PENGAMANAN FILE TEKS PADA APLIKASI MEMO MENGGUNAKAN VIGENERE CIPHER DAN RSA BERBASIS ANDROID

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh :

M. Rizqi Nur Iman
NIM : 09021381722136

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2022

LEMBAR PEGESAHAN SKRIPSI

Pengamanan File Teks Pada Aplikasi Memo Menggunakan Vigenere Cipher dan RSA Berbasis Android

Oleh:

M. Rizqi Nur Iman
NIM: 09021381722136

Palembang, Juli 2022

Pembimbing I,	Pembimbing II
Al Farissi, S.Kom, M.Cs.	Osvari Arsalan, S.Kom, M.T
NIP.198512152014041001	NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP 197812222006042003

TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari Senin tanggal 25 Juli 2022 telah dilaksanakan ujian sidang skripsi oleh jurusan Teknik Informatika Universitas Sriwijaya

Nama : M. Rizqi Nur Iman
Nim : 09021381722136
Judul : Pengamanan File Teks Pada Aplikasi Memo menggunakan Vigenere Cipher dan RSA Berbasis Android

Dan dinyatakan **LULUS**

1. Ketua Penguji

Yunita M. Cs.
NIP. 198306062015042002

2. Penguji 1

Mastura Diana Marieska, M.T
NIP. 198603212018032001

3. Penguji 2

Desty Rodiah, M.T
NIP. 198912212020122011

4. Pembimbing 1

Al Farissi, S.Kom., M.Cs.
NIP. 198512152014041001

5. Pembimbing 2

Osvari Arsalan,S.Kom., M.T
NIP. 198806282018031001

Mengetahui,

Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: M. Rizqi Nur Iman
Nim	: 09021381722136
Judul	: Pengamanan File Teks Pada Aplikasi Memo Menggunakan Vigenere Cipher dan RSA Berbasis Android
Hasil Pengecekan Software iThenticate/Turnitin	:18%

Menyatakan laporan Proyek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan ini, maka saya akan bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapa pun.

Palembang, Juli 2022

M. Rizqi Nur Iman

NIM.09021381722136

MOTTO DAN PERSEMBAHAN

Motto :

“Maka sesungguhnya bersama kesulitan itu ada kemudahan.Sesungguhnya bersama kesulitan itu ada kemudahan” – Q.S. Al Insyirah : 5-6

“I hated every minute of training, but I said, ‘Don’t quit. Suffer now and live the rest of your life as a champion.” – Muhammad Ali

“If you can’t fly, then run, if you can’t run then walk if you can’t walk then crawl, but whatever you do you have to keep moving forward” - Martin Luther King, Jr.

"I can accept failure, everyone fails at something. But I can't accept not trying." – Michael Jordan

Kupersembahakan karya tulis ini kepada :

- Allah SWT
- Diri Sendiri
- Orang Tua
- Keluarga Besarku
- Teman - teman seperjuanganku
- Dosen Pembimbing
- Fakultas Ilmu Komputer, Universitas Sriwijaya

Text Files Security on Android Based Memo Application

Using Vigenere Cipher and RSA

By :

M. Rizqi Nur Iman

Nim. 09021381722136

ABSTRACT

The smartphone is a device that cannot be separated from human daily life and *Android* smartphones are the most widely used in Indonesia. According to Kominfo, 66.31% of Indonesians are use *Android*-based smartphones in 2017. With smartphones there are many things that can be done, such as write down the important personal notes on the memo. However, 67% of smartphone users have experienced personal data theft. Therefore, in order to reduce this an *Android*-based software was developed to store memos by applying the *Vigenere cipher* and RSA cryptographic algorithms. In this device RSA is used in passwords and will generate *ciphertext* and then used as a key for *Vigenere cipher* in securing text *file*s. This software security was tested by using the Avalanche Effect. The security testing is performed on text *file*s that have a .txt format and have a size of 400B-100KB. This security test is also carried out under several conditions, namely on original *file*s, *file*s that have changed the initial, middle, and final letters, as well as the same *file* but using a different password. Based on the security test, the Avalanche Effect value is 50%. So it can be concluded that the algorithm in the study is good because it is in accordance with the Avalanche Effect standard.

