NUANSA INFORMATIKA ***p-ISSN :1858-3911* , *e-ISSN : 2614-5405***
Volume 18 Nomor 2 Juli 2024 https://journal.fkom.uniku.ac.id/ilkom

Perancangan Aplikasi Enkripsi Dan Dekripsi Gambar Cetak Biru Pada PT. Patco Elektronik Teknologi Menggunakan Algoritma *RSA* Berbasis Android

Arafat Bagoes Setyawan[1], Muhammad Khaerudin [2], Siti Setiawati [3]
Program Studi Informatika, Fakultas Ilmu Komputer
Universitas Bhayangkara Jakarta Raya
E-mail:
[1]arafatsetyawan08@gmail.com,[2]muhammad.kherudin@dsn.ubharajaya.ac.id,[3]siti.setiawati@dsn.ubharajaya.ac.id

Abstrak

PT. Patco Elektronik Teknologi adalah perusahaan terkemuka dalam industri Elektronik, menghadapi kebutuhan mendesak untuk meningkatkan keamanan data cetak biru (blueprint) mold di divisi Moldshop. Proses perbaikan mold melalui mesin CNC memerlukan akses yang aman terhadap gambar cetak biru standar perusahaan. Oleh karena itu, penelitian ini bertujuan untuk merancang aplikasi enkripsi dan dekripsi file gambar cetak biru berbasis Android menggunakan algoritma Rivest Shamir Adleman. Serta mengidentifikasi keterbatasan anggaran, ketersediaan perangkat Android, dan keamanan data sebagai permasalahan utama yang harus diatasi. Metode yang digunakan pada penelitian ini yaitu Rivest Shamir Adleman salah satu dari metode kriptografi asimetris yang paling terkenal dan banyak digunakan, untuk penelitian ini algoritma Rivest Shamir Adelman akan diterapkan ke dalam program android sebagai enkripsi dan dekripsi gambar cetak biru. Studi ini menghasilkan aplikasi berbasis Android bernama Rivest Shamir Adleman yang berhasil dirancang untuk melakukan enkripsi dan dekripsi file gambar cetak biru. Aplikasi tersebut tidak hanya dirancang tetapi juga berhasil dibangun dan diuji, hasil pengujian menunjukkan bahwa program ini dapat dengan cepat enkripsi dan dekripsi file gambar cetak biru, dengan hasil rata-rata 4-15 detik saat menggunakan metode Rivest Shamir Adlemen. dan pada saat dekripsi mendapatkan hasil 2-5 Detik. Dengan menggunakan algoritma Rivest Shamir Adlemen untuk enkripsi dan dekripsi, file gambar cetak menjadi biru dapat diamankan dengan tingkat keamanan yang tinggi.
Kata Kunci*— Kriptografi, Rivest Shamir Adleman, Android.*

Abstract

PT. Patco Elektronik Teknologi, a leading company in the Electronics industry, urgently needs to enhance the security of blueprint mold data in its Moldshop division. The process of mold repair using CNC machines requires secure access to the company's standard blueprint drawings. Hence, this study aims to develop an Android-based application for encrypting and decrypting blueprint images using the Rivest Shamir Adleman algorithm. It also addresses challenges such as budget constraints, Android device availability, and data security. The method chosen, Rivest Shamir Adleman, is renowned for its asymmetric cryptography and will be implemented in the Android application for securing blueprint images. The research successfully resulted in the creation, implementation, and testing of the Rivest Shamir Adleman Android application. Testing demonstrated that the program can efficiently encrypt and decrypt blueprint images, with encryption averaging 4 to 15 seconds and decryption 2 to 5 seconds using this method. By employing Rivest Shamir Adleman, the application ensures high-level security for blueprint image files
Keywords*— Cryptography, Rivest Shamir Adleman, Android*

Diajukan: 7 Mei 2024 *Disetujui: 3 Juli 2024* *Dipublikasi: 20 Juli 2024*

1. PENDAHULUAN

PT. Patco Elektronik Teknologi merupakan industri elektronik yang mengkhususkan diri dalam produksi printer dan peralatan perawatan kesehatan, menghadapi tantangan signifikan dalam memastikan keamanan dan kerahasiaan data vital mereka. Di dalam struktur organisasi PT. Patco Elektronik Teknologi, terdapat sebuah divisi kunci yang

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

berperan penting dalam memastikan kualitas produk mereka, yaitu Moldshop. Divisi ini bertanggung jawab untuk melakukan persiapan dan perbaikan terhadap cetakan (mold) yang menjadi inti dari produksi perusahaan. Proses perbaikan cetakan melibatkan penggunaan teknologi mutakhir, terutama mesin CNC yang dioperasikan oleh operator Moldshop.

