Penggabungan Algoritma OTP dan RSA untuk Pengamanan File Text pada Platform Android

Diajukan Sebagai Syarat Untuk Menyelesaikan

Pendidikan Program Strata-1 Pada

Jurusan Teknik Informatika

Oleh :

Muhammad Aldi Riansyah

NIM : 09021381722094

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2022

LEMBAR PENGESAHAN TUGAS AKHIR

Penggabungan Algoritma OTP dan RSA untuk Pengamanan File Text pada Platform Android

Oleh:

Muhammad Aldi Riansyah
NIM: 09021381722094

Pembimbing I	Pembimbing II
Alfarissi, S.Kom., M.Cs.	Kanda Januar Miraswan, M.T.
NIP. 19851215014041001	NIP. 199001090201903 1012

Mengetahui,

Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SKRIPSI

Pada hari Jumat tanggal 22 Juli 2022 telah dilaksanakan ujian sidang skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Muhammad Aldi Riansyah

NIM : 09021381722094

Judul : Penggabungan Algoritma OTP dan RSA untuk Pengamanan *File Text* pada Platform Android.

dan dinyatakan **LULUS**

1. Ketua
   Rizki Kurniati, M.T.
   NIP. 199107122019032016 .....
2. Pembimbing I
   Al Farissi, S.Kom., M.Cs
   NIP. 19851215014041001 .....
3. Pembimbing II
   Kanda Januar Miraswan, M.T
   NIP. 1990010902019031012 .....
4. Penguji I
   Mastura Diana Marieska., M.T
   NIP. 198603212018032001 .....
5. Penguji II
   Muhammad Qurhanul Rizqie., M.T
   NIP. 198712032022031006 .....

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Muhammad Aldi Riansyah
NIM	: 09021381722094
Program Studi	: Teknik Informatika
Judul Skripsi	: Penggabungan Algoritma OTP dan RSA untuk Pengamanan *File Text* pada Platform Android.

Hasil Pengecekan Software *iThenticate/TuritIn* : 17%

Menyatakan bahwa Laporan Projek saya merupakan hasil kerja sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan dari siapapun.

Palembang, Agustus 2022

Muhammad Aldi Riansyah

NIM. 09021381722094

MOTTO DAN PERSEMBAHAN

"Jangan engkau bersedih,

sesungguhnya Allah bersama kita"

-Q.S At-Taubah : 40-

"Sabar Sesaat saja di saat marah

akan menyelamatkan kita dari ribuan penyesalan"

-Ali Bin Abi Thalib-

Kupersembahkan Karya tulis ini kepada :

- *Orangtuaku tercinta dan saudara-saudaraku tercinta*
- *Keluarga besarku*
- *Sahabat-sahabat Tersayangku*
- *Fakultas Ilmu Komputer*
- *Universitas Sriwijaya*

KATA PENGANTAR

Penulis ucapkan syukur kepada Allah atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Skripsi dengan judul **"Penggabungan Algoritma OTP dan RSA untuk Pengamanan *File Text* pada Platform Android"** dengan baik untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin mengucapkan terimakasih kepada pihak-pihak yang telah berperan memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung dalam menyelesaikan tugas akhir ini. Penulis ingin menyampaikan rasa terima kasih kepada :

1. Bapak Jaidan Jauhari, M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya beserta jajarannya. Ibu Alvi Syahrini Utami selaku Ketua Jurusan Teknik Informatika beserta jajarannya, dan Ibu Mastura Diana Marieska selaku Sekretaris Jurusan Teknik Informatika.
2. Bapak Al Farissi., S.Kom., M.Cs selaku pembimbing I dan Bapak Kanda Januar Miraswan, M.T selaku pembimbing II yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
3. Ibu Alvi Syahrini Utami, M.Kom selaku dosen pembimbing akademik, yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Skripsi.
4. Ibu Mastura Diana Marieska, M.T selaku dosen penguji I, dan Bapak Muhammad Qurhanul Rizqie, M.T selaku dosen penguji II yang telah memberikan masukkan dan dorongan dalam proses pengerjaan Skripsi.
5. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Mbak Wiwin, beserta seluruh staf tata usaha yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.
7. Orang tuaku, Endang Yuliani dan Febriansyah Muslimin., S.E, kakakku, dr. Muhammad Aldo Giansyah dan adikku, Alda Shakila Putri yang selalu mendukung dalam pengerjaan

Skripsi. Seluruh keluarga besarku, khususnya Nyai Huzaimah serta Om dan Tante yang selalu mendoakan dan memberikan dukungan baik dalam bentuk moril maupun materil.