Keywords: *Avalanche Effect, Cryptography, Memo, RSA, Smartphone, Vigenere cipher.*

Palembang, Juli 2022

Pembimbing 1,	Pembimbing 2,
Al Farissi, S.Kom., M.Cs.	Osvari Arsalan,S.Kom., M.T
NIP. 198512152014041001	NIP. 198806282018031001

Mengetahui,

Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.

NIP. 197812222006042003

Pengamanan File Teks Pada Aplikasi Memo Menggunakan Vigenere Cipher dan RSA Berbasis Android

Oleh:

M. Rizqi Nur Iman

Nim. 09021381722136

ABSTRAK

Smartphone merupakan perangkat yang tak lepas dari kehidupan sehari-hari manusia saat ini dan *smartphone Android* merupakan yang banyak dipakai di Indonesia. Menurut Kominfo sebanyak 66,31% masyarakat Indonesia menggunakan *smartphone* berbasis *Android* pada tahun 2017. Dengan *smartphone* banyak hal yang dapat dilakukan, mencatat catatan pribadi yang penting pada memo salah satunya. Namun sebanyak 67% pengguna *smartphone* telah mengalami pencurian data pribadi. Maka dari itu untuk mengurangi hal tersebut dikembangkanlah perangkat lunak yang berbasis *Android* untuk menyimpan memo dengan menerapkan algoritma kriptografi *Vigenere cipher* dan RSA. Pada perangkat ini RSA digunakan pada *password* dan akan menghasilkan *ciphertext* yang kemudian digunakan sebagai kunci untuk *Vigenere cipher* dalam mengamankan *file* teks. Perangkat lunak ini diuji keamanannya menggunakan *Avalanche Effect*. Pengujian keamanan dilakukan pada *file* teks yang memiliki format .txt dan berukuran 400B-100KB. Pengujian keamanan ini juga dilakukan pada beberapa kondisi yaitu pada *file* asli, *file* yang telah diubah huruf awal, tengah, akhir, serta *file* yang sama namun menggunakan *password* yang berbeda. Berdasarkan pengujian keamanan tersebut dihasilkan nilai *Avalanche Effect* sebesar 50%. Sehingga disimpulkan bahwa algoritma pada penelitian sudah baik karena sudah sesuai dengan standar *Avalanche Effect*.

Keywords: *Avalanche_Effect*, Kriptografi, Memo, RSA, *Smartphone*, *Vigenere cipher*

Palembang, Juli 2022

Pembimbing 1,

Al Farissi, S.Kom., M.Cs.
NIP. 198512152014041001

Pembimbing 2,

Osvari Arsalan, S.Kom., M.T
NIP. 198806282018031001

Mengetahui,

Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

KATA PENGANTAR

Bismillahirrahmamanirrahim, puji syukur penulis panjatkan kepada Allah SWT atas segala rahmatNya sehingga penulis dapat menyelesaikan penyusunan skripsi ini berjudul "**Pengamanan File Teks Pada Aplikasi Memo Menggunakan Vigenere Cipher dan RSA Berbasis Android**". Skripsi ini disusun dan diajukan untuk memenuhi syarat perolehan gelar sarjana (S.Kom) pada Fakultas Ilmu Komputer Universitas Sriwijaya. Untuk selanjutnya penulis mengucapkan banyak terima kasih kepada pihak-pihak yang telah banyak membantu dalam penyelesaian skripsi ini, antara lain:

1. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
2. Ibu Alvy Syahrini Utami, M.Kom, selaku ketua jurusan Teknik Informatika
3. Bapak Al Farissi, S.Kom., M.Cs. dan bapak Osvari Arsalan,S.Kom., M.T selaku pembimbing penulis yang telah banyak membantu, mengarahkan dan membimbing dan memberikan saran untuk menyelesaikan skripsi ini.
4. Ibu Mastura Diana Marieska, M.T dan Ibu Desty Rodiah, MT selaku penguji skripsi yang telah memberikan saran agar skripsi ini menjadi lebih baik lagi.
5. Seluruh Dosen Teknik Informatika Universitas Sriwijaya yang pernah mengajar penulis dari awal semester hingga akhir semester.
6. Kedua orang tuaku dan adikku yang telah sangat membantu penulis, selalu mendoakan dan selalu memberi motivasi agar terus semangat dalam mengerjakan skripsi.
7. Keluarga besar juga yang selalu mendoakan dan selalu memotivasi agar penulis bersemangat dalam mengerjakan skripsi.
8. Teman-temanku, M. Aldi Ariqi, Muhammad Rafly Hafizin, Rezki Adina, dan Anang Nugraha yang telah meluangkan waktu untuk membantu dalam penyelesaian skripsi ini.
9. Seluruh teman-teman di Kelas TI Bil B 2017, yang telah menemani suka dan duka selama masa perkuliahan.