Saat ini yang terjadi di PT. Patco Elektronik Teknologi, terdapat satu komputer yang terletak di bagian injection yang menjadi akses utama ke gambar cetak biru mold karena tidak adanya dana untuk membeli komputer lainnya. Namun, komputer ini juga digunakan oleh operator produksi untuk keperluan pencetakan label produksi. Para operator Moldshop harus mengakses gambar cetak biru melalui satu komputer di bagian injection, yang juga digunakan untuk keperluan produksi lainnya. Hal ini menyebabkan ketidakefisienan dalam proses kerja karena akan memakan banyak waktu, terlebih lagi karena spesifikasi komputer yang digunakan tidak sepenuhnya memadai. Selain itu, risiko keamanan data juga meningkat, karena akses terhadap gambar cetak biru tidak terbatas. Bahaya potensial dari akses tidak sah atau kebocoran data tidak boleh diabaikan. Lalu karena komputer yang digunakan oleh operator moldshop juga digunakan untuk keperluan pencetakan label produksi, ada risiko bahwa file gambar cetak biru dapat hilang atau terpengaruh selama proses ini.

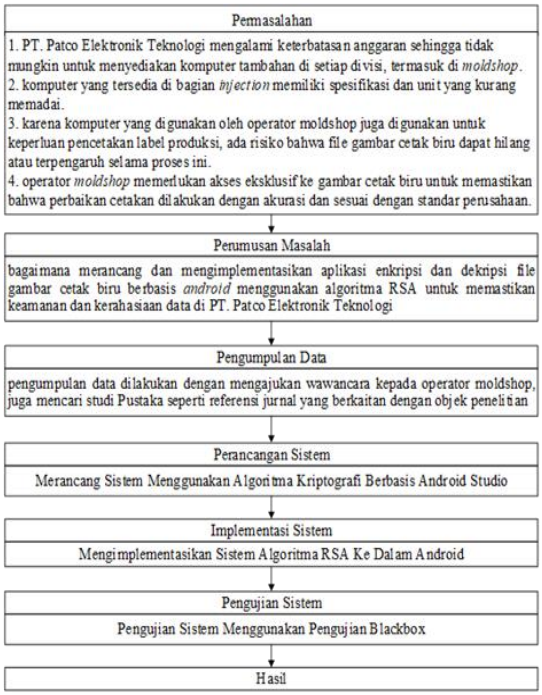
Dalam upaya untuk meningkatkan keamanan data, penulis memproposisikan rancangan aplikasi enkripsi dan dekripsi file gambar cetak biru. Aplikasi ini akan menggunakan algoritma RSA, yang dikenal sebagai salah satu metode enkripsi paling kuat dan andal yang tersedia saat ini. Keunggulan utama dari algoritma RSA adalah kemampuannya untuk mengamankan komunikasi dan data melalui sistem kunci publik dan pribadi.

Penelitian ini menjadi lengkap karena ditunjang oleh penelitian terdahulu, artikel yang tulis oleh Adriansyah Tampubolon yang berjudul "Implementasi Kombinasi Algoritma RSA dan Algoritma DES pada Aplikasi Pengaman Pesan Teks" menyatakan bahwa menggunakan kombinasi Algoritma RSA (*Rivest Shamir Adlemen*) dan Algoritma DES (*Data Encryption Standard*) untuk mengamankan pesan teks. Aplikasi yang menggunakan kombinasi ini bekerja dengan baik dan dapat mengenkripsi dan mendekripsi pesan teks, meningkatkan keamanan pesan[1].