8. Sahabat-sahabatku, Muhammad Daffa Nitisastra, Muhammad Hadiidtyariangga, Muhammad Alviansyah Hidayat, yang selalu ada ketika penulis sedang dalam kesusahan.
9. Teman-teman perkumpulan discord “Renoga123”, M. Imam Renaldy Gumay, Berlian M. Naufal, M. Aldi Ariqi, Anang Nugraha, Muhammad Rafly Hafidzin, Adrian Azwaltama, yang telah banyak membantu penulis dalam penulisan Skripsi.
10. Teman-temanku kelas “Tibil Baper 17” dan jurusan Teknik Informatika yang telah membuat hidup penulis menjadi lebih berwarna selama perkuliahan.
11. Seluruh pihak yang telah membantu dalam penyusunan dan penyempurnaan Skripsi ini yang tidak dapat disebutkan satu persatu

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Skripsi ini dapat bermanfaat bagi kita semua.

Palembang, Agustus 2022

Muhammad Aldi Riansyah

Combining OTP and RSA Algorithms for Text File Security on the Android Platform

By :

Muhammad Aldi Riansyah

NIM. 09021381722094

ABSTRACT

In this era of rapidly developing technology and information, there are many security applications developed to prevent these threats, but there are still those applications that have not applied security techniques to the application so that the files stored in the application are not guaranteed security. The focus of this research is to develop a security scheme for securing text on the Android platform by applying a combination of the OTP (One-Time Pad) and RSA (Rivest Shamir Adleman) algorithms so that the files stored can be guaranteed security. The files to be tested are .txt type files total of 4 files. After the security process is carried out, the next scheme is to test the level of security based on the Avalanche Effect Value. From the test results, it can be concluded that the combination of the OTP (One-Time Pad) and RSA (Rivest Shamir Adleman) is considered not good enough to be applied to securing the text files becuase the resulting Avalanche Effect value is stable at 33%.

Keywords: File Security, OTP, RSA (Rivest Shamir Adleman), Avalanche Effect

Palembang, Agustus 2022

Pembimbing I	Pembimbing II
Alfarissi, S.Kom., M.Cs.	Kanda Januar Miraswan, M.T.
NIP. 19851215014041001	NIP. 199010902019031012

Mengetahui,

Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.

NIP. 197812222006042003

Penggabungan Algoritma OTP dan RSA untuk Pengamanan *File Text* Pada Platform Android

Oleh :

Muhammad Aldi Riansyah

NIM. 09021381722094

ABSTRAK

Pada era teknologi dan informasi yang berkembang pesat ini sangat banyak aplikasi pengamanan yang dikembangkan untuk mencegah ancaman tersebut, tetapi masih ada aplikasi yang belum menerapkan teknik pengamanan pada aplikasinya sehingga file yang disimpan pada aplikasi tersebut tidak terjamin keamanannya. Fokus pada penelitian ini adalah mengembangkan skema pengamanan pada pengamanan file text pada platform android dengan menerapkan penggabungan algoritma OTP (*One-Timed Pad*) dan RSA (Rivest Shamir Adleman) sehingga file yang disimpan dapat terjamin keamanannya. *File* yang akan diuji berupa *file* bertipe .txt berjumlah 4 *file*. Setelah proses pengamanan dilakukan, selanjutnya skema yang dilakukan adalah dengan menguji tingkat keamanannya berdasarkan nilai *Avalanche Effect*. Dari hasil pengujian dapat disimpulkan bahwa penggabungan algoritma OTP (*One-Timed Pad*) dan RSA (Rivest Shamir Adleman) dinilai kurang baik untuk diterapkan pada pengamanan file text dikarenakan nilai *Avalanche Effect* yang dihasilkan stabil diangka 33%.

Kata Kunci: Pengamanan *file*, OTP, RSA (Rivest Shamir Adleman), Avalanche Effect

Palembang, Agustus 2022

Pembimbing I	Pembimbing II
Alfarissi, S.Kom., M.Cs.	Kanda Januar Miraswan, M.T.
NIP. 19851215014041001	NIP. 199010902019031012

Mengetahui,

Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.

