Implementasi Algoritma RSA-CRT dan Algoritma *One Time-Pad* Secara *Hybrid Cryptosystem* pada Pengamanan Teks

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

Oleh:

Muhammad Febriansyah
NIM: 09021281823030

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2022

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI ALGORITMA RSA-CRT DAN ALGORITMA *ONE TIME-PAD* SECARA *HYBRID CRYPTOSYSTEM* PADA PENGAMANAN TEKS

Oleh :

MUHAMMAD FEBRIANSYAH
NIM : 09021281823030

Palembang, 30 Agustus 2022

Pembimbing I

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

Pembimbing II

Osvari Arsalan,S.Kom., M.T
NIP. 1601142806880003

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari Kamis tanggal 04 Agustus 2022 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

Nama : Muhammad Febriansyah
NIM 09021281823030
Judul : Implementasi Algoritma RSA-CRT dan Algoritma *One Time-Pad* Secara *Hybrid Cryptosystem* pada Pengamanan Teks

dan dinyatakan **LULUS**

1. Ketua Penguji

   Dr. M. Fachrurozi M.T. .....
   NIP 198005222008121002

2. Penguji I

   Novi Yusliani, M.T. .....
   NIP 198211082012122001

3. Penguji II

   Kanda Januar Miraswan, M.T. .....
   NIP 199001092019031012

4. Pembimbing I

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

5. Pembimbing II

   Osvari Arsalan,S.Kom., M.T. .....
   NIP 1601142806880003

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom
NIP 197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: Muhammad Febriansyah
NIM	: 09021281823030
Program Studi	: Teknik Informatika
Judul Skripsi	: Implementasi Algoritma RSA-CRT dan Algoritma *One Time-Pad* Secara *Hybrid Cryptosystem* pada Pengamanan Teks

Hasil Pengecekan Software (iThenricate/Turnitin) : 5%

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, 04 Agustus 2022

Muhammad Febriansyah
NIM. 09021281823030

MOTTO DAN PERSEMBAHAN

Motto :

- *I know the world's a broken bone but melt your headaches call it home*
- *Now if you never shoot, you'll never know and if you never eat, you'll never grow*
- *I only see my goals, I don't believe in failure 'cause I know the smallest voices, they can make it major*
- *I know you're sad and tired, you've got nothing left to give. But you'll find another life to live*

Kupersembahkan karya tulis ini kepada :

- Kedua orang tua dan almh adikku
- Keluargaku
- Teman Seperjuangan
- Teknik Informatika
- Fakultas Ilmu Komputer
- Universitas Sriwijaya

ABSTRACT

Communication is one of the basic human traits that are useful for interacting with each other. One of the methods of communication used by humans is text or writing which serves to convey messages to the recipient. The message can contain information that is confidential and is likely to be intercepted by parties who are not responsible for knowing the contents of the message and changing it before it reaches the recipient. Therefore text security is important to maintain the confidentiality of the information in the message. With the Hybrid Cryptosystem method with the RSA-CRT algorithm (asymmetric algorithm) and the One Time Pad algorithm (symmetric algorithm) a software will be produced to increase security in text messages that encrypt/decrypt messages with session-key One Time Pad generate various character messages. which are coded as symbols that are difficult for cybercriminals to know and are secured with an RSA-CRT public key in the form of numbers that are difficult to know so as to increase the level of message key security.

***Keywords**: One Time Pad Algorithm, RSA-CRT Algorithm, Hybrid Cryptosystem, Text Security*

ABSTRAK

Komunikasi adalah salah satu sifat dasar manusia yang gunanya untuk berinteraksi satu sama lain. Salah satu metode berkomunikasi yang digunakan manusia ialah teks atau tulisan yang berfungsi untuk menyampaikan pesan kepada penerimanya. Pesan tersebut dapat berisi suatu informasi yang bersifat rahasia dan besar kemungkinan disadap oleh pihak-pihak yang tidak bertanggung jawab untuk mengetahui isi pesan tesebut dan merubahnya sebelum sampai kepenerimanya. Maka dari itu pengamanan teks merupakan hal penting untuk menjaga kerahasiaan informasi pada pesan tersebut. Dengan metode *Hybrid Cryptosystem* dengan algoritma RSA-CRT (algoritma asimetris) dan algoritma *One Time Pad* (algoritma simetris) akan dihasilkan sebuah perangkat lunak untuk meningkatkan keamanan pada pesan teks yang membuat enkripsi/dekripsi pesan dengan *session-key One Time Pad* menghasilkan berbagai pesan karakter yang bersandi seperti simbol yang sulit untuk diketahui *cybercriminal* dan diamankan dengan kunci *public* RSA-CRT dalam bentuk angka yang sulit diketahui sehingga mampu meningkatkan tingkat keamanan kunci pesan.