Percobaan menunjukkan bahwa algoritma RSA dapat digunakan untuk mengenkripsi dan mendekripsi gambar RGB. Hasilnya menunjukkan bahwa gambar yang dienkripsi dengan algoritma ini sangat berbeda dengan gambar aslinya.

2. METODE PENELITIAN

Makalah ini menggunakan metode kualitatif deskriptif, yaitu Rivest Shamir Adleman salah satu dari metode kriptografi asimetris yang paling terkenal dan banyak digunakan, untuk penelitian ini algoritma *Rivest Shamir Adelman* akan diterapkan ke dalam program android sebagai enkripsi dan dekripsi gambar cetak biru. Teknik pengumpulan data dilakukan dengan wawancara kepada operator Moldshop pada tanggal 08 Mei 2023, observasi dan dokumentasi, serta mencari referensi dari buku atau jurnal yang berkaitan. Sementara dalam dalam penelitian ini, data direduksi, disajikan, dan diambil kesimpulan menggunakan kerangka penelitian berikut:



Gambar 1 : Kerangka Penelitian

2.1. Perancangan

Perancangan adalah Proses untuk mendefinisikan sesuatu yang akan dikerjakan dengan menggunakan teknik yang bervariasi serta di dalamnya melibatkan deskripsi mengenai arsitektur serta detail komponen dan juga keterbatasan yang akan dialami dalam proses pengerjaannya[2].

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

2.2. Aplikasi

Secara istilah pengertian aplikasi adalah suatu program yang siap untuk digunakan yang dibuat untuk melaksanankan suatu fungsi bagi pengguna jasa aplikasi serta penggunaan aplikasi lain yang dapat digunakan oleh suatu sasaran yang akan dituju. Pengertian aplikasi menurut Kamus Besar Bahasa Indonesia, "Aplikasi adalah penerapan dari rancang sistem untuk mengolah data yang menggunakan aturan atau ketentuan bahasa pemrograman tertentu"[3].

2.3. Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "cryptos" artinya "*secret*" (rahasia), sedangkan "graphein" artinya "writing" (tulisan). Jadi kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam menjaga kerahasiaan data dengan kriptografi, data sederhana yang dikirim (*plaintext*) diubah ke dalam bentuk data sandi (*ciphertext*), kemudian data sandi tersebut hanya dapat dikembalikan kebentuk data sebenarnya hanya dengan menggunakan kunci (*key*) tertentu yang dimiliki oleh pihak yang sah saja. Tentunya hal ini menyebabkan pihak lain yang tidak memiliki kunci tersebut tidak akan dapat membaca data yang sebenarnya sehingga dengan kata lain data akan tetap terjaga kerahasiannya[4].

Tujuan penerapan kriptografi adalah untuk membuat sesuatu yang tersembunyi, dapat suatu pesan rahasia berupa teks, suara, gambar dan video. Di dalam sistem kriptografi terdapat 5 bagian yaitu [5]:

1. *Plaintext* adalah pesan atau data dalam bentuk aslinya teks yang dapat terbaca. Plaintext adalah masukan bagi algoritma enkripsi.
2. *Secret Key* adalah masukan bagi algoritma enkripsi merupakan nilai yang bebas terhadap teks asli dan menentukan hasil keluaran algoritma enkripsi.
3. *Chipertext* adalah keluaran algoritma enkripsi. Ciphertext dapat dianggap sebagai pesan tersembunyi yang akan terlihat acak.
4. Algoritma Enkripsi memiliki 2 masukan teks asli dan kunci rahasia. Algoritma enkripsi melakukan transpormasi terhadap teks asli sehingga menghasilkan teks sandi.
5. Algoritma Dekripsi memiliki 2 masukan yaitu teks sandi dan kunci rahasia. Algoritma dekripsi memulihkan kembali teks sandi menjadi teks asli bila kunci rahasia algoritma enkripsi sama dengan algoritma dekripsi.

2.4. Enkripsi dan Dekripsi

Enkripsi merupakan sebuah teknik yang dilakukan mengacak data asli menjadi kode rahasia sehingga menyulitkan orang yang tidak berkepentingan untuk mengakses dan mengetahui data yang asli. Dekripsi adalah kebalikan dari enkripsi, dimana berfungsi untuk mendeskripsikan data yang telah dienkripsi sehingga data yang telah menjadi kode rahasia diubah kembali menjadi data biasa atau aslinya[6].

