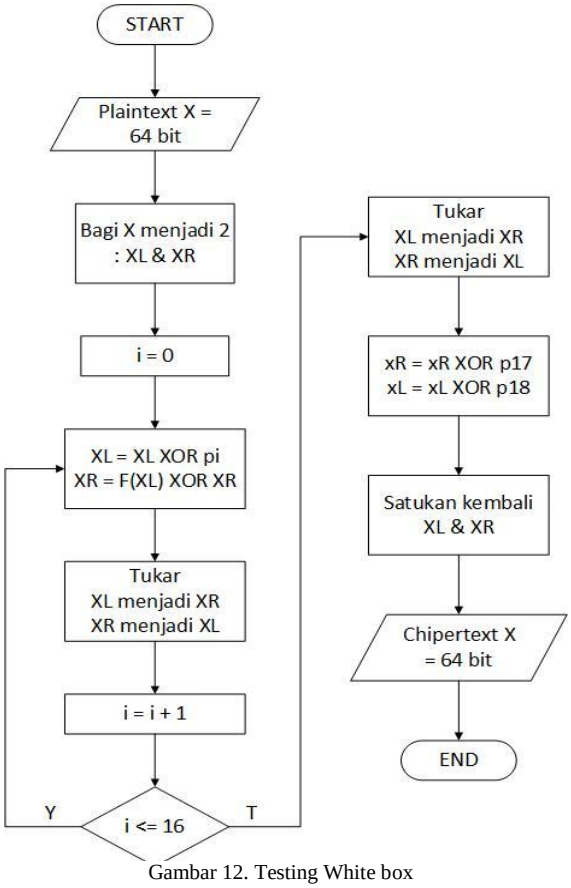
Sumber: Hasil Penelitian
Gambar 9. User Interface Inbox



Sumber: Hasil Penelitian
Gambar 10. User Interface Screen Splash

Sumber: Hasil Penelitian
Gambar 11. User Interface About

4. Testing
   White Box



Gambar 12. Testing White box

Kompleksitas Siklomatis (pengukuran kuantitatif terhadap kompleksitas logis suatu program) dari grafik alir dapat diperoleh dengan perhitungan:
Dimana:

$$V(G) = E - N + 2$$

E = Jumlah *edge* grafik alir yang ditandakan dengan gambar panah
N = Jumlah simpul grafik alir yang ditandakan dengan gambar lingkaran
V(G) = Jumlah *Region*
Sehingga kompleksitas siklomatisnya
V(G) = 13-13+2 = 2

Baris set yang dihasilkan jalur *independent* adalah sebagai berikut:
a. 1-2-3-4-5-6-7-8-9-10-11-12-13
b. 1-2-3-4-5-6-7-8-5-6-7-8-9-10-11-12-13

Black Box
Pengujian selanjutnya dilakukan untuk memastikan bahwa suatu *event* atau *input* menjelaskan proses yang tepat dan menghasilkan *output* yang sesuai dengan rancangan yang telah dibuat, berikut hasil pengujian *black box* untuk aplikasi ini.

Tabel 1.Hasil Pengujian *Black Box*

	Sekenario uji	*Text Case*	Hasil yang diharapkan	Keterangan
	Memilih *Button Create Message*	Menampilkan tampilan mengirim pesan	Tampil *layout create Message*	Sesuai
	Memilih *Button Inbox*	Menampilkan pesan masuk	Tampil *layout inbox*	Sesuai
	Memilih *Button Sent*	Menampilkan pesan keluar	Tampil *layout sent*	Sesuai
	Memilih *Button About*	Menampilan info tentang aplikasi	Tampil *layout about*	Sesuai

Sumber:Hasil Penelitian

IV. KESIMPULAN

Berdasarkan hasil penulisan yang telah dilakukan dapat disimpulkan bahwa:
1. Pada pada penelitian ini telah berhasil dibuat aplikasi Android dengan menggunakan algoritma kriptografi *blowfish* dalam pembuatan aplikasi enkripsi dan dekripsi untuk pesan singkat atau *Short Message Service (SMS)*.
2. Aplikasi dapat melakukan enkripsi dan dekripsi dengan dengan baik menggunakan smartphone Android. Hal ini dibuktikan dengan proses pengiriman dan penerimaan yang dikirim secara utuh.
3. Hasil dari teks pesan tidak dapat muncul ketika penerima tidak menggunakan kunci yang sama dengan kunci pengirim sehingga kerahasiaan pesan dapat terjaga dengan baik.
4. Dalam proses pengiriman pesan menggunakan jaringan provider SIM Card pada perangkat android, dan bagi perangkat android dengan fitur dual SIM Card, maka aplikasi akan mendeteksi pengguna SIM Card pada slot SIM 1 (slot utama).
5. Dengan hasil enkripsi yang berupa kata-kata sandi (chipertext) dan chipertext tersebut hanya bisa diterjemahkan kedalam plaintext oleh aplikasi yang dibuat ini, dapat mengatasi permasalahan SMS snooping dan SMS interception.

REFERENSI

[1] Andriani, Rosdian Dwi. 2015. "Simulasi Pembelajaran Short Message Service Berbasis Visual Basic 6.0" (Online). (http://telekomunikasi.poltekom.ac.id. Diakses 2 Februari 2016).
[2] A,S Rosa dan M. Shalahuddin. 2013, Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek), Bandung: Modula.
[3] Defni dan Indri Rahmayun. 2014. "Enkripsi SMS (Short Message Service) Pada telepon Selular Berbasis Android Dengan Metode RC6". ISSN : 1693-752X. Padang : Jurnal Momentum, Vol.16 No.1.
[4] Irawan, Rio, dkk. 2015. "Aplikasi Enkripsi dan Dekripsi Pesan Singkat Menggunakan Algoritma Knapsack Berbasis Android". ISSN : 2338-493X. Pontianak : Jurnal Coding Sistem Komputer Untan Vol 03, No. 3, hal 57-66.
[5] Meyers, Desoki. 2008. *An Implementation of Blowfish Cryptosystem*. University of Louisville.
[6] Nofriadi M.Kom. 2015, "Java Fundamental dengan Netbeans 8.0.2", Yogyakarta: Deepublish.
[7] Safaat H, Nazruddin. 2012, Android Pemograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android, Bandung: Informatika.
[8] Schneier, Bruce. 1994. "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)". (http://schneier.com. Diakses 11 desember 2015).
[9] Sitinjak, Suriski dkk. 2010. "Aplikasi Kriptografi File Menggunkan Algoritma Blowfish". ISSN 1979-2328. Yogyakarta : Seminar Nasional Informatika 2010.
[10] Tumbur, Sony Theo. 2013. "Implementasi Algoritma Blowfish dalam Layanan Pesan Singkat pada Platform Android". (online) (http://informatika.stei.itb.-ac.id/, diakses 11 desember 2015).
[11] Trianggana, Dimas Aulia dan Herlina Latipa Sari. 2015. "Analisis Perbandingan kinerja Algoritma Blowfish dan Algoritma Twofish pada Proses Enkripsi dan Dekripsi". ISSN : 2355 – 5920. Bengkulu : Jurnal Pseudocode, Vol.2 No.1.
[12] Winarno, Edi. 2011, Membuat Sendiri Aplikasi Android untuk Pemula. Jakarta: Pt. Elex Media Komputindo.