IMPLEMENTASI ENKRIPSI - DEKRIPSI UNTUK FILE GAMBAR DAN TEKS PADA SISTEM OPERASI ANDROID

Sang Putu Krisna Juliana[1], Koredianto Usman[2], Unang Sunarya[3]

[1]Teknik Telekomunikasi, Fakultas Ilmu Terapan, Universitas Telkom

Abstrak

Di era global seperti sekarang ini keamanan sebuah data merupakan suatu hal yang harus diutamakan dalam pertukaran data, khususnya pada data digital seperti gambar dan teks. Karena mungkin saja di dalam gambar dan teks tersebut terdapat informa si pribadi atau rahasia yang tidak boleh sampai diketahui oleh pihak ketiga. Salah satu pertukaran data yang banyak dilakukan yaitu menggunakan perangkat telepon genggam berbasis Android.

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode y ang tidak bisa dimengerti (tidak terbaca). Adapun tujuan dari enkripsi gambar ini agar file yang akan dikirim bisa sampai ke penerima tanpa bisa dilihat oleh pihak lain, dan hanya bisa dilihat jika sudah dilakukan proses dekripsi dengan kata kunci yang sud ah disepakati sebelumnya oleh pihak pengirim dan pihak penerima. Algoritma sandi ini ada yang bersifat kunci - simetris dan ada yang bersifat kunci - asimetris. Skema algoritma sandi ini akan disebut kunci - simetris apabila untuk setiap proses enkripsi maupun dekripsi data secara keseluruhan digunakan kunci yang sama. Salah satu contoh algoritma sandi kunci - simetris adalah stream cipher .

Dalam implementasi enkripsi - dekripsi file gambar dan teks pada android ini memanfaatkan metode stream cipher RC4, percobaan yang sudah dilakukan menunjukkan bahwa gambar yang terenkripsi di pengirim bisa kembali seperti semula pada penerima setelah dilakukan proses dekripsi, rata - rat a waktu proses enkripsi yaitu 1, 027 detik sedangkan rata - rat a waktu proses dekripsi ya itu 1, 035 detik. Dari uji statistik citra asli dengan citra terenkripsi didapa t rata - rata nilai NPCR yaitu 99, 16% sedangka n rata - rata nilai UACI yaitu 34, 67%. Untuk jarak pengiriman antara pengirim dan penerima itu tergantung dar i kualitas sinyal tiap prov ider . Dari hasil perhitungan didapat lama untuk melakukan brute force attack pada aplikasi ini adalah selama 3, 28 x 10 248 tahun.

Kata Kunci : Enkripsi, Dekripsi, Kunci - simetris, Stream Cipher RC4

Abstract

In today's global era of a data security is a matter that should be prioritized in the exchange of data, particularly in the digital data such as images and text. Because it may be in the picture and the text contained personal information or confidential information which should not be until known by a third party. One of the many data exchange is performed using mobile devices based on Android.

Encryption is a process that changes a code of conduct that could be understood to be a code that can not be understood (unreadable). The purpose of encryptio n is that image files can be sent to the recipient without being able to be seen by others, and can only be seen if you've done the decryption process with keywords that have been previously agreed upon by the sender and the recipient. There are algorithms that are password - key and symmetric - key there is asymmetric. This cipher algorithm scheme will be called symmetric if for key - encryption or decryption process any overall data use the same key. While schema password algorithm called asymmetric key - if usin g a different key for encryption and decryption. One example of symmetric - key encryption algorithm is a stream cipher.

In the implementation of encryption and decryption of the image files and text on this android utilizing RC4 stream cipher method, experi ments that have been conducted indicate that the image is encrypted on the sender can go back to normal at the receiver after the decryption process, the average time the encryption process that is 1,027 seconds while the average time is 1,035 seconds decr yption process. Of statistical test image with the original encrypted image obtained average value of NPCR is 99.16% while the average value is 34.67% UACI. For delivery distance between the sender and the receiver depends on the signal quality of each pro vider. Obtained from the calculation of time to do a brute force atta ck on this application is for 3. 28 x 10 248 years.

