# ANALISIS PERFORMA ALGORITMA KRIPTOGRAFI RSA DAN RSA-CRT DALAM PENGAMANAN PESAN TEKS

Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 pada
Jurusan Teknik Informatika


Oleh:

Ihtiar Alfath Raden Pangestu
09021381823093

**Jurusan Teknik Informatika**
**FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA**
**2023**

# LEMBAR PENGESAHAN SKRIPSI

## ANALISIS PERFORMA ALGORITMA KRIPTOGRAFI RSA DAN RSA-CRT DALAM PENGAMANAN PESAN TEKS

Oleh :

Ihtiar Alfath Raden Pangestu
09021381823093

Palembang, 2 Januari 2023

Pembimbing I

Alfarissi, M.Comp.Sc.
NIP. 198512152014041001

Pembimbing II,

Muhammad Qurhanul Rizqie, M.T., Ph.D.
NIP. 198712032022031006

Mengetahui,
Ketua Jurusan Teknik Informatika,

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

## TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari **Selasa** tanggal **20 Desember 2022** telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

| | |
|---|---|
| Nama | : Ihtiar Alfath Raden Pangestu |
| N I M | : 09021381823093 |
| Judul | : Analisis Performa Algoritma Kriptografi RSA dan RSA-CRT dalam Pengamanan Pesan Teks |

dan dinyatakan **LULUS**.

1. Ketua

   Alvi Syahrini Utami, M.Kom.
   NIP. 197812222006042003

2. Penguji

   Osvari Arsalan, M.T.
   NIP. 198806282018031001

3. Pembimbing I

   Al Farissi, M.Cs.
   NIP. 198512152014041001

4. Pembimbing II

   Muhammad Qurhanul Rizqie, M.T., Ph.D.
   NIP. 198712032022031006

Mengetahui,
Ketua Jurusan Teknik Informatika,

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

## HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

| | |
|---|---|
| Nama | : Ihtiar Alfath Raden Pangestu |
| NIM | : 09021381823093 |
| Program Studi | : Teknik Informatika Bilingual |
| Judul Skripsi | : Analisis Performa Algoritma Kriptografi RSA dan RSA-CRT dalam Pengamanan Pesan Teks |

Hasil pengecekan Software *iThenticate/Turnitin* : 2%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya 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 oleh siapapun.

Palembang, 3 Januari 2023


Ihtiar Alfath Raden Pangestu
NIM. 09021381823093

## MOTTO DAN PERSEMBAHAN

- Trust the process, every human being has a different time for success
- What you get, that's what you learn

Kupersembahkan karya tulis ini kepada :

- Keluargaku
- Teman-teman seperjuangan
- Fakultas Ilmu Komputer
  Universitas Sriwijaya

# PERFORMANCE ANALYSIS OF RSA AND RSA-CRT CRYPTOGRAPHY ALGORITHMS IN SECURING MESSAGES

**By:**

**Ihtiar Alfath Raden Pangestu**
**09021381823093**

## ABSTRACT

The RSA algorithm is an asymmetric method with an advantage in message security, while the RSA-CRT algorithm is an RSA algorithm that implements the CRT (Chinese Remainder Theorem) method. In this study, an analysis was carried out of the RSA and RSA-CRT cryptographic algorithms for text message security. The key used in the RSA and RSA-CRT algorithm will always be generated when the encryption process occurs with a key length of 2048 bits. In this study, the analysis carried out was calculating the Avalanche Effect value and processing time. The results obtained in this study are that the RSA algorithm has an average Avalanche Effect value which is equivalent to the RSA-CRT algorithm because both algorithms have percentage value of Avalanche Effect of 22%. However, the effectiveness of the encryption of the two algorithms is not categorized as good because it has an Avalanche Effect value of less than 50%. In securing messages, the decryption processing time of the RSA-CRT algorithm is faster than the RSA algorithm with an overall average of 268,15 ms on the RSA-CRT algorithm and 1598,35 ms on the RSA algorithm. While for the encryption processing time, both algorithms have an equivalent processing time because the encryption processing time is almost the same, this is because the two algorithms have the same encryption method.

