APLIKASI KRIPTOGRAFI UNTUK SMS (SHORT MESSAGING SERVICE) MENGGUNAKAN STRUKTUR FEISTEL BERBASIS ANDROID

Gede Arna Jude Saskara[1], Koredianto Usman[2], Unang Sunarya[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Short Messaging Service (SMS) merupakan suatu layanan yang paling banyak digunakan untuk menyampaikan suatu informasi. Informasi yang dikirim dengan menggunakan SMS sangat beragam dari informasi yang biasa hingga informasi yang sangat rahasia. Untuk menjaga kerahasiaan pesan tersebut dikembangkanlah suatu ilmu yang mempelajari tentang cara pengamanan informasi/pesan yang dikenal dengan istilah kriptografi. Algoritma kriptografi ini ada yang simetri dan asimetri. Disebut algoritma simetri dikarenakan kunci yang digunakan untuk me-enkripsi dan mendekripsi pesan nilainya sama sedangkan algoritma kriptografi asimetri kunci enkripsi dan dekripsi nilainya berbeda. Salah satu algoritma kriptografi simetri adalah algoritma Feistel.

Sekarang ini banyak tersedia smartphone salah satunya smartphone yang menggunakan operating system Android yang dapat mengirimkan pesan, untuk menjaga keamanan pesan tersebut dikembangkanlah aplikasi yang dapat menjaga kerahasiaan pesan pada handphone Android. Aplikasi ini menggunakan algoritma struktur Feistel dengan kunci nomor handphone tujuan dan pengguna. Pada algoritma ini juga ditambahkan dengan permutasi dan feedback untuk meningkatkan avalanche effect.

Berdasarkan hasil pengujian, untuk mengenkripsi pesan aplikasi ini membutuhkan waktu 0.0592 detik. Sedangkan untuk mendekrip cipher text membutuhkan waktu 0.0402 detik. Proses pengujian dengan mencari nilai avalanche effect didapat rata-rata avalanche effectnya 53.9%. Sedangkan pengujian dengan menggunakan brute force attack dibutuhkan waktu 1392.6 tahun. Dengan aplikasi Kriptografi SMS ini dapat membantu mengamankan informasi penting dan rahasia yang biasa dikirim melalui SMS.

Kata Kunci : Kriptografi, Enkripsi, Dekripsi, Simetri, Asimetri.

Abstract
Short Messaging Service (SMS) is services that most widely used to convey information. Information that sent by using SMS is very diverse, from the usual information to highly confidential information. To maintain the confidentiality of the message is by developing a study of how security information / messages known as cryptography. Cryptographic Algorithms that exist are symmetry and asymmetry. Called algorithm symmetry because the key that used to encrypt and decrypt message has same value, and for algorithm asymmetry the key that used to encrypt and decrypt message has different value. One of the symmetry of the cryptographic algorithms is algorithm Feistel.

Nowadays, many smartphone that are available, one of them is smartphone that use Android operating system that can send messages, to maintain the security of the message is by developing applications that can maintain the confidentiality of messages on Android phone. This app is uses Feistel algorithms structure with key phone number destination and user. On this algorithm is also added the permutation and feedback to improve avalanche effect.

ased on test results, to encrypt a message this application requires a time 0.059 seconds, but to decrypt the cipher text takes 0.0439 seconds. The testing process to find the value of avalanche effect, obtained an average 53.9% avalanche effect but for the testing that using brute force attack takes a very long time it's about 1392.588 years. With the creation of Cryptography SMS application can help maintain the important and confidential information that usually sent via SMS.

Keywords : Cryptography, Encryption, Decryption, Symmetry, asymmetry.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Informasi merupakan suatu yang sangat penting dan standar dalam berbagai aspek kehidupan. Dahulu informasi dikirim dengan cara memberikan kode asap, ada juga yang menggunakan peluit dengan kode-kode tertentu, hingga mengirim informasi dengan membuat surat dan dikirim menggunakan burung. Seiring dengan perkembangan teknologi yang tiada habisnya yang memungkinkan manusia untuk dapat berkomunikasi dan saling bertukar informasi pada jarak yang dekat ataupun dengan jarak yang jauh sekalipun. Untuk jarak jauh misalnya antar kota, antar wilayah, antar Negara bahkan hingga antar Benua. Dengan jarak yang jauh bukan merupakan suatu kendala lagi dalam melakukan komunikasi.