2.5. RSA (Rivest Shamir Adleman)

Algoritma RSA diperkenalkan poleh tiga peneliti MIT (Massacussets Institute of Technology), yaitu Ronald Rivest, Adi Shamir, dan Leornad Adleman pada tahun 1976. Algoritma RSA termasuk ke dalam algoritma asimetri karena kunci enkripsinya berbeda dengan kunci untuk dekripsi. Algoritma RSA menggunakan sepasang kunci, yaitu kunci publik untuk mengenkripsi pesan dan kunci privat untuk mendekripsi pesan. Kunci publik tidak dirahasiakan, sedangkan kunci privat dirahasiakan dan hanya diketahui oleh pemilik kunci[7].

Berikut adalah langkah-langkah pembangkitan pasangan kunci di dalam RSA[7]:

1. Pilih dua buah bilangan prima sembarang, misalkan α dan b (dirahasiakan).
2. Hitung n= α x b, nilai n tidak perlu dirahasiakan.
3. Hitung m=(α-1)(b-1). Setelah dihitung α, dan b dapat dihapus untuk mencegah diketahui oleh pihak lain.
4. Pilih sebuah bilangan bulat untuk kunci publik, misalkan e, yang relatif prima terhadap m.
5. Hitung kunci dekripsi, misalkan d, dengan kekongruaenan ed = 1 (mod m).

2.6. Android Studio

Pada perkembangannya, android tidak hanya merambah perangkat mobile saja tetapi google juga mengembangkan Android TV untuk televisi, Android Auto untuk mobil, dan Android Wear untuk jam tangan. Android merupakan sistem operasi untuk mobile berbasis linux yang mencakup sistem operasi, middleware, dan aplikasi. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka. Awalnya Google Inc. membeli

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Android Inc. yang merupakan pendatang baru yang membuat peranti lunak untuk ponsel/smartphone. Kemudian untuk mengembangkan Android makan dibentuklah Open Handset Alliance, konsorsium dari perusahaan pembuat peranti keras, peranti lunak, dan telekomunikasi termasuk Google, HTC, Intel, Motorola, Qualcomm, T-Mobile, dan Nvidia[8].

2.7. UML (Unified Modeling Language)

Unified Modeling Language (UML) adalah salah satu standar bahasa yang banyak digunakan di dunia industri untuk mendefinisikan *requirement*, membuat analisis dan desain, serta menggambarkan arsitektur dalam pemrograman berorientasi objek. UML merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung. UML muncul karena adanya kebutuhan pemodelan visual untuk menspesifikasikan, menggambarkan, membangun, dan dokumentasi dari sistem perangkat lunak. UML hanya berfungsi untuk melakukan pemodelan. Jadi penggunaan UML tidak terbatas pada metodologi tertentu, meskipun pada kenyataannya UML paling banyak digunakan pada metodologi berorientasi objek[9].

2.8. Blackbox Testing

Teknik pengujian yang penulis gunakan adalah *Black-Box Testing*. *Black Box Testing* yaitu menguji desain dan kode program. Pengujian dimaksudkan untuk mengetahui apakah fungsi-fungsi, masukan, dan keluaran dari perangkat lunak sesuai dengan spesifikasi yang dibutuhkan. Cara pengujian hanya dilakuakan dengan menjalankan atau mengeksekusi unit atau model secara *offline* dan *online* melalui publik, kemudian diamati apakah hasil dari unit itu sesuai dengan proses yang diinginkan[10].

2.9. Tahapan Penelitian

2.9.1. Analsisi Sistem Berjalan

Sistem yang berjalan saat ini dimana operator moldshop melakukan perbaikan mold diperlukan waktu yang lama, untuk melihat file cetak biru dibutuhkan waktu lagi dimana operator moldshop harus ke komputer operator line, dengan mengantri dengan operator line dan belum lagi terjadi freeze pada komputer, pernah juga terjadi hilangnya gambar cetak biru karena tidak sengaja terhapus oleh operator line. Karena sistem komputer yang kurang mendukung mengakibatkan kurang aman dan efisien dalam melihat gambar cetak biru mold. Dalam analisis sistem ini bertujuan untuk membuat sistem baru dengan perancangan sistem aplikasi sehingga melihat gambar cetak biru dapat lebih aman dan efisien.