Palembang, Juli 2022

M. Rizqi Nur Iman

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini akan memberikan penjelasan mengenai latar belakang penelitian dengan topik "Pengamanan *file* teks pada aplikasi memo menggunakan *Vigenere cipher* dan RSA berbasis *android*" serta penjelasan umum mengenai keseluruhan penelitian yang mencakup tujuan penelitian, manfaat penelitian yang akan dilaksanakan dan batasan masalah dari penelitian.

1.2 Latar Belakang

Perkembangan teknologi yang terjadi sekarang ini semakin memudahkan manusia dalam beraktivitas sehari – hari, salah satunya *smartphone* yang menjadi alat yang tak bisa dipisahkan dari manusia. Banyak jenis sistem operasi yang dapat menjalankan sebuah *smartphone*, salah satunya *Android*. *Android* merupakan sistem operasi *smartphone* yang paling banyak digunakan di dunia, di Indonesia 66,31% masyarakatnya menggunakan *smartphone* (Kominfo,2017). Dengan *smartphone* manusia dapat dipermudah kegiatannya dengan beragam aplikasi yang tersedia, contohnya mencatat. Sekarang mencatat sesuatu dapat dilakukan secara digital dan memo dapat menjadi sarana mencatat tersebut.

Kita dapat mencatat hal - hal penting dan bersifat rahasia dalam aplikasi memo, tetapi pencurian data pada *smartphone* telah banyak terjadi. Sebanyak 67% pengguna *smartphone* telah mengalaminya pencurian data pribadi mereka(Akraman & Priyadi, 2018). Maka dari itu dibutuhkan pengamanan pada aplikasi smartphone yang dapat mengamankan data pengguna, dalam hal ini

pengamanan pada aplikasi memo. Pengamanan itu bisa dilakukan dengan kriptografi, kriptografi terdiri dari algoritma kriptografi kunci simetri, asimetri dan *hybrid*, kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang mempunyai pengertian dengan cara menyamarkannya (mengacak) menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu, dengan pengamanan menggunakan kriptografi kemungkinan data dicuri dari smartphone akan berkurang.

Vigenere cipher merupakan salah satu algoritma kriptografi simetris berjenis *Polyalphabetic Substitution Cipher*, yang memproses informasi dalam bentuk teks antara teks informasi pesan dan teks kata kunci yang dipopulerkan oleh Blaise de Vigenere 1586. Algoritma ini merupakan algoritma kriptografi yang cukup kuat pada masanya dan bertahan cukup lama hingga pada tahun 1917 berhasil dipecahkan oleh Friedman dan Kasiski, maka dari itu modifikasi dan pengembangan dari *Vigenere cipher* dapat dilakukan untuk meningkatkan kekuatannya(Ardhianto et al., 2021). Salah satu cara meningkatkan kekuatan *Vigenere cipher* dengan menggunakan tabel ASCII, yang *key*-nya sebanyak 256 karakter sehingga hasil enkripsinya relatif lebih aman dibanding dengan *Vigenere cipher* alfabet biasa (26 karakter) (Hidayatulloh et al., 2015). Untuk meningkatkan lagi tingkat keamanan dari *Vigenere cipher* maka algoritma ini juga dapat digabungkan dengan algoritma kriptografi asimetri.