**Keywords:** Cryptography, RSA, RSA-CRT

# ANALISIS PERFORMA ALGORITMA KRIPTOGRAFI RSA DAN RSA-CRT DALAM PENGAMANAN PESAN TEKS

**Oleh:**

**Ihtiar Alfath Raden Pangestu**
**09021381823093**

## ABSTRAK

Algoritma RSA merupakan algoritma asimetri yang memiliki keunggulan dalam pengamanan pesan, sedangkan algoritma RSA-CRT merupakan algoritma RSA yang menerapkan metode CRT (*Chinese Remainder Theorem*). Pada penelitian ini, dilakukan analisis terhadap performa algoritma kriptografi RSA dan RSA-CRT pada pengamanan pesan teks. Pesan teks yang dapat diproses enkripsi dan dekripsi merupakan pesan dengan bentuk *file*. Kunci yang digunakan pada algoritma RSA dan RSA-CRT akan selalu dibangkitkan saat proses enkripsi terjadi dengan panjang kunci 2048 bit. Dalam penelitian ini, analisis yang dilakukan yaitu perhitungan nilai *Avalanche Effect* dan kecepatan pemrosesan. Hasil yang didapatkan pada penelitian yaitu algoritma RSA memiliki rata – rata keseluruhan nilai Avalanche Effect yang setara dengan algoritma RSA-CRT karena kedua algoritma memiliki persentase nilai *Avalanche Effect* sebesar 22%. Namun, efektivitas enkripsi kedua algoritma tersebut belum dikatakan baik karena memiliki nilai *Avalanche Effect* kurang dari 50%. Dalam mengamankan pesan, kecepatan pemrosesan dekripsi algoritma RSA-CRT jauh lebih cepat dibandingkan algoritma RSA, dengan rata – rata keseluruhan 268,15 ms pada algoritma RSA-CRT, sedangkan pada algoritma RSA sebesar 1598,35 ms. Sedangkan untuk kecepatan pemrosesan enkripsi kedua algoritma memiliki kecepatan yang setara karena kecepatan pemrosesan enkripsi yang dimiliki hampir sama, hal ini dikarenakan kedua algoritma memiliki metode enkripsi yang sama.

**Kata Kunci:** Kriptografi, RSA, RSA-CRT

# KATA PENGANTAR

Puji dan syukur kehadirat Allah SWT yang telah senantiasa melimpahkan rahmat dan hidayah-Nya, tak lupa shalawat serta salam senantiasa tercurahkan kepada junjungan Nabi Muhammad SAW yang selalu kita nantikan syafa'atnya di akhirat nanti. Penulis mengucapkan syukur kepada Allah SWT atas limpahan nikmat sehat-Nya, baik itu berupa sehat fisik maupun akal pikiran, sehingga penulis dapat menyelesaikan Skripsi yang berjudul "**Analisis Performa Algoritma Kriptografi RSA dan RSA-CRT dalam Pengamanan Pesan Teks**" dengan tepat waktu, dan ini disusun untuk memenuhi salah satu syarat kelulusan tingkat Strata-1 pada Jurusan Teknik Informatika Universitas Sriwijaya.

Penulis menyadari dalam pengerjaan tugas akhir ini penulis banyak mendapatkan dukungan serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan kali ini penulis ingin mengucapkan ucapan terimakasih yang tak terhingga kepada pihak yang telah banyak mendukung dan memberi bantuan, yaitu kepada:

1. Allah SWT yang telah memberikan nikmat, rahmat serta hidayah-Nya kepada penulis dalam menyelesaikan skripsi ini.
2. Orang tua yang paling saya sayangi yaitu Papa Trimono dan Mama Mutmainah, Saudara lelakiku Al Aziiz Afi Akbar, serta seluruh keluarga besar yang telah memberikan semangat, dukungan, bantuan serta doa kepada penulis selama ini.

3. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Alfarissi, M.Comp.Sc. dan Bapak Muhammad Muhammad Qurhanul Rizqie, M.T., Ph.D. selaku pembimbing yang telah membimbing, memberikan motivasi dan telah membantu penulis.
6. Bapak Muhammad Fachrurrozi, M.T. selaku pembimbing akademik yang selalu membimbing serta memberikan masukan dan saran kepada penulis dalam proses perkuliahan.
7. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Sahabat seperjuangan saya Arya Pradata, Cindy Wijaya, Dhiya Calista, Zora Cahya Ardiya Prameswari dan teman-teman lain yang tidak dapat disebutkan satu-persatu yang telah memberikan semangat dan bantuan kepada penulis.
9. Alvedo Mohd Izazi selaku rekan yang selalu memberi dukungan, bantuan, saran, serta tempat untuk bertukar pikiran penulis untuk menyelesaikan tugas akhir ini.
10. Dan untuk semua pihak yang telah banyak membantu pengerjaan tugas akhir ini yang tidak dapat disebutkan satu-persatu.