Kata Kunci : Algoritma *One Time Pad*, Algoritma RSA-CRT, *Hybrid Cryptosystem*, Pengamanan Teks

KATA PENGANTAR

Puji syukur kepada Allah SWT atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas Akhir ini disusun untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Dalam menyelesaikan Tugas Akhir ini banyak pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung. Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih kepada pihak-pihak yang telah membantu penulis dalam menyelesaikan Tugas Akhir ini, yaitu kepada:

1. Kedua Orang Tua serta keluarga penulis tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama mengikuti dan melaksanakan perkuliahan di Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya hingga penulis dapat menyelesaikan Skripsi ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Ibu Alvi Syahrini Utami, M.Kom, selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Al Farissi, M. Cs, dan Bapak Osvari Arsalan, M.T. sebagai pembimbing Tugas Akhir yang mengarahkan dan memberi motivasi dalam proses pengerjaannya

5. Bapak Kanda Januar Miraswan, M.T. selaku dosen pembimbing akademik, yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan.
6. Ibu Novi Yusliani, M.T. dan Bapak Kanda Januar Miraswan, M.T. sebagai Dosen penguji, yang telah memberikan masukkan dan dorongan dalam proses pengerjaan Tugas Akhir.
7. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Mbak Winda dan Kak Ricy serta seluruh staf tata usaha yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.
9. Para teman seperjuangan Ahmad Yasykur Luthfi, Altundri Wahyu, M.Sultan Al-Farid, Syechki Al-Qodri, Rafliandi Ardana, Farhan Rizky Albimanzura, Clarina Juliatuty Pratiwi, Nadya Anggraini, Anisa Aulia, M. Rifqi Dzaky, dan teman – teman lainnya yang telah membantu dalam menyelesaikan tugas akhir .
10. Teman-teman dari kelas IF REG C 2018, kakak tingkat, adik tingkat, serta teman-teman lainnya yang telah mendengarkan keluh kesah penulis serta memberikan berbagai masukkan selama menempuh Pendidikan di Fakultas Ilmu Komputer Universitas Sriwijaya.
11. BEM KM Fasilkom Unsri Kabinet Gelora Juang, BPH HMIF Fasilkom Unsri, BEM KM Fasilkom Unsri Kabinet Lentera Karya yang telah memberikan kesempatan penulis dalam berkarya serta turut andil dalam menjalankan berbagai

tugas yang diberikan sehingga penulis dapat menerapkan tugas tersebut ke lingkungan yang lebih luas.

12. Semua orang yang tak tertuliskan dalam kata pengantar ini namun turut membantu dan melancarkan dalam proses untuk mencapai salah satu syarat gelar sarjana ini.

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 Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, 3 Agustus 2022

Muhammad Febriansyah
NIM.09021281823030

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab ini akan menjelaskan mengenai latar belakang penelitian judul skripsi "**Implementasi Algoritma RSA-CRT dan Algoritma *One Time-Pad* Secara *Hybrid Cryptosystem* pada Pengamanan Teks**", rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan skripsi.

1.2 Latar Belakang

Komunikasi adalah salah satu sifat dasar manusia yang gunanya untuk berinteraksi satu sama lain. Metode yang digunakan manusia untuk berkomunikasi berkembang seiring berjalannya waktu. Salah satunya adalah menggunakan teks atau tulisan yang mana sarana tersebut berfungsi untuk menyampaikan pesan kepada penerimanya. Pesan tersebut dapat berisi suatu informasi yang bersifat rahasia didalamnya. Besar kemungkinan pesan tersebut disadap oleh pihak-pihak yang tidak bertanggung jawab dimana isi dari pesan tersebut bisa diketahui oleh pihak yang tidak bertanggung jawab dan mengalami perubahan sebelum sampai ke penerima. Maka dari itu pengamanan teks merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi yang ada pada pesan tersebut.

