JOEICT (Jurnal of Education and Information Communication Technology)
Volume 1, Nomor 1, Tahun 2017: 29 – 36

PENERAPAN TEKNIK KRIPTOGRAFI PADA KEAMANAN SMSANDROID

Ika Febriana[1)], Ganjar Aji S[2)]
Pendidikan Teknologi Informasi
STKIP PGRI TULUNGAGUNG
Jalan Mayor Sujadi No.7, Tulungagung, 66261
e-mail :ikaclouds1@gmail.com[1)], ganjarajisofyan95@gmail.com[2)]

ABSTRAK

Kriptografi telah menjadi bagian penting Dalam dunia teknologi informasi saat ini. Hampir semua penerapan teknologi informasi menggunakan Kriptografi untuk menjamin kemananan dan kerahasiaan informasi. Sebuah pesan yang tidak disandikan atau dienkripsi disebut plaintext, sedangkan pesan yang telah disandikan dengan sebuah algortitma kriptografi disebut chypertext. Dan proses mengubah plaintext menjadi chypertext disebut encryption. Kriptografi merupakan suatu teknik mengamankan pesan dengan cara melakukan enkripsi terhadap isi pesan tersebut agar aman sedangkan (Short Message Service) Merupakan layanan yang disediakan oleh telepon seluler untuk mengirim dan menerima pesan singkat, SMS dinilai sangat praktis, murah dan efisien. Secara umum, SMS dikirim dalam bentuk plain text (meskipun di encoding/deconding denganProtocol Data Unit) tanpa terenkripsi dari pengirim ke penerima SMS. Jika terjadi penyadapan pada jalur komunikasi, maka teks SMS akan sangat mudah dibaca oleh penyadap. Dalam enskripsi data khususnya yang akan dibahas yaitu SMS, terdapat berbagai algoritma yang dapat digunakan untuk mengamankan suatu data. Dalam hal ini perlu menggunakan aplikasi SMSEncoder untuk merubah pesan menjadi sebuah enkripsi.

***Kata kunci** : Cryptography, Short Messaging Service (SMS), plain text, Chyper Text*

ABSTRACT

Cryptography has become an important part in information technology. Almost all the application of information technology use cryptography to ensure the security and confidentiality of information. A message that is not encoded or encrypted known plaintext, while the message that was encrypted by a cryptographic algorithm called chypertext. And the process of converting plaintext into chypertext called encryption. Cryptography is a technique to secure the message by means of encrypting the contents of the message to be safe while (Short Message Service) is a service provided by a mobile phone to send and receive short messages, SMS is considered very practical, cheap and efficient. In general, an SMS is sent in plain text (although in encoding / decoding with Protocol Data Unit) without encrypted from sender to recipient SMS. In case of wiretapping on telecommunication lines, then the SMS text will be readable by eavesdroppers. In particular data encryption to be discussed is the SMS, there are many different algorithms that can be used to secure the data. In this case the application needs to use SMS Encoder to transform intoencrypted message.

***Keywords** : Cryptography, Short Messaging Service (SMS), plain text, Chyper Text*

I PENDAHULUAN

Android berkembangpesat karena mempunyi *platform* yang sangak lengkap baik dalam sistem operasi, aplikasidan *tool* pengembangannya, market aplikasi serta mendapatkan dukungan yang sangat tinggidari komunitas *open source* di dunia. Meskipun Android memiliki fitur yang lengkap, namun layanan SMS (*Short Message Service)* sebagai layanan pertukaran informasi atau pesanpendek menjadi media komunikasi favorit karena saat ini semua telepon genggam memiliki layanan