2.9.2. Pengumpulan Data

1. Studi Pustaka
   Peneliti mengumpulkan data melalui jurnal, buku, literatur, serta bacaan-bacaan yang berkaitan dengan penelitian yang sedang dilakukan.

2. Observasi
   Peneliti melakukan pengamatan dan peninjauan secara langsung pada bagian moldshop. Hal ini dilakukan untuk mendapatkan data yang akurat dan sesuai dengan keadaan sebenarnya di lapangan. Adapun tempat penelitian akan dilaksanakan di PT. Patco Elektronik Teknologi.

3. Wawancara
   Wawancara ini dilakukan dengan operator moldshop, Hal ini dilakukan untuk meyakinkan bahwa data yang dikumpulkan akurat.

2.9.3. Analisis Kebutuhan Fungsional

Berikut kebutuhan fungsional yang terdapat pada rancangan aplikasi yang dibangun :

1. Mengimplementasikan penggunaan bahasa pemrograman java dalam membangun aplikasi pengamanan citra menggunakan algoritma rsa
2. Aplikasi dapat menggambarkan penerapan algoritma rsa sebagai media pengamanan gambar cetak biru.
3. input dan output berupa file gambar yang dapat diproses dengan algoritma RSA.

2.9.4. Kebutuhan NonFungsional

perangkat yang penulis gunakan agar aplikasi berjalan baik,yaitu sebagai berikut :

1. Perangkat Lunak (Software)
   a. Operating System Windows 10
   b. Android Studio
   c. Xampp
2. Perangkat Keras (Hardware)

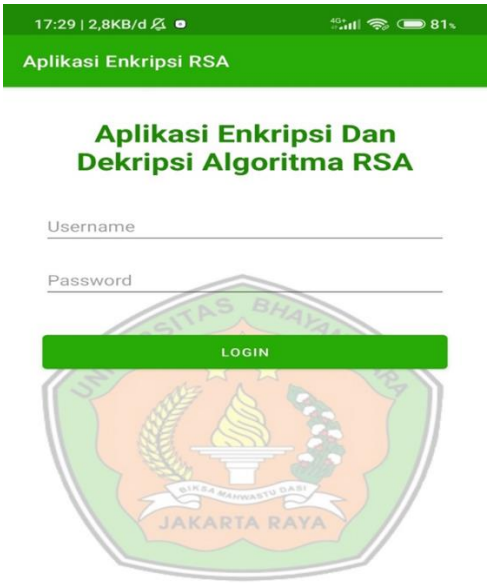
p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

a. Komputer yang setara dengan Intel Core i3
b. Ram 16 GB
c. SSD 120GB
d. Mouse, keyboard dan monitor

3. HASIL DAN PEMBAHASAN

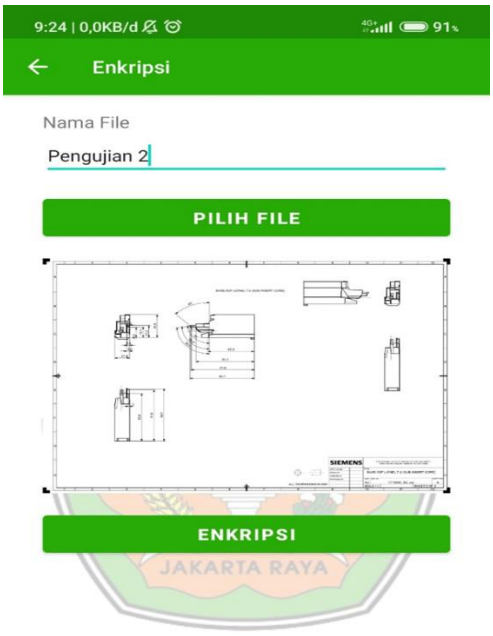
Pada tahap ini merupakan hasil penerapan Algoritma RSA di android Studio.

1. Halaman awal
   Pada gambar 2 halaman login karyawan dimana admin dan karyawan sama-sama wajib melakukan login sebelum masuk ke dalam sistem, dimana admin dan karyawan memasukan username dan password yang telah ditentukan.