Akhir kata, Penulis sangat menyadari bahwa tugas akhir ini masih jauh dari kata sempurna. Untuk itu kritik dan saran yang membangun dari semua pihak

sangat dibutuhkan dalam penyempurnaan tugas akhir ini. Semoga tugas akhir ini bermanfaat bagi semua pihak.

Palembang, 3 Januari 2023

Ihtiar Alfath Raden Pangestu

## DAFTAR ISI

Halaman

## DAFTAR GAMBAR

Halaman

# DAFTAR TABEL

Halaman

# BAB I

# PENDAHULUAN

## 1.1 Pendahuluan

Dalam Bab pendahuluan hal yang akan dibahas yaitu latar belakang pemilihan topik "Analisis Performa Algoritma Kriptografi RSA dan RSA-CRT dalam Pengamanan Pesan Teks". Selain itu juga Bab ini membahas rumusan masalah, tujuan serta manfaat penelitian, batasan masalah, dan sistematika penulisan. Semua gambaran secara umum pada penelitian akan dijelaskan pada Bab ini.

## 1.2 Latar Belakang

Seiring berkembangnya zaman teknologi informasi menjadi salah satu kebutuhan yang dibutuhkan dalam kehidupan, dan memiliki peranan penting pada setiap lapisan masyarakat. Dikarenakan berubahnya cara manusia untuk menjalani kehidupan, hal tersebut menjadi landasan berkembangnya pola pikir dan pengetahuan manusia sehingga dapat mengembangkan teknologi informasi (Saputra, et al., 2017).

Dengan memanfaatkan teknologi informasi manusia dapat saling bertukar informasi, penggunaan keamanan data saat bertukar informasi merupakan suatu hal yang sangat penting agar pesan yang memiliki sifat rahasia maupun penting dapat terjaga dan tetap utuh, selain itu pihak yang tidak memiliki hak untuk mengetahui isi pesan tersebut tidak mengetahuinya. Salah satu cara untuk menjaga kerahasiaan dan keutuhan pesan yaitu dengan memanfaatkan Kriptografi.

Kriptografi merupakan ilmu mengenai teknik merubah data asli (*plaintext*) menjadi suatu hal yang sulit untuk dibaca (*ciphertext*) dengan menggunakan kunci enkripsi dan untuk dapat membaca data tersebut dengan cara dekripsi terlebih dahulu *ciphertext* dengan menggunakan kunci deskripsi (Kromodimoeljo, 2010). Dalam penerapannya algoritma kriptografi dibagi menjadi 2 berdasarkan jenis kuncinya yaitu algoritma kriptografi kunci simetri (kunci publik) dan algoritma kriptografi kunci asimetri (kunci privat) (Saputro, Hidayati, & Ujianto, 2020).

Algoritma RSA merupakan algoritma Kriptografi yang memiliki jenis kunci asimetri sehingga kunci yang digunakan untuk melakukan proses enkripsi berbeda dengan kunci yang digunakan untuk dekripsi (Tampubolon, 2021). Keamanan enkripsi serta dekripsi pada algoritma RSA dapat dilihat melalui sulitnya dalam melakukan pemfaktoran nilai modulus n yang besar (Indriani, Alfina, & Syahputri, 2022).

Algoritma RSA-CRT merupakan algoritma perkembangan dari algoritma RSA yang menggunakan teorema CRT (*Chinese Remainder Teorem)*, sehingga dalam melakukan komputasi memakan waktu sekitar 4 kali lebih cepat. Saat melakukan pemrosesan algoritma RSA-CRT melalui 3 tahap proses yang sama seperti algoritma RSA yaitu pembangkitan kunci, enkripsi, dan deskripsi (Wibowo, Umam, & Hikmah, 2020).

Algoritma kriptografi terdapat berbagai macam jenis dan setiap algoritma memiliki keunggulan serta kelemahan yang berbeda – beda, oleh karena itu terdapat banyak pihak yang mengkombinasikan atau mengembangkan algoritma kriptografi

yang bertujuan untuk meningkatkan keunggulan dan meminimalisir kelemahan dari algoritma. Untuk mengetahui kelebihan dan kekurangan algoritma perlu dilakukannya proses analisis performa algoritma. Menurut (Permatasari, Aminudin, & Arifianto, 2019) analisis performa algoritma kriptografi dapat dilakukan dengan melihat hasil perbandingan metode pengujian yang dilakukan, contohnya seperti pengujian *avalanche effect* untuk mengetahui bagus atau tidak suatu algoritma dan pengujian kecepatan eksekusi untuk mengetahui kualitas kecepatan eksekusi enkripsi dan dekripsi suatu algoritma.