ini dan yang paling penting adalah biaya SMS relatif murah. Namun demikian SMS tidak menjamin integritas dan keamanan pesan yang disampaikan. Pesan yang bersifat personal atau rahasia tidak dijamin sampai ke penerima tanpa diketahui informasinya oleh pihak yang tidak bertanggung jawab. Beberapa resiko yang dapat mengancam keamanan pesan pada layanan SMS antara lain SMS *spoofing,* SMS *snooping,* dan SMS *Interception.*SMS bekerja dalam jaringan nirkabel. Dalam aplikasinya, pentrasmisian SMSmembutuhkan beberapa komponen khusus untuk mengirimkan pesan sampai ke tujuan.
Komponen yang diperlukan untuk melakukan komunikasi SMS diantaranya adalah : BTS(*Base Transceiver Station*), MSC (*Mobile Switching Center*),SMSC (*SMS Service Center*)komponen yang paling krusial adalah SMSC adalah sebuah perangkat yang terpasang pada3jaringan utama SMSC ini berfungsi untuk menerima SMS dan menelusuri nomor tujuan, dan mengirimkannya ke perangkat tujuan (Telepon Seluler). SMSC ini juga berperan sebagai penyimpanan sementara untuk SMS. Jadi, jika nomor tujuan tersebut tidak aktif, SMS tersebut akan tersimpan pada SMSC dan SMSC akan mengirimkannya kembali jika perangkat tujuan telah aktif kembali. Sebagai tambahan, SMSC akan memberikan notifikasi kepada pengirim apakah pengiriman SMS tersebut berhasil ataupun tidak. Namun, karenaketerbatasan memori penyimpanan, SMSC tidak dapat menyimpan SMS untuk jangka waktu
yang lama.Dengan tersimpannya SMS pada SMSC, maka seorang operator dapat memperoleh informasi atau membaca SMS di dalam SMSC tersebut. Dengan demikian dibutuhkan suatu metode dan aplikasi yang dapat mempertimbangkan solusi *encrypted end to end* dengan melakukan enkripsi terhadap pesan SMS.Enkripsi dimaksudkan untuk melindungi dan menyamarkan informasi agar tidak terlihat oleh pihak atau orang yang bukan seharusnya. [1]

II PEMBAHASAN

Aplikasi
Menurut kadir(2003), aplikasi atau juga disebut program aplikasi adalah program yang dibuat oleh pemakai yang ditujukan hanyauntuk melakukan suatu tugas khusus)[2].

Kriptografi
Kriptografi berasal dari bahasa Yunani yaitu cryptós yang artinya “secret” (yang tersembunyi) dan gráphein
yang artinya “writting” (tulisan). Jadi, kriptografi berarti ”secret writting” (tulisan rahasia). Menurut Bruce Schneier (1996) kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan(Cryptography is the art and science of keeping messages secure) [3].

Terminologi dalam Kriptografi
Ada beberapa istilah-istilah yang penting dalam kriptografi, yaitu :

1. Pesan (Plaintext dan Ciphertext)
   Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan asli disebut plainteks (plaintext) atau teks-jelas (cleartext). Sedangkan pesan yang sudah disandikan disebut cipherteks (chipertext)

2. Pengirim dan Penerima
   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (sender) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (receiver) adalah entitas yang menerima pesan.
3. Penyadap (eavesdropper) adalah orang yang mencoba menangkap pesan selama ditransmisikan.
4. Kriptanalisis dan Kriptologi : Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis.
   Kriptologi (cryptology) adalah studi mengenai kriptografi dan kriptanalisis.
5. Enkripsi dan Dekripsi : Proses menyandikan plainteks menjadi cipherteks disebut enkripsi

(encryption) atau enciphering. Sedangkan proses mengembalikan cipherteks menjadi plainteks semula
dinamakan dekripsi (descryption) atau deciphering.

6. Cipher dan Kunci : Algoritma kriptografi disebut juga cipher yaitu aturan untuk enchipering dan dechipering, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Kunci (key) adalahparameter yang digunakan untuk transformasi enciphering dan dechipering. Kunci biasanya berupastring atau deretan bilangan[4].

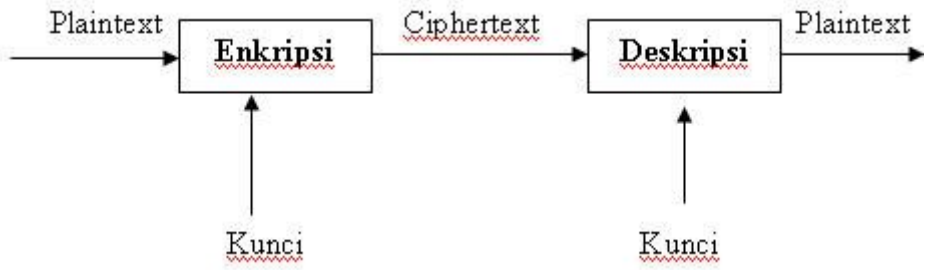
Kriptografi Kunci Simetri (Kriptografi Kunci-Privat)

Pada sistem kriptografi kunci-simetri, kunci untuk enkripsi sama dengan kunci untuk dekripsi, oleh karena itulah dinamakan kriptografi simetri. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kuncinya. Ada banyak algoritma kriptografi modern yang termasuk ke dalam sistem kriptografi simetri, diantaranya adalah DES (Data Encryption Standard), Blowfish, Twofish, Triple-DES, IDEA, Serpent, AES (Advanced Encryption Standard)[5].

Menurut Lung dan Munir (2005) Algoritma kriptografi *(cipher)* simetri dapat dikelompokkan menjadi dua kategori,
[6]

1. Cipher aliran (stream cipher)
   Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal, yang dalam hal ini
   rangkaian bit dienkripsikan/didekripsikan bit per bit.