Gambar 2 : Halaman Awal

2. Halaman Enkripsi
   Pada gambar 3 merupakan halaman enkripsi, dimana halaman ini hanya dapat diakses oleh karyawan dalam bentuk android, dimana pada halaman ini karyawan memasukan nama file dan memilih file gambar cetak biru yang akan dienkripsi.



Gambar 3 : Halaman Enkripsi

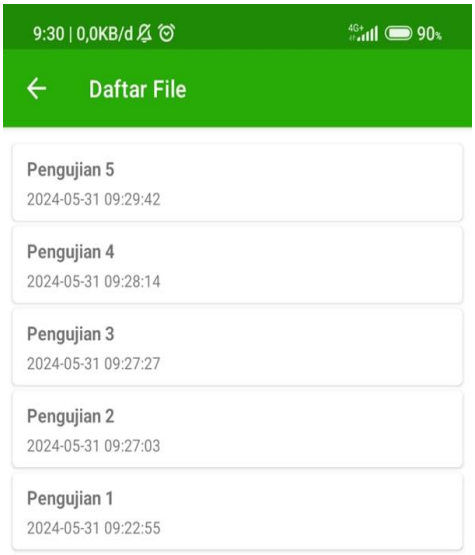
3. Halaman Hasil enkripsi
   Pada gambar 4 merupakan halaman hasil enkripsi, dimana halaman ini akan menampilkan hasil file enkripsi, size sebelum enkripsi, size sesudah enkripsi dan waktu enkripsinya.

Gambar 4 : Halaman Dekripsi

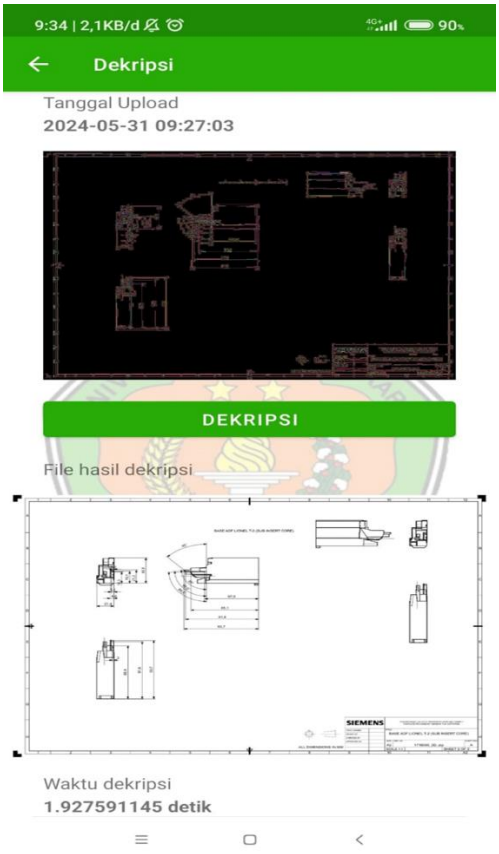
4. Halaman Dekripsi

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

Pada gambar 5 operator memilih file yang akan di dekripsi, pada gambar 6 hasil dari dekripsi dari hasil pemilihan file.



Gambar 5 : Halaman Pemilihan File



Gambar 6 : Halaman Hasil Dekripsi

5. Pengujian Waktu RSA

Tabel 1 Pengujian

No.	Size Sebelum Enkripsi	Size Sesudah Enkripsi	Waktu Enkripsi	Waktu Dekripsi
1	216,66 kb	621,35 kb	14.674 Detik	4.965 Detik
2	99,48 kb	197,09 kb	4.217 Detik	2.045 Detik
3	147,50 kb	241,10 kb	4.614 Detik	2.089 Detik
4	217,28 kb	909,38 kb	15.188 Detik	5.942 Detik
5	204,83 kb	780,19 kb	4.256 Detik	4.134 Detik

Berdasarkan table 1 di atas telah mendapatkan hasil bahwa untuk size mengalami peningkatan lebih besar pada saat setelah melakukan enkripsi, dan untuk waktu enkripsi mendapatkan hasil rata-rata pada saat melakukan enkripsi menggunakan metode RSA yaitu 4-15 detik, dan pada saat dekripsi mendapatkan hasil 2-5 detik.