Berbagai algoritma telah dikembangkan baik algoritma simetris maupun algoritma asimetris dengan berbagai kelebihan dan kekurangannya. Oleh karena itu, pada penelitian ini akan menggunakan metode *Hybrid*, yang mana akan dilakukan

proses enkripsi dan dekripsi menggunakan kombinasi algoritma kriptografi asimetris dan simetris. *Hybrid Cryptosystem* adalah kombinasi kriptografi simetris pada proses enkripsi dan dekripsinya yang kemudian kunci dari hasil proses kriptografi simetris tersebut di enkripsi dan dekripsi pula menggunakan kriptografi asimetris (Rachmawati et al., 2018). Pengirim menghasilkan kunci simetris untuk mengenkripsi pesan. Kunci kemudian dienkripsi menggunakan kunci publik penerima. Di sisi penerima, menerima dua *cyphertext*: *cyphertext* kunci simetris dan *cyphertext* pesan asli. Penerima menggunakan kunci privat untuk mendekripsi cipherteks kunci simetris, dan kemudian menggunakan kunci tersebut untuk mendekripsi cipherteks pesan asli.

Pada penelitian ini, proses *hybrid cryptosystem* menggunakan algoritma RSA-CRT sebagai algoritma asimetris dan algoritma *One Time Pad* sebagai algoritma simetris. Algoritma *One Time Pad* adalah sejenis algoritma simetri. *One Time Pad* adalah algoritma yang sempurna dan tidak bisa dipecahkan *Unbreakable Cypher* (Munir, 2006). Algoritma ini kelemahannya adalah kunci yang digunakan harus benar-benar acak dan panjang. Kuncinya harus sama dengan panjang pesan (Prameswara, 2012). Algoritma RSA-CRT adalah algoritma asimetris yang digunakan dalam penelitian ini. Enkripsi dan dekripsi kunci menggunakan kunci yang berbeda yaitu kunci publik dan pribadi. Kunci publik digunakan untuk proses enkripsi kunci sedangkan kunci privat digunakan untuk proses dekripsi kunci. Algoritma RSA-CRT (Rivest Shamir Adleman – Chinese Remainder Theorem), memberikan keuntungan dalam meningkatkan keamanan kunci (Paul et al. 2011).

Berdasarkan latar belakang, bahwa meningkatkan keamanan pada pesan teks

dapat dilakukan menggunakan algoritma RSA-CRT dan Algoritma *One Time Pad*. Algoritma RSA-CRT akan digunakan untuk mengamankan kunci dari algoritma *One Time Pad*.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah penulis uraikan di atas, rumusan masalah pada penelitian ini adalah:

1. Bagaimana membangun perangkat lunak *Hybrid Cryptosystem* Menggunakan Algoritma RSA-CRT dan Algoritma *One Time Pad?*
2. Bagaimana kinerja algoritma RSA-CRT dan algoritma *One Time Pad* terhadap pengamanan teks?

1.4 Tujuan

1. Menghasilkan perangkat lunak *Hybrid Cryptosystem* menggunakan algoritma RSA-CRT dan algoritma *One Time Pad.*
2. Mengetahui kinerja algoritma RSA-CRT dan algoritma *One Time Pad* terhadap metode *Hybrid Cryptosystem*.

1.5 Manfaat

1. Menambah pengetahuan penulis dalam melakukan proses enkripsi dan dekripsi suatu pesan teks dengan menggunakan algoritma *One Time-Pad* dan algoritma RSA-CRT.
2. Penelitian ini diharapkan dapat bermanfaat untuk meningkatkan keamanan teks yang bersifat rahasia.
3. Sebagai bahan referensi bagi peneliti lain yang ingin membahas topik yang terkait dengan penelitian ini.

1.6 Batasan Masalah

1. Tipe data yang dienkripsi dan dekripsi adalah plainteks berupa *file* .txt dengan karakter ASCII.
2. Penelitian akan menguji *avalanche effect* pengamanan kunci serta kecepatan enkripsi dan dekripsi dari *Hybrid Cryptosystem* (RSA-CRT dan *One Time Pad*).

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini terdiri dari beberapa bagian utama yang dijelaskan sebagai berikut.

BAB I. PENDAHULUAN

Pada bab ini berisi tentang latar belakang, rumusan masalah, tujuan dan manfaat

penelitian, batasan masalah/ruang lingkup, metodologi penelitian, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan dibahas dasar-dasar teori yang digunakan dalam penelitian, seperti definisi-definisi kriptografi, Algoritma RSA-CRT, Algoritma One-Time Pad, dan beberapa penelitian yang relevan terhadap skripsi.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan tahapan-tahapan yang dilakukan dalam penelitian ini. Setiap program penelitian dijelaskan secara rinci dengan mengacu pada Kerangka. Di akhir bab ini, berisi desain manajemen proyek untuk melakukan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab ini menjelaskan lingkungan desain dan implementasi Hybrid Kriptosistem menggunakan Algoritma RSA-CRT dan Algoritma One-Time Pad, implementasi program hasil eksekusi, dan hasil pengujian.