Saat ini banyak layanan yang membantu dalam proses pengiriman informasi seperti *E-Mail (Electronic Mail)* dan *SMS (Short Messaging Service)* untuk *E-Mail* menggunakan internet dalam proses pengiriman informasinya sedangkan untuk *SMS* dikirim melalui jaringan telekomunikasi pada telepon selular. *SMS* merupakan yang layanan pengiriman informasi yang paling banyak digunakan dikarenakan hampir semua orang di dunia ini memiliki telepon selular. Dan juga dikarenakan biaya yang murah dibandingkan dengan menelepon langsung. Informasi yang dikirim dengan menggunakan layanan *SMS* bisa saja merupakan informasi penting/rahasia yang tidak boleh diketahui oleh orang lain. Misal informasi bisnis antar Perusahaan, informasi pertahanan Negara. Untuk menjaga kerahasian pesan tersebut dikembangkanlah suatu ilmu yang mempelajari tentang cara pengamanan informasi/pesan yang dikenal dengan istilah kriptografi.

Kriptografi merupakan suatu ilmu yang berfungsi untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Pesan yang akan dikirim tersebut di enkripsi menjadi suatu *cipher text* atau suatu kalimat yang tidak beraturan susunan hurufnya sebelum dikirim. Setelah sampai ke tujuan *cipher text* tersebut di dekripsi menjadi pesan seperti awal. Algoritma kriptografi ini ada yang simetri dan asimetri. Disebut algoritma simetri dikarenakan kunci yang digunakan

untuk me-enkripsi dan mendekripsi pesan nilainya sama sedangkan algoritma asimetri kunci enkripsi dan dekripsi nilainya berbeda.

Pada kategori kunci simetri modern beroperasi dalam mode bit dan dapat dikelompokkan menjadi 2 kategori yaitu *cipher* aliran (*stream cipher*) dan *cipher* blok (*block cipher*). Hampir semua algoritma *cipher* blok bekerja dalam model *Feistel*. Model *Feistel* ini ditemukan oleh Horst Feistel tahun 1970. Model ini juga banyak dipakai dalam algoritma kriptografi seperti *DES*, *LOKI*, *GOST*, *Lucifer*, dll.

Andi Kurniawan Dwi (2012) pernah membuat aplikasi kriptografi pada *SMS* berbasis android dengan menggunakan metode Vigenere Cipher dan menyimpulkan bahwa dengan dengan aplikasi *SMS* yang dibuat dapat meningkatkan keamanan pada layanan *SMS* seperti *snooping* maupun *interception*, namun pada aplikasi ini memiliki kelemahan dengan adanya karakter yang berulang dan user yang akan dikirimi pesan harus mengetahui kunci yang digunakan[7]. Becik Gati Anjari (2012) juga membuat aplikasi enkripsi *SMS* pada telepon selular berbasi android dengan menggunakan metode yang sama dengan Andi Kurniawan Dwi (2012) yaitu metode Vigenere Cipher namun pada aplikasi yang dibuat oleh Becik Gati Anjari (2012) metode Vigenere Cipher sudah dimodifikasi dan diberi *Key* tambahan dengan metode tersebut dapat menghilangkan kelemahan metode vigenere yaitu adanya karakter yang berulang. selain itu juga dengan memberikan kunci tambahan keamanan dan privasi pengguna lebih terjamin[6]. Chandra Ari Wijaya dan Willya Triana (2011) mengimplementasikan algoritma *Twofish* untuk enkripsi dan dekripsi pesan pada ponsel berbasis android menyimpulkan bahwa dengan menggunakan algoritma *Twofish* pengiriman pesan dapat tergjaga keamanannya namun apabila pesannya panjang maka proses pengenkripsiannya akan lama[10].