4. KESIMPULAN

Hasil dari penelitian ini adalah aplikasi berbasis Android yang mampu melakukan enkripsi dan dekripsi file gambar cetak biru dengan menerapkan *Rivest Shamir Adleman* berhasil dirancang. Aplikasi tersebut tidak hanya dirancang tetapi juga berhasil dibangun dan diuji, hasil pengujian menunjukkan bahwa aplikasi dapat melakukan enkripsi dan dekripsi file gambar cetak biru dengan baik dimana hasil rata-rata pada saat melakukan enkripsi menggunakan metode *Rivest Shamir Adleman* yaitu 4-15 Detik, dan pada saat dekripsi mendapatkan hasil 2-5 Detik. Implementasi algoritma *Rivest Shamir Adleman* untuk enkripsi dan dekripsi memastikan bahwa file gambar cetak biru dapat diamankan dengan tingkat keamanan yang tinggi.

5. SARAN

Dalam pembuatan sistem ini tentu masih banyak kekurangan yang masih perlu dilakukan perbaikan dan pengembangan lebih lanjut agar menjadikan aplikasi ini semakin menarik dan diminati banyak orang. Oleh karena itu peneliti menyarankan beberapa hal untuk bahan pengembangan sistem ini agar memiliki tampilan yang lebih menarik lagi, untuk

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

penelitian selanjutnya, peneliti bisa menggabungkan / membuat perbandingan metode RSA dengan metode yang lainnya dan mengembangkan jaringan lokal ke jaringan internet

DAFTAR PUSTAKA

[1] A. Tampubolon, "Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks," *Jurnal Sains Manajemen Informatika dan Komputer*, vol. 20, no. 1, pp. 38–43, 2021, [Online]. Available: https://ojs.trigunadharma.ac.id/

[2] A. R. Adiguna, M. C. Saputra, and F. Pradana, "Analisis dan perancangan sistem informasi manajemen gudang pada PT Mitra Pinasthika Mulia Surabaya," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, vol. 2548, p. 964X, 2018.

[3] A. Juansyah, "Pembangunan aplikasi child tracker berbasis assisted–global positioning system (a-gps) dengan platform android," *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*, vol. 1, no. 1, pp. 1–8, 2015.

[4] S. Wardoyo, T. Ryadi, and R. Fahrizal, "Analisis performa file transport protocol pada perbandingan metode IPv4 murni, IPv6 murni dan tunneling 6to4 berbasis router mikrotik," *Jurnal Nasional Teknik Elektro*, vol. 3, no. 2, pp. 106–117, 2014.

[5] N. Azis, "Perancangan aplikasi enkripsi dekripsi menggunakan metode caesar chiper dan operasi xor," *ikraith-informatika*, vol. 2, no. 1, pp. 72–80, 2018.

[6] A. Arisantoso, M. Sanwasih, and M. R. Pahlevi, "PENERAPAN APLIKASI PENGAMANAN DATA/FILE DENGAN METODE ENKRIPSI DAN DEKRIPSI ALGORITMA 3DES DALAM JARINGAN LOKAL AREA," *SEMNASTEKNOMEDIA ONLINE*, vol. 5, no. 1, pp. 2–9, 2017.

[7] T. Informatika and I. Artikel, "APLIKASI ENKRIPSI GAMBAR MENGGUNAKAN METODE (RIVEST SHAMIR ADLEMAN) RSA." [Online]. Available: https://jurnal.umpar.ac.id/index.php/syllog

[8] H. Nasruddin Safaat, "Pemograman Aplikasi Mobile Smartphone Dan Tablet PC Berbasis Android," *Bandung: Informatika Bandung*, 2015.

[9] A. K. S. Putra, "Program studi teknik informatika fakultas teknologi informasi dan elektro universitas teknologi yogyakarta," 2017.

[10] A. S. Rosa and M. Salahuddin, "Modul pembelajaran rekayasa perangkat lunak (terstruktur dan berorientasi objek)," *Bandung: modula*, vol. 2, 2011.