BAB V. HASIL DAN ANALISIS PENELITIAN

Bab ini menyajikan hasil tes berdasarkan prosedur yang direncanakan. Analisis tersebut dijadikan sebagai dasar untuk menarik kesimpulan dalam penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Bab ini menarik kesimpulan dari semua uraian pada bab sebelumnya dan juga

memberikan saran bahwa diharapkan dapat membantu mengimplementasikan *Hybrid Cryptosystem* ini.

1.8 Kesimpulan

Berdasarkan Penjelasan diatas Komunikasi adalah salah satu sifat dasar manusia yang gunanya untuk berinteraksi satu sama lain. Metode yang digunakan manusia untuk berkomunikasi berkembang seiring berjalannya waktu. Salah satunya adalah menggunakan teks atau tulisan yang mana sarana tersebut berfungsi untuk menyampaikan pesan kepada penerimanya. Pesan tersebut dapat berisi suatu informasi yang bersifat rahasia didalamnya. Maka dari itu keberadaan dan implementasi Kriptografi sangat dibutuhkan dan diharapkan dengan adanya penelitian ini dapat menambah ilmu pengetahuan dan implementasi terkait *Hybrid Cryptosystem* terkhususnya menggunakan Algoritma RSA-CRT dan Algoritma *One Time Pad*.

DAFTAR PUSTAKA

Abid, R., 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*. https://doi.org/10.1007/s00779-021-01607-3

Arutselvan, B., & Maheswari, R. (2013). *Crt Based Rsa Algorithm For Improving Reliability And Energy Efficiency With Kalman Filter In Wireless Sensor Networks*. *4*(5), 1924–1929.

Assafli, H. T., & Hashim, I. A. (2020). Security enhancement of AES-CBC and its performance evaluation using the avalanche effect. *2020 3rd International Conference on Engineering Technology and Its Applications, IICETA 2020*, 7–11. https://doi.org/10.1109/IICETA50496.2020.9318803

Garg, D., & Verma, S. (2009). Improvement over public key cryptographic algorithm. *2009 IEEE International Advance Computing Conference, IACC 2009*, *March*, 734–739. https://doi.org/10.1109/IADCC.2009.4809104

Karuppiah, M., Ramanujam, S., & Professor, A. (2011). Designing an algorithm with high Avalanche Effect. *IJCSNS International Journal of Computer Science and Network Security*, *11*(1), 106. https://www.researchgate.net/publication/266468045

Kuppuswamy, P., & Al-Khalidi, S. Q. Y. (2014). Hybrid encryption/decryption technique using new public key and symmetric key algorithm. *International Journal of Information and Computer Security*, *6*(4), 372–382. https://doi.org/10.1504/IJICS.2014.068103

Paul, V., & S, R. P. (2011). A Hybrid Crypto System based on a new Circle-Symmetric key Algorithm and RSA with CRT Asymmetric key Algorithm for E-commerce Applications. *International Journal of Computer Applications*, *Icvci*, 14–18.

Rachmawati, D., Sharif, A., Jaysilen, & Budiman, M. A. (2018). Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm. *IOP Conference Series: Materials Science and Engineering*, *300*(1), 0–7. https://doi.org/10.1088/1757-899X/300/1/012042

Romindo, J. (2020). Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security. *International Journal of Information*

System & Technology Akreditasi, *4*(1), 471–481.
Saragih, N. E. (2018). Implementasi Algoritma *One Time Pad* pada Pesan. *Jurnal Ilmiah MATRIK*, *Vol.20 No.*(3), 31–40.

Ariyus, D. (2008). Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi. ANDI: Yogyakarta

Munir, Rinaldi. (2006). Kriptografi. Informatika: Bandung

Prameswara, G. 2013. Implementasi Algoritma *One Time Pad* pada data teks dan Knapsack pada kunci. Skripsi. Universitas Sumatera Utara.

Arief, A., & Saputra, R. (2016). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging. Scientific Journal of Informatics, 3(1), 46-54.

Stein, C., Cormen, T., Rivest, R., & Leiserson, C. (2001). Introduction to algorithms. The MIT Press, 31(77), 13.M