RSA (Rivest Shamir Adleman) merupakan algoritma asimetri dengan berdasar pada konsep bilangan prima dan aritmatika modulo. RSA memiliki keamanan yang terletak pada tingkat kesulitan dalam memfaktorkan bilangan nonprima menjadi

faktor primanya. Dalam dekripsinya untuk menemukan kunci dekripsinya dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya yang tidak mudah untuk dilakukan karena belum adanya algoritma yang efisien untuk melakukan pemfaktoran. Cara yang bisa digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor. Semakin besar bilangan yang akan difaktorkan, maka semakin lama waktu yang dibutuhkan. Jadi semakin besar bilangan yang difaktorkan membuat semakin sulit pemfaktorannya, maka semakin kuat pula algoritma RSA. Selagi belum ada algoritma yang efisien untuk memfaktorkan bilangan bulat menjadi faktor primanya, maka algoritma RSA tetap direkomendasikan untuk menyandikan dan tetap dapat dipakai. (Ginting et al., 2015).

Dalam penggunaannya *plaintext* yang digunakan untuk enkripsi dengan RSA berupa angka-angka, sedangkan *file* teks yang digunakan biasanya berbentuk tulisan, sehingga *file* teks tersebut diubah dari *file* teks berupa tulisan menjadi bilangan menggunakan ASCII (*American Standard Code for Information Interchange*) (Ginting et al., 2015).

Berdasarkan penjelasan yang telah diuraikan di atas, agar kekuatan algoritma *Vigenere cipher* untuk mengamankan *file* teks bertambah penulis memilih *Vigenere cipher*, sebuah *Polyalphabetic Substitution Cipher* yang memproses informasi dalam bentuk teks antara teks informasi pesan dan teks kata kunci bersama RSA yang memiliki keamanan yang terletak pada tingkat kesulitan dalam memfaktorkan bilangan nonprima menjadi faktor primanya untuk digunakan

dalam membangun aplikasi memo untuk mengamankan *file* teks dengan basis *Android.*

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah diberikan sebelumnya, permasalahan yang muncul adalah bagaimana tingkat pengamanan *file* teks pada aplikasi memo dengan algoritma *Vigenere cipher* dan RSA.

1.4 Tujuan Penelitian

Tujuan penelitian ini dilakukan adalah sebagai berikut :

1. Melakukan pengamanan pada data berupa teks berformat *.txt dengan menggunakan algoritma *Vigenere cipher* dan RSA.
2. Membangun aplikasi Memo yang memiliki pengamanan data berupa teks berformat *.txt dengan menggunakan algoritma *Vigenere cipher* dan RSA.
3. Menguji *Avalanche Effect* pada proses enkripsi dan dekripsi menggunakan algoritma *Vigenere cipher* dan RSA.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah dapat membantu mengamankan data pengguna dari pencurian informasi dan dapat dijadikan acuan untuk penelitian selanjutnya

1.6 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut :

1. Aplikasi hanya melakukan pengamanan pada data berupa *file* *.txt.
2. Pengaman dilakukan pada *file* dengan ukuran 400B – 100KB
3. Penelitian ini hanya dilakukan dengan menggunakan basis *Android*.

1.7 Sistematika Penulisan

Sistematika penulisan dari penelitian sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini akan dijelaskan mengenai latar belakang, rumusan masalah, tujuan, manfaat, batasan penelitian dan sistematika penulisan dari penelitian dengan judul Pengamanan *File* Teks Menggunakan *Vigenere cipher* dan RSA Berbasis *Android*

BAB II TINJAUAN PUSTAKA

Pada bab ini berisikan penjelasan landasan teori dari penelitian yang dilakukan mengenai *Vigenere cipher*, RSA, *Avalanche Effect*, *Android*, Memo, dan penelitian terkait terdahulu.

BAB III METODELOGI PENELITIAN

Pada bab ini akan membahas setiap tahapan pada penelitian yang dilakukan, pengumpulan data yang digunakan untuk penelitian, dan metode pengembangan yang dipakai pada penelitian.

BAB IV REKAYASA PERANGKAT LUNAK

Pada bab ini berisi uraian dari tahapan-tahapan yang dilakukan dalam proses mengembangkan perangkat lunak pengamanan *file* teks dengan basis *Android* dengan menggunakan metode RUP (*Rational Unified Process*) dengan pemodelan UML (*Unified Modeling Language*).

BAB V HASIL DAN ANALISIS PENELITIAN

Pada bab ini akan dijelaskan hasil beserta analisis penelitian dari perangkat lunak yang telah dikembangkan pada bab sebelumnya.