Berdasarkan penjelasan diatas penulis melakukan penelitian yang bertujuan untuk mengetahui perbandingan performa algoritma baik pada proses enkripsi maupun dekripsinya, jika algoritma yang dianalisis performanya adalah algoritma perkembangan dengan algoritma aslinya yaitu RSA-CRT dan RSA.

## 1.3 Rumusan Masalah

Berdasarkan penjelasan pada latar belakang terdapat permasalahan yang teridentifikasi yaitu sebagai berikut:

1. Bagaimana cara mengukur performa algoritma Kriptografi RSA dan RSA-CRT dalam mengamankan pesan teks?
2. Bagaimana performa algoritma Kriptografi RSA dan RSA-CRT dalam mengamankan pesan teks?

## 1.4 Tujuan Penelitian

Berikut merupakan tujuan dilakukanya penelitian ini yaitu:

1. Mengukur performa algoritma Kriptografi RSA dan RSA-CRT dalam mengamankan pesan teks.
2. Menganalisis performa algoritma Kriptografi RSA dan RSA-CRT dalam mengamankan pesan teks.

## 1.5 Manfaat Penelitian

Berikut merupakan manfaat dilakukannya penelitian ini yaitu:

1. Mampu merumuskan secara pengukuran performa algoritma Kriptografi RSA dan RSA-CRT dalam mengamankan pesan teks.
2. Mengetahui performa algoritma Kriptografi RSA dan RSA-CRT dalam mengamankan pesan teks.
3. Hasil penelitian ini dapat dijadikan sebagai referensi bagi peneliti lain dalam bidang Kriptografi.

## 1.6 Batasan Masalah

Batasan masalah pada penelitian yang dilakukan yaitu:

1. Algoritma yang dianalisis performanya pada penelitian ini hanya RSA dan RSA-CRT dengan menggunakan bahasa pemrograman Java.
2. Pesan yang dapat diamankan hanya pesan yang berbentuk teks. Tabel, grafik, gambar, dan sebagainya tidak termasuk.

## 1.7 Sistematika Penulisan

Pada penulisan laporan teradapat sistematika penulisan, sistematika penulisan yang digunakan penulis pada penulisan laporan tugas akhir ini yaitu

mengikuti sistematika standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya yaitu:

**BAB I. PENDAHULUAN**

Dalam Bab ini menguraikan hal – hal dasar dilakukannya penelitian ini yang meliputi latar belakang penelitian dilakukan, perumusan masalah, tujuan serta manfaat penelitian, batasan masalah, dan sistematika penulisan.

**BAB II. KAJIAN LITERATUR**

Dalam Bab ini menguraikan semua landasan teori yang berhubungan dengan penelitian antara lain yaitu Teknologi Informasi, Kriptografi, algoritma RSA, algoritma RSA-CRT, RUP (*Rational Unified Process*) dan penelitian yang relevan.

**BAB III. METODOLOGI PENELITIAN**

Dalam Bab Metodologi Penelitian akan membahas mengenai langkah – langkah yang akan dilalui saat melakukan penelitian. Langkah – langkah yang akan dilalui dijelaskan secara mendetail yang akan dijadikan sebagai acuan kerangka kerja, serta terdapat perencanaan manajemen proyek saat melakukan penelitian.

**BAB IV. PENGEMBANGAN PERANGKAT LUNAK**

Dalam Bab ini membahas mengenai langkah – langkah yang dilalui dalam mengembangkan perangkat lunak pada penelitian analisis performa algoritma Kriptografi RSA dan RSA-CRT dalam pengamanan pesan teks.

**BAB V. HASIL DAN ANALISIS**

Hasil pengujian dari penelitian yang telah dilakukan akan dianalisis dan dibahas pada Bab ini. Basis dari kesimpulan yang akan diambil pada penelitan dibuat berdasarkan hasil dan analisis pengujian yang telah dilakukan.

**BAB VI. KESIMPULAN DAN SARAN**

Semua kesimpulan dan saran yang ada pada penelitian ini didapatkan dari segala uraian pada beberapa Bab sebelumnya. Pada Bab ini diharapkan dapat berguna serta bermanfaat untuk pengembangan penelitian kedepannya.

## 1.8 Kesimpulan

Dalam Bab ini dapat diambil kesimpulan bahwa permasalahan yang akan diselesaikan pada penelitian ini yaitu bagaimana mengukur dan menganalisis performa algoritma kriptografi perkembangan dengan algoritma aslinya yaitu RSA-CRT dengan RSA pada sistem keamanan pesan teks.