Keywords : Encryption, Decryption, Key - symmetric, Stream Cipher RC4

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Di era globalisasi seperti sekarang ini, informasi merupakan hal yang sangat dibutuhkan dalam aspek kehidupan setiap manusia. Salah satu informasi yaitu berupa gambar dan teks. Dewasa ini telah terjadi banyak kejahatan di dunia digital khususnya pada perangkat telepon genggam. Banyak gambar dan teks yang sifatnya pribadi yang dimiliki pengguna telepon genggam tersebar luas di jejaring sosial atau dijadikan konsumsi pribadi oleh pihak yang tidak bertanggung jawab. Hal ini bisa terjadi pada saat pengiriman gambar atau teks melalui *email* atau pada saat pertukaran data melalui kartu memori di telepon genggam.

Untuk itulah, perlu dilakukan sebuah pengamanan pada gambar atau teks tersebut. Salah satu contoh pengamanan adalah dilakukannya proses enkripsi gambar dan teks. Ada dua keuntungan yang didapat saat melakukan proses enkripsi gambar dan teks ; yang pertama yaitu jika pengguna melakukan pengiriman data melalui *email*, orang yang menyadap di tengah jalan tidak bisa memahami gambar atau teks tersebut ; yang kedua pada saat kartu memori berpindah tangan, maka pemegang kartu memori yang baru tidak akan bisa melihat gambar yang sudah ter-enkripsi.

Berdasarkan latar belakang diatas maka penulis memiliki inisiatif untuk mengimplementasikan metode enkripsi *cipher* aliran (*stream cipher*) untuk file gambar pada system operasi android. Metode ini dipilih karena algoritma enkripsi menggunakan *stream cipher* lebih sederhana dibandingkan dengan metode yang lain sehingga waktu yang diperlukan untuk proses enkripsi dan dekripsi relatif pendek. Salah satu metode *stream cipher* adalah RC4.

1.2 Tujuan dan Manfaat

Tujuan dan manfaat yang ingin dicapai pada Proyek Akhir ini adalah :

1. Gambar atau teks yang telah dienkripsi di pengirim bisa kembali menjadi bentuk semula setelah dilakukan proses dekripsi di penerima
2. Aplikasi ini dapat membantu seseorang dalam mengamankan file gambar atau teks yang sifatnya pribadi di *smartphone* androidnya
3. Mengetahui performansi aplikasi yang telah dirancang

1.3 Rumusan Masalah dan Batasan Masalah

1.3.1 Rumusan Masalah

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

1. Bagaimana gambar atau teks yang telah dienkripsi di pengirim bisa kembali menjadi bentuk semula setelah dilakukan proses dekripsi di penerima.
2. Bagaimana aplikasi ini dapat membantu seseorang dalam mengamankan file gambar atau teks yang sifatnya pribadi di smartphone androidnya.
3. Bagaimana mengetahui performansi aplikasi yang telah dirancang.

1.3.2 Batasan Masalah

Pengimplementasian aplikasi mengamankan file gambar menggunakan metode *stream cipher* terbatas pada hal-hal 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 kunci simetris RC4.
3. Tidak membahas algoritma kriptografi yang lain.
4. Tidak membahas bagaimana pendistribusian kunci yang digunakan, antara pengirim dan penerima, dengan asumsi kunci yang didistribusikan aman.
5. File gambar memiliki format .PNG dengan warna RGB (*Red Green Blue*) dengan ukuran maksimal 320 x 480 pixel dengan *bit depth* 32 bit.

1.4 Metodologi

Metodologi penyelesaian masalah dalam Proyek Akhir ini adalah sebagai berikut :

1. Studi Literatur

   Mengumpulkan bahan-bahan dan data-data untuk mendapatkan dasar teori yang kuat tentang pembuatan sistem informasi yang berbasis Android serta hal-hal yang berkaitan dengan judul proyek akhir ini.

2. Pengumpulan Data

   Bertujuan untuk pengambilan sampel gambar dan teks.