BAB VI KESIMPULAN DAN SARAN

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

1.8 Kesimpulan

Bab ini telah menjelaskan mengenai latar belakang permasalahan yang akan dilakukan yaitu mengenai pengaman pada aplikasi memo menggunakan algoritma berbasis *android*.

DAFTAR PUSTAKA

Akraman, R., & Priyadi, Y. (2018). *Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna Smartphone Android di Indonesia*. *02*, 115–122.

Anggreni, N. K. A. S., Linawati, & Sastra, I. N. P. (2019). *Sistem Pengamanan Anonym dengan Menggunakan Algoritma Kriptografi ElGamal*. *18*(2).

Ardhianto, E., Handoko, W. T., & ensial, E. S. H. (2021). *Evolusi Cipher Vigenere dalam Peningkatan Pengamanan Informasi*. *7*(2), 1–5.

Ariqi, A. (2021). *Hybrid Cryptosystem menggunakan Blowfish dan RSA (Rivest Shamir Adleman) untuk Penyimpanan Online Berbasis Android*.

Ependi, U., Kunang, Y., & Novifika, S. (2014). Implementasi Metode Rational Unified Process Pada Mobile Digital Library. *Jurnal Ilmiah Matrik*, *03*, 35–44.

Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). *Implementasi Algoritma Kriptografi RSA untuk*. *3*(2), 253–258.

Harahap, M. K. (2016). Analisis Perbandingan Algoritma Kriptografi Klasik *Vigenere cipher* Dan One Time Pad. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *1*(1), 61–64. https://doi.org/10.30743/infotekjar.v1i1.43

Hidayatulloh, M., Insannudin, E., & Kunci, K. (2015). *Enkripsi Dan Dekripsi Menggunakan Vigenere cipher Ascii Java*.

Irawan, M. D. (2017). Implementasi Kriptografi *Vigenere cipher* Dengan Php. *Jurnal Teknologi Informasi*, *1*(1), 11. https://doi.org/10.36294/jurti.v1i1.21

Kang, H., & Cho, J. (2015). *Case Study on Efficient Android Programming Education using Multi Android Development Tools*. *8*(August), 1–5. https://doi.org/10.17485/ijst/2015/v8i

Kharisma, R. S., Aziz, M., & Rachman, F. (2017). *Pembuatan Aplikasi Notes Menggunakan Substitution Cipher Kombinasi Kode ASCII dan Operasi Xor Berbasis Android*. *XII*, 1–7.

Mardianti, M., Sutardi, & Aksara, L. M. F. (2019). Keamanan dan penyisipan pesan teks pada gambar dengan kriptografi metode Hill Cipher dan Steganografi metode END of *FILE*. *SemanTIK*, *5*(1), 185–194.

Muhammad Ardhi Prakasa, Rita Magdalena, R. Y. N. F. (2018). *Steganografi Discrete Wavelet Transform Dan Algoritma Kriptografi*. *September*, 151–159.

Novitasari, O. (2017). *Implementasi Rational Unified Process Pada Sistem*

Informasi Simpan Pinjam Kelompok Perempuan. *2016*, 126–129.

Pahrizal, & Pratama, D. (2016). *Implementasi Algoritma RSA Untuk Pengamanan Data Berbentuk Teks*. *III*, 44–49.

Permana, A. A. (2018). *Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode*. *4*(3), 110–115.

Rachman, F. (2018). *Perancangan Aplikasi Memo Menggunakan Algoritma Kriptografi Caesar Cipher Dan RSA Berbasis Android*. 121–127.

Sri Anggreni, N. K. A. L., & Putra Sastra, I. N. (2019). *Sistem Pengamanan Anonym dengan Menggunakan*. *18*(2).

Syawal, M. F., Fikriansyah, D. C., & Agani, N. (2016). *Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere cipher Dan Metode LSB*. *4*(3).

Tia, T. K., & Kusuma, W. A. (2018). Model Simulasi Pengembangan Perangkat Lunak Menggunakan Rational Unified Process (Rup). *Teknika: Engineering and Sains Journal*, *2*(1), 33. https://doi.org/10.51804/tesj.v2i1.226.33-40

Vekariya, M. (2015). Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms. *International Journal of Computer Engineering and Sciences*, *1*(1), 1. https://doi.org/10.26472/ijces.v1i1.20