# DAFTAR PUSTAKA

F, R., & Anwar. (2021). Implementasi Kriptografi Dengan Metode Advanced Encryption Standard (AES) Untuk Realtime Chat Berbasis Mobile Pada E-Learning Politeknik Negeri Lhokseumawe. *JAISE : Journal of Artificial Intelligence and Software Engineering*, 1-8.

Fauzi, A., Novriyenni, Maulita, Y., & Pardede, A. M. (2017). Analisis Hybrid Cryptosystem Algoritma Algoritma RSA dan Triple DES. *Jurnal Teknik Informatika Kaputama (JTIK)*, 36-44.

Fox, R. (2013). *Information Technology An Introduction for Today's Digital World.* Boca Raton: Taylor & Francis Group.

Herteno, R., Ramadansyah, W., Soesanto, O., Nugroho, R. A., & Arrahimi, A. R. (2019). Steganografi Untuk Pesan Terenkripsi Menggunakan RSA-CRT di Android. *Kumpulan jurnaL Ilmu Komputer (KLIK)*, 16-26.

Hidayat, A., Arifudin, R., & Akhlis, I. (2020). *Journal of Advances in Information Systems and Technology*, 1-10.

Indriani, U., Alfina, O., & Syahputri, N. (2022). Penerapan Algoritma RSA Dalam Keamanan File Ms Word. *Journal of Machine Learning and Data Analytics (MALDA)*, 95-100.

Kromodimoeljo, S. (2010). *Teori dan Aplikasi Kriptografi.* SPK IT Consulting.

Lestari, R., Buaton, R., & Gultom, I. (2021). Penerapan Algoritma OTP dan Algoritma RSA CRT dalam Pengamanan Citra. *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*, 180-190.

Permatasari, S., Aminudin, & Arifianto, S. (2019). Modifikasi Enkripsi Dan Dekripsi AES Menggunakan Polybius Chiper Dalam Pengamanan Data. *Repositor*, 117-124.

Permatasari, S., Aminudin, & Arifianto, S. (2019). Modifikasi Enkripsi Dan Dekripsi AES Menggunakan Polybius Chiper Dalam Pengamanan Data. *Repositor*, 117-124.

Puspita, Y., Fitriani, Y., Astuti, S., & Novianti, S. (2020). Selamat Tinggal Revolusi Industri 4.0, Selamat Datang Revolusi Industri 5.0. *Seminar Nasional Pendidikan 10 Januari 2020* (pp. 122-130). Palembang: Prosiding Seminar Nasional Pendidikan Program Pascasarjana Universitas PGRI Palembang.

Rabia, A., Iwendi, C., Javed, A. R., Rizwan, M., Jalil, Z., Anajemba, J. H., & Biamba, C. (2021). An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. *Personal and Ubiquitous Computing*.

Saputra, G. W., Rivai, M. A., Su'udah, M., Wulandari, S. L., Dewi, T. R., & Fitroh. (2017). Pengaruh Teknologi Informasi Terhadap Kecerdasan (Intelektual, Spiritual, Emosional dan Sosial) Studi Kasus: Anak-Anak. *Studia Informatika: Jurnal Sistem Informasi*, 77-88.

Saputro, T. H., Hidayati, N., & Ujianto, E. (2020). Survei tentang Algoritma Kriptografi Asimetris. *JIP (Jurnal Informatika Polinema)*, 67-72.

Sinaga, M. C. (2017). *Kriptografi Python.* Medan: Matius Celcius Sinaga.

Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., & Srinjiwi. (2019). Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, 1-10.

Sulistiyorini, & Prihanto, A. (2019). Perbandingan Efisiensi Algoritma RSA dan RSA-CRT Dengan Data Teks Berukuran Besar. *Journal of Informatics and Computer Science*, 84-90.

Tampubolon, A. (2021). Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, 38-43.

Tia, T. K., & K, W. A. (2018). Model Simulasi Pengembangan Perangkat Lunak Menggunakan Rational Unified Process (RUP). *Teknika : Engineering and Sains Journal*, 33-40.

Triandi, B. (2019). Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0. *Jurnal Riset Komputer*, 477-483.

V, A., & N, N. (2021). Performance Analysis of Random NumberGenerators in Cryptographic Algorithms. *International Journal of Mechanical Engineering*, 2115-2119.

Wibowo, N. C., Umam, K., & Hikmah, A. (2020). Komparasi Waktu Algoritma RSA Dengan RSA-CRT Base On Computer. *WJIT : Walisongo Journal of Information Technology*, 13-26.