NIP. 19781222200604200

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab ini akan menjelaskan tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, dan batasan masalah yang ada, serta menjelaskan tentang keseluruhan penelitian. Pendahuluan dimulai dengan penjelasan mengenai latar belakang masalah dimana algoritma yang digunakan dapat menyelesaikan kasus pada Pengabunggan algoritma dengan menerapkan OTP dan RSA yang menjadi latar belakang pada penelitian ini.

1.2 Latar Belakang

Dengan pesatnya kemajuan teknologi di dunia ini, memberikan kemudahan bagi setiap pihak untuk melakukan pertukaran informasi. Namun, kemajuan teknologi ini juga memberikan ancaman karena banyak pihak yang tidak berwenang berusaha untuk mengambil informasi tersebut untuk kepentingan mereka masing-masing atau untuk organisasi. Untuk mengatasi ancaman ini, banyak pihak yang berusaha untuk menyandikan informasi yang mereka miliki sehingga informasi tersebut tidak memiliki makna dan sulit untuk dipecahkan. Salah satu metode yang dapat diterapkan dalam menyandikan informasi tersebut adalah metode kriptografi.

Kriptografi merupakan metode untuk mengamankan data, baik berupa teks maupun gambar. Metode ini dilakukan dengan melakukan penyandian pesan kedalam bentuk yang tidak dipahami oleh pihak ketiga (Waruwu & Telaumbanua, 2016). Pada menjaga keamanan sebuah pesan, kriptografi mengubah pesan asli (*plaintext*) ke dalam bentuk pesan tersandi (*ciphertext*). Untuk mengubah suatu file agar tidak dapat dibaca, dilakukan suatu proses yaitu enkripsi. Enkripsi dapat mengubah pesan menjadi sebuah sandi tersebut sehingga tidak dapat diketahui

dan dipahami isinya oleh pihak yang tidak memiliki kewenangan. Untuk mengembalikan pesan yang telah terenkripsi sebelumnya, dilakukan suatu proses yaitu dekripsi.

Terdapat dua algoritma kriptografi yaitu algoritma kunci simetris dan algoritma kunci asimetris. Algoritma simetris menggunakan satu kunci yang sama dalam proses enkripsi dan dekripsinya sedangkan algoritma asimetris menggunakan kunci yang berbeda pada proses enkripsi dan dekripsi. Adapun algoritma yang diambil peneliti adalah OTP *Cipher* sebagai algoritma simetris dan RSA sebagai algoritma asimetris.

Pada penelitian Saragih (2018) digunakan algoritma OTP sebagai algoritma enkripsi dan dekripsi yang digunakan pada platform android, dimana hasilnya menunjukkan bahwa algoritma OTP sangatlah aman digunakan karena kunci yang digunakan hanyalah satu kali. Kemudian pada penelitian Agustina, dkk (2017) digunakan algoritma RSA sebagai algoritma enkripsi dan dekripsi juga yang diimplementasikan pada platform web, dimana hasilnya menunjukkan bahwa semakin besar ukuran file yang digunakan, maka semakin lama proses file terenkripsi.

Pada tugas akhir ini, peneliti akan melakukan penggabungan pada algoritma OTP dan RSA untuk mengamankan file text pada platform android. Penggabungan kedua algoritma tersebut diharapkan mendapatkan algoritma yang mudah dipahami dan efektif untuk diterapkan pada platform android, khususnya untuk mengamankan file text yang ukurannya tidak terlalu besar. Kemudian diharapkan kedua algoritma ini dapat menghasilkan tingkat keamanan yang tinggi, namun memiliki proses eksekusi yang tidak lama dan penggunaan memori yang seminimum mungkin.

1.3 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah dari penelitian ini adalah bagaimana mengembangkan penggabungan OTP dan RSA untuk pengamanan file text yang

akan diimplementasikan pada platform Android, serta bagaimana tingkat keamanan yang dihasilkan dari penggabungan algoritma OTP dan RSA tersebut.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Merancang dan membangun perangkat lunak pengamanan file text menggunakan penggabungan algoritma OTP dan RSA pada platform Android.
2. Menguji tingkat keamanan file text yang telah terenkripsi.

