ANALISIS PERBANDINGAN EFISIENSI ALGORITMA KUNCI PUBLIK RABIN-P DAN ALGORITMA KUNCI PUBLIK RSA-CRT PADA PENGAMANAN PESAN

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

Oleh:

Robi Hidayat
NIM: 09021381722088

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN SKRIPSI

ANALISIS PERBANDINGAN EFISIENSI ALGORITMA KUNCI PUBLIK RABIN-P DAN ALGORITMA KUNCI PUBLIK RSA-CRT PADA PENGAMANAN PESAN

Oleh:

Robi Hidayat

NIM: 09021381722088

Palembang, Januari 2022

Pembimbing I

Dr. Abdiansah, S. Kom., M.Cs.
NIP. 198410012009121005

Pembimbing II

Mastura Diana Marieska, M.T
NIP. 198603212018032001

Mengetahui,

Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M. Kom
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari Kamis tanggal 06 Januari 2022 telah dilaksanakan ujian sidang skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Robi Hidayat
NIM : 09021381722088
Judul : Analisis Perbandingan Efisiensi Algoritma Kunci Publik Rabin-P dan Algoritma Kunci Publik RSA-CRT pada Pengamanan Pesan

1. Pembimbing I

   Dr. Abdiansah, S. Kom., M.Cs.
   NIP. 198410012009121005 .....

2. Pembimbing II

   Mastura Diana Marieska, M. T
   NIP. 198603212018032001 .....

3. Penguji I

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

4. Penguji II

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

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M. Kom.
NIP. 197812222006042003

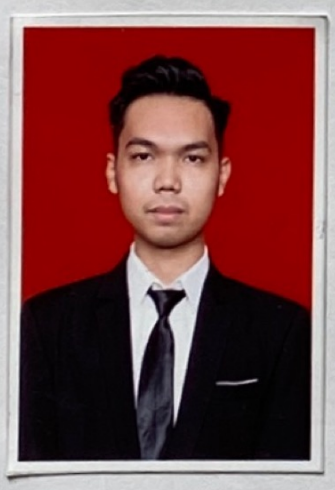
HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	: Robi Hidayat
NIM	: 09021381722088
Judul	: Analisis Perbandingan Efisiensi Algoritma Kunci Publik Rabin-P dan Algoritma Kunci Publik RSA-CRT pada Pengamanan Pesan
Hasil Pengecekan Software iThenticate/Turnitin	: 8%

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 akan bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan berlaku.

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



Palembang, Januari 2022

Robi Hidayat
NIM. 09021381722088

MOTTO DAN PERSEMBAHAN

MOTTO:

"Never regret a day in your life. Good days bring you happiness
And bad days give you experience"

"Tetap Semangat"

Kupersembahkan Karya Tulis ini kepada:

- **Allah SWT.**
- **Orang tua dan saudara kandung saya**
- **Keluarga besar saya**
- **Dosen pembimbing**
- **Sahabat dan teman seperjuangan ku**
- **Fakultas Ilmu Komputer Universitas Sriwijaya**

ANALYSIS OF EFFICIENCY COMPARISON OF RABIN-P PUBLIC KEY ALGORITHM AND RSA-CRT PUBLIC KEY ALGORITHM ON MESSAGE SECURITY

By:

Robi Hidayat
NIM: 09021381722088

ABSTRACT

The essential criteria of a good cryptographic algorithm are practical and efficient. Rabin-p and RSA-CRT cryptography were chosen to compare because these algorithms have similarities in the key generation process. The research aims to analyze the efficiency between Rabin-p and RSA-CRT against computational execution time measurement and algorithm complexity. The study used five test samples of text files in .txt with text contents of messages of 100- 500 words and repeated as many as 10 times each sample. The results resulted in an average Rabin-p low encryption time rate of 6.6 x 10^3 ms and a high of 12.5 x 10^4 ms, for the lowest decryption time value of 0.09 x 10^4 ms and a high of 0.11 x 10^4. The average time of RSA