2. Cipher blok (block cipher)
   Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk blok bit, yang dalam hal ini
   rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. Gambar di bawah menjelaskan tentang Skema Proses Kriptografi.



Gambar 1. Skema Proses Kriptografi

Pada gambar 1. Skema proses kriptografi Fasilitas untuk mengkonversikan sebuah plaintext ke ciphertext atau sebaliknya disebut *Cryptographic system* atau *Cryptosystem* dimana sistem tesebut terdiri dari algoritma–algorima tertentu yang tergantung pada sistem yang digunakan. Algoritma kriptografi (*cryptographic algorithm*) disebut *cipher* yang merupakan persamaan matematik yang digunakan dalam proses enkripsi dan deskripsi dimana proses tersebut diatur oleh satu atau lebih kunci kriptografi. Kunci-

kunci tersebut secara umum digunakan untuk proses pengenkripsian dan pendekripsian tidak perlu identik, tergantung sistem yang digunakan[7].

Proses enkrisi dan deskrisi secara matematis diterangkan sebagai berikut :

EK (M) = C (Proses Enkripsi)

DK (C) = M (Proses Deskripsi)

Keterangan :

EK : Enkripsi.

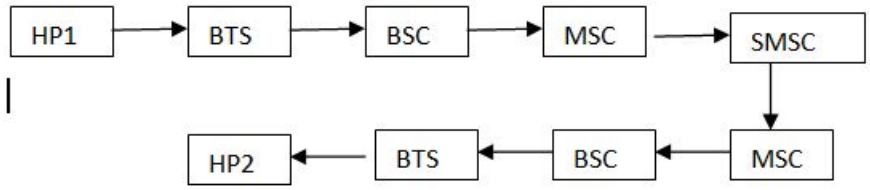
DK : Deskripsi.

M : Message (Pesan sebelum dienkripsi).

C : Cipher (Pesan setelah dienkrisi).

SMS (*SHORT MESSAGING SERVICE)*

Pada gambar di bawah menjelaskan tentang skema proses SMS



Gambar 2. Skema Proses SMS

Pada gambar 2. Skema proses SMS, SMS bekerja dalam jaringan nirkabel. Dalam aplikasinya, pentrasmisian SMSmembutuhkan beberapa komponen khusus untuk mengirimkan pesan sampai ke tujuan.Komponen yang diperlukan untuk melakukan komunikasi SMS diantaranya adalah :

a. BTS (*Base Transceiver Station*) BTS ini merupakan sebuah perangkat yang memfasilitasikomunikasi nirkabel antara perangkat user dengan jaringan. Perangkat user ini dapatmeliputi telepon selular, komputer dengan koneksi internet nirkabel, dan lain-lain.

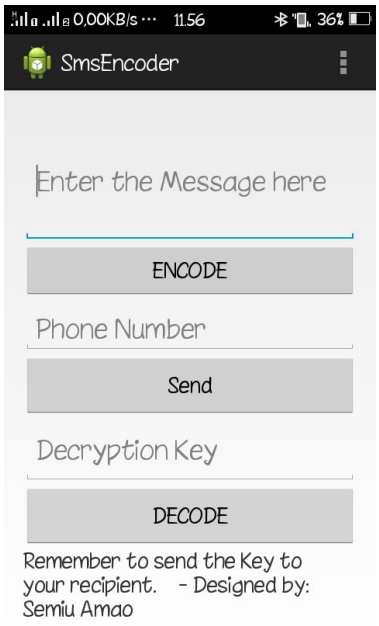
b.MSC (*Mobile Switching Center*) MSC ini adalah sebuah noda layanan pengiriman utamabagi GSM/CDMA. Perangkat ini berfungsi untuk *routing* panggilan suara, SMS, FAX,maupun *conference call*.

c. SMSC (*SMS Service Center*) SMSC adalah sebuah perangkat yang terpasang padajaringan utama SMSC ini berfungsi untuk menerima SMS dan menelusuri nomor tujuan,dan mengirimkannya ke perangkat tujuan (Telepon Seluler).[8]

III PENERAPAN TEKNIK KRIPTOGRAFI PADA SMS ANDROID

3.1 Perancangan Antarmuka (Interface)

Gambar dibawah menunjukkan Tampilan Aplikasi SMS ENCODER



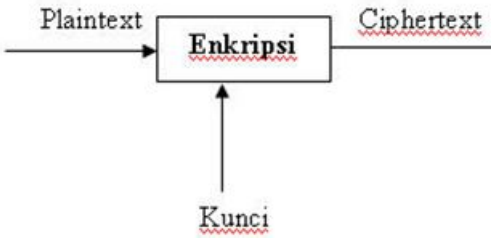
Gambar 3. Tampilan Aplikasi SMS ENCODER

Pada gambar 3 diatas, ,di sini terdapat 3 Input yang harus disi yakni ENCODE, SEND, dan DECODE. Contoh pengimplementasiannya :