1.5 Manfaat Penelitian

Adapun manfaat pada penelitian ini adalah sebagai berikut :

1. Membuat skema pengamanan *file* menggunakan penggabungan algoritma OTP (*One-Time Pad*) dan RSA (Rivest Shamir Adleman) untuk pengamanan *file text* pada platform Android
2. Memudahkan pengguna platform Android untuk menyimpan *file text* dengan aman.
3. Mengetahui tingkat keamanan dari skema yang telah dikembangkan.

1.6 Batasan Masalah

Batasan – batasan yang ditetapkan dalam pengembangan perangkat lunak untuk enkripsi gambar, antara lain :

1. Aplikasi berjalan pada *Smartphone* dengan *Operating System Android*.
2. File yang dapat dienkripsi hanyalah file berjenis .txt
3. Untuk melakukan dekripsi, pengguna harus menggunakan aplikasi ini.

1.7 Sistematika Penulisan

Sistematika penulisan tugas akhir ini akan mengikuti standar penulisan tugas akhir Fakultas Ilmu komputer adalah sebagai berikut :

BAB I. PENDAHULUAN

Pada bab ini, diuraikan mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah/ruang lingkup, metodologi penelitian, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini, akan membahas dasar – dasar teori yang digunakan dalam penelitian, seperti definisi sistem, informasi, dan semua yang digunakan pada tahapan analisis, perancangan, dan implementasi metode.

BAB III. METODOLOGI PENELITIAN

Pada bab ini, akan membahas mengenai tahapan yang akan dipakai pada penelitian. Setiap rencana dari tahapan penelitian dideskripsikan secara rinci dengan berdasar pada kerangka kerja.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini, akan diurai tahapan-tahapan yang dilaksanakan dalam proses pengembangan perangkat lunak pengamanan *file text* berbasis Android dengan menggunakan metode *Ration Unified Process* (RUP).

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada bab ini, akan diuraikan mengenai hasil dan analisis penelitian dari pengembangan perangkat lunak yang telah dilaksanakan pada bab IV.

BAB VI. KESIMPULAN DAN SARAN

Pada bab ini, akan diuraikan mengenai kesimpulan dan saran untuk penelitian selanjutnya yang mengacu dari hasil dan analisis penelitian yang telah dilaksanakan.

1.8 Kesimpulan

Proses pertukaran data, terkhususnya gambar semakin banyak. Untuk menjaga keamanan informasi, kriptografi dapat dilakukan. Enkripsi dan dekripsi adalah hal yang penting dalam kunci kriptografi. Kunci pada kriptografi adalah kunci simetri dan kunci asimetri. Dalam penelitian ini, peneliti mencoba menggabungkan OTP dan RSA dalam meng-enkripsi file text.

DAFTAR PUSTAKA

Agustina, A. N., Aryanti, & Nasron. (2017). Pengamanan Dokumen Menggunakan Kombinasi Metode Rsa (Rivest Shamir Adleman) Dan Vigenere Cipher. *Prosiding Seminar Nasional Multi Disiplin Ilmu & Call For Papers UNISBANK*, 14–19.

Anwar, S., Nugroho, I., & Lestariningsih, E. (2013). Perancangan Dan Implementasi Aplikasi Mobile Semarang Guidance Pada Android. *Dinamik*, *20*(2), 243541.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi Dan Sistem Komputer*, *3*(2), 253. https://doi.org/10.14710/jtsiskom.3.2.2015.253-258

Manurung, J., Sirait, K., Panggabean, J. F., & Komputer, D. (2018). Penerapan Algoritma Rsa Untuk Pengamanan File. *Terakreditasi DIKTI*, *2*(2), 112–116.

Saragih, N. E. (2018). Implementasi Algoritma One Time Pad pada(Nidia Enjelita Saragih). *Jurnal Ilmiah MATRIK*, *Vol.20 No.*(3), 31–40.

Toyib, R., & Darnita, Y. (2020). Pengamanan Data Teks Dengan Menggunakan Algoritma Zero-Knowledge Proof. *Jurnal Media Infotama*, *16*(1), 16–23. https://doi.org/10.37676/jmi.v16i1.1114

Waruwu, T. S., & Telaumbanua, K. (2016). Kombinasi Algoritma OTP Cipher dan Algoritma BBS dalam Pengamanan File. *JSM STMIK Mikroskil*, *17*(1), 119–126.