3. Desain dan Implementasi sistem

   Tahap ini meliputi desain dan pembuatan sistem aplikasi yang telah direncanakan.

4. Pengujian

   Tahap ini akan dilakukan pengujian sistem aplikasi yang dibuat apakah sudah berjalan dengan baik atau tidak.

5. Mengambil Kesimpulan

1.5 Sistematika Penulisan

BAB I Pendahuluan

Menjelaskan tentang latar belakang, perumusan masalah, batasan masalah, tujuan, metode penyelesaian masalah, dan sistematika penulisan proposal proyek akhir.

BAB II Landasan Teori

Menjelaskan tentang dasar-dasar teori yang digunakan dalam pembuatan proyek akhir ini.

BAB III Perancangan Sistem

Menjelaskan tentang perancangan sistem yang akan dibuat serta untuk mendefinisikan kebutuhan dalam pembuatan proyek akhir.

BAB IV Implementasi dan Pengujian

Bab ini membahas mengenai implementasi dan pengujian aplikasi pada *gadget* berbasis Android dan melakukan analisa.

BAB V Kesimpulan dan Saran

Bab ini berisikan kesimpulan akhir mengenai hasil perancangan dan analisa yang diperoleh serta saran dan harapan untuk pengembangan lebih lanjut.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan tujuan yang ingin dicapai pada bab I serta hasil analisa pengujian *alpha* dan *beta* pada bab IV, dapat ditarik beberapa kesimpulan sebagai berikut.

1. Dari pengujian *alpha* disimpulkan bahwa aplikasi dapat dijalankan pada sistem operasi Android, dan gambar atau teks hasil enkripsi di pengirim mampu kembali ke bentuk semula di penerima setelah dilakukan proses dekripsi.
2. Dari hasil pengimplementasian enkripsi dekripsi pada handphone yang berbasis android dengan menggunakan metode stream cipher RC4, aplikasi ini mampu melakukan proses enkripsi dan dekripsi dengan waktu yang relatif cepat. Dimana rata-rata waktu yang diperlukan untuk mengenkripsi 30 sampel pesan adalah 1.027 detik dan rata-rata waktu yang digunakan untuk mendekripsi pesan yang telah di enkripsi adalah 1.037 detik.
3. Dari uji statistik yang telah dilakukan didapat rata-rata nilai NPCR yaitu 99.16% dan nilai UACI yaitu 34.67%, maka dapat ditarik kesimpulan bahwa aplikasi yang dibangun tahan terhadap differential attacks.

5.2 Saran

Saran untuk pengembangan aplikasi :

1. Tambahkan fungsi *Send* pada Halaman Pemrosesan Gambar dan Halaman Pemrosesan Teks agar mempermudah dalam proses pengiriman.
2. Pengembangan aplikasi agar dapat digunakan pada sistem operasi selain android.

DAFTAR PUSTAKA

[1] Dharmaadi, I Putu Arya.2013. *Partially Image Encryption with Combination Method of RC4 Stream Cipher and Chaotic Function*. Bandung : Telkom University.

[2] How do I save an image in external storage gallery in android. http://stackoverflow.com/questions/12967046/how-do-i-save-an-image-in-external-storage-gallery-in-android (diakses 7 September 2013)

[3] H., N. S. 2012. Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android. Bandung: INFORMATIKA.

[4] Ivan Michael Siregar, S. M. (2011). *Membongkar Source Code berbagai Aplikasi Android.* Yogyakarta: GAVA MEDIA.

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

[6] Pengujian Alpha dan Beta pada perangkat lunak. efrylia.files.wordpress.com/2010/05/**pengujian**-pl.pdf (diakses 30 September 2013)

[7] Rukhin, Andrew., et all. 2010. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Special Publication 800-22.

[8] Sutoyo, T., Mulyanto, Edi., Suhartono, Vincent., Nurhayati, O.D., Wijanarto. 2009. *Teori Pengolahan Citra Digital*. Yogyakarta : Andi