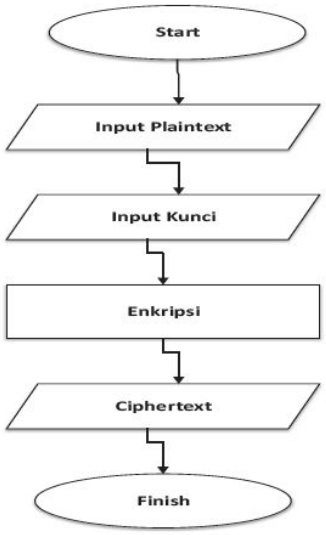
1. ENCODE = setelah menginputkan deskripsi teks, maka ketika di klik Encode , pesan tersebut akan berubah menjadi sebuah enkripsi. .
2. SEND = nomor penerima pesan.
3. DECODE = Pendeskripsian pesan.

3.2 Enkripsi File

Gambar 4 dibawah menunjukkan skema proses dan flowchart Enkripsi



Gambar 4. Skema Proses Enkripsi

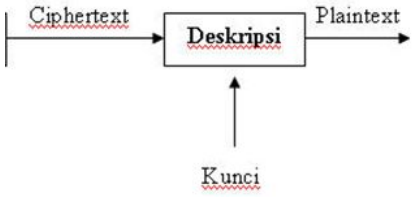


Gambar 5. Flowchart Enkripsi file

Pada tahap ini??? merancang program untuk mengenkripsi text Kunci yang digunakan untuk proses enkripsi text bisa berupa gabungan angka, huruf dan karakter khusus sesuai keinginan dari penggunanya. Setelah proses enkripsi text berhasil maka hasil outputnya berupa cipherteks yang sudah tidak dapat dimengerti maknanya.

3.3 Proses Dekripsi File

Gambar dibawah menunjukkan Skema Proses Deskripsi



Gambar 6. Skema Proses Deskripsi

Kunci yang digunakan untuk proses enkripsi text bisa berupa gabungan angka, hurufdan karakter khusus sesuai keinginan dari penggunanya proses dekripsi textberhasil maka hasil *output*nya berupa plainteks yang bisa dimengerti maknanya.

3.4 IMPLEMENTASI

Pada gambar di bawah menunjukkan hasil implenetasi teknik enkripsi sms android

Hasil Enkripsi

Hasil Deskripsi

Gambar 7. Enkripsi dan deskripsi File

Pada gambar 7 diatas terlihat hasil aplikasi yang telah melakukan deskripsi pada hasil enkripsi yang ada.

III KESIMPULAN

Dari hasil penulisan, dapat ditarik kesimpulan bahwa :

Kriptografi dapat diimplementasikan untuk keamanan sms android. Aplikasi ini masih sederhana, disarankan menambahkan fitur lain seperti simpan kunci ataupun kirim kunci otomatis Pengembangan selanjutnya agar dapat meningkatkan fungsional dan manfaat aplikasi ini. Beberapa saran dari penulis

untuk pengembangan aplikasi ini yaitu: Menambahkan algortima kriptografi yang lain agar dapat menjadi pilihan enkripsi. Sedangkan untuk prioritas kekuatan keamanan disarankan agar menggunakan algoritma kriptografi yang lebih kuat atau terbaru.

DAFTAR PUSTAKA

[1]Rahayu,Tri Puji, Yakub, Limiady,Irwan, *Aplikasi Enkripsi Pesan Teks (SMS) Pada Perangkat Handphone Dengan Algoritma Caesar Cipher*.

[2] Kadir, Abdul, 2003, Pengenalan Sistem Informasi, Andi, Yogyakarta.

[3] Schneier, Bruce, 1996, Applied *Cryptography*, Second Edition, John Wiley & Son, New York.

[4]Munir, Rinaldi. 2006. *Pengantar Kriptografi*

[5] Munir, Rinaldi. 2004. *Bahan Kuliah IF5054 Kriptografi.*

[6] Lung, C., Munir, R., 2005, Studi dan Implementasi AES dengan Empat Mode Operasi Block Cipher.

[7] Anjar, *Enkripsi blowfish.* <www.ilmukomputer.org> diakses tanggal 28-12-2016

[8] Pangestu, Tegar Aji, *Implementasi Algoritma Rijndael pada Aplikasi AndroidPengirim Short Message Service (SMS) Terenkripsi*.