Vigenere Cipher masih lemah terhadap *avalanche attack* maka dari itu diperlukan langkah untuk meningkatkan *avalance affect* yang disebut *confusion*. Salah satu langkah *confusion* yaitu menambah *feedback* pada pemrosesan algoritmanya. Struktur *feedback* untuk *confusion* yang sering digunakan adalah struktur *Feistel*. Berdasarkan latar belakang diatas maka penulis memiliki inisiatif untuk membuat aplikasi untuk mengamankan pesan menggunakan algoritma kriptografi model *Feistel* dengan Kunci nomor handphone pengguna dan tujuan untuk memenuhi syarat *authentication* pada platform android. Selain itu juga pada

algoritma ini ditambahkan permutasi dimana permutasi ini merupakan proses untuk mengacak setiap karakter agar tidak pada posisi yang sama sehingga dapat menigkatkan *avalanche effectnya*.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka dirancang suatu perangkat yang mencakup permasalah-permasalahan berikut :

1. Bagaimana merancang aplikasi enkripsi dan dekripsi pesan pada *SMS* di Android yang menggunakan algoritma struktur *Feistel*.
2. Bagaimana implementasi kriptografi pada handphone berbasis android dengan menggunakan metode blok cipher *Feistel*
3. Bagaimana performansi dalam pengenkripsian dan pendekripsian data *SMS* yang didapat dari hasil pengujian.

1.3 Batasan Masalah

Pengembangan aplikasi mengamankan pesan menggunakan algoritma kriptografi model *Feistel* terbatas pada hal-hal sebagai berikut.

1. Aplikasi ini dibuat menggunakan eclipse dan SDK sehingga hanya dapat digunakan pada perangkat android
2. Algoritma yang dipakai dalam aplikasi ini menerapkan algoritma *cipher* blok model *Feistel*.
3. Tidak membahas algoritma kriptografi yang lain.
4. Tidak membahas proses pengiriman dan penerimaan *SMS* yang terjadi di luar aplikasi ini.
5. Kunci yang digunakan pada aplikasi ini berupa angka.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini yang mengacu pada rumusan masalah adalah sebagai berikut.

1. Merancang aplikasi enkripsi dan dekripsi pesan pada *SMS* di Android menggunakan *cipher* blok model *Feistel.*
2. Mengimplementasikan algortima Kriptografi pada aplikasi yang berbasis Android.
3. Mengetahui perfomansi sistem yang dirancang.

1.5 Metode Penelitian

Tujuan yang ingin dicapai dalam penelitian ini yang mengacu pada rumusan masalah adalah sebagai berikut.

1. Merancang aplikasi enkripsi dan dekripsi pesan pada *SMS* di Android menggunakan *cipher* blok model *Feistel.*
2. Mengimplementasikan algortima Kriptografi pada aplikasi yang berbasis Android.
3. Mengetahui perfomansi sistem yang dirancang.

1.6 Sistematika Penulisan

Adapun sistematika penulisan laporan hasil penelitian tugas akhir ini adalah sebagai berikut :

1. **BAB I Pendahuluan**

   Pada BAB ini membahas mengenai latar belakang masalah, perumusan masalah dan batasan masalah, tujuan, metodologi penelitian, serta sistematika penulisan dari kegiatan tugas akhir ini.

2. **BAB II Landasan Teori**

   Pada BAB ini akan membahas mengenai teori dasar yang berhubungan dengan aplikasi yang akan dibangun.

3. **BAB III Analisis dan Perancangan Sistem**

   BAB ini berisi analisa terhadap seluruh sistem yang dibuat untuk menentukan kebutuhan apa saja yang harus dipenuhi dan pengembangannya disesuaikan dengan keterbatasan yang dimiliki oleh sumber daya telepon selular.

4. **BAB IV Implementasi dan Analisis Hasil Sistem**

   Pada bagian ini dibahas tentang implementasi dan pengujian terhadap aplikasi yang dikembangkan serta analisis aplikasi.

5. **BAB V Kesimpulan dan Saran**

   Pada BAB ini berisi kesimpulan dan saran dari seluruh kegiatan penelitian tugas akhir ini yang bisa digunakan sebagai masukan untuk pengembangan lebih lanjut.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan implementasi dan pengujian yang telah dilakukan pada bab sebelumnya maka dapat ditarik kesimpulan sebagai berikut :

1. Dari hasil pengimplementasian kriptografi pada handphone yang berbasis android dengan menggunakan metode blok cipher *Feistel*, aplikasi melalukan proses enkripsi dan dekripsi dengan waktu yang cepat. Dimana rata-rata waktu yang digunakan untuk mengenkripsi 30 sampel pesan adalah 0.0592 detik dan rata-rata waktu yang digunakan untuk mendekripsi pesan yang telah di enkripsi adalah 0.0402 detik.
2. Untuk mengetahui bagus atau tidaknya suatu algoritma kriptografi dilakukan penghitungan *avalanche effect* dimana berdasarkan hasil pengujian didapat nilai *avalanche effect* sebesar 53.9% yang dapat dikatakan algoritma yang digunakan cukup baik. Jika dibandingkan dengan algoritma struktur *Feistel* tanpa modifikasi didapat *avalanche effect* sebesar 4.1 % yang dapat dikatakan algoritma *Feistel* tanpa modifikasi jelek.
3. Berdasarkan percobaan cracking dengan mencoba semua kemungkinan kuncinya yang biasa dikenal dengan proses *Brute Force Attack* memerlukan waktu yang sangat lama untuk mengetahui pesan yang dikirimkan yaitu selama 1392.6 tahun.

5.2 Saran

Adapun saran untuk pengembangan aplikasi ini kedepannya adalah :

1. Pada proses penyimpanan password pada database sebaiknya di enkripsi terlebih dahulu atau juga bisa dengan menggunakan hash function.
2. Memperbarui *layout* aplikasi agar menjadi lebih baik lagi.
3. Kedepannya pada aplikasi ini bukan hanya pesan teks biasa yang dapat di enkripsi atau dekripsi melainkan gambar yang dikirim melalui MMS.
4. Mengganti kunci atau memperpanjang kunci pada algoritma kriptografi sehingga dapat meningkatkan keamanan dari pesan.

5. Menambahkan karakter pada daftar numeric sehingga semua karakter dapat dibaca dan tidak mudah ditebak karena berbeda dengan nilai ASCII.
6. Kedepannya aplikasi dapat dikembangkan ke *platform* handphone lain seperti Blackberry, Iphone dan Windows Phone.

DAFTAR PUSTAKA

[1] Arius, Dony. 2008. *Pengantar Ilmu Kriptografi, Teori, Analisis dan Implementasi*. Yogyakarta : Penerbit Andi.

[2] Menezes, Alfred J., Paul C van Oorschot, dan Scott A. Vanstone. 1996. *Handbook of Applied Cryptography*. CRC Press.

[3] Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Informatika.

[4] Safaat, Nazruddin.2012. *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*. Bandung : Informatika

[5] Schneier, Bruce. 1996. *Aplied Criptography 2nd*,.John Wiley & Sons.

[6] Anjari, Becik Gati. 2012. *Enkripsi SMS (Short Messaging Service) pada Telepon Selular Berbasis Android*. http://www.eepis-its.edu/id/ta/1822/Enkripsi-*SMS*-(short-Message-Service)-Pada-Telepon-Selular-Berbasis-Android (diakses tanggal 25 September 2012).

[7] Dwi, Andi Kurniawan. 2012. *Penerapan Algoritma Vigenere Cipher pada Aplikasi SMS Android*. http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2011-2012/Makalah-2012/Makalah-Kripto-2012-031.pdf (diakses tanggal 18 Oktober 2012).

[8] Pakpahan, Hombar. 2009. *Pengertian SMS*. http://www.ombar.net/2009/09/pengertian-*SMS*.html. (diakses tanggal 11 Oktober 2012)

[9] Wahyunani, Achicha. "Arsitektur Android" http://studyfuture.blogspot.com/2011/03/arsitektur-android.html (diakses pada tanggal 27 Juni 2013)

[10] Wijaya, Chandra Ari., Willya Triana. 2011. *Implementasi Algoritma Twofish untuk Enkripsi dan Dekripsi SMS pada Ponsel Berbasis Android*. http://eprints.mdp.ac.id/401/1/IMPLEMENTASI%20ALGORITMA%20TWOFISH%20UNTUK%20ENKRIPSI%20DAN%20DEKRIPSI%20*SMS*%20PADA%20PONSEL%20BERBASIS%20ANDROID.pdf (diakses tanggal 18 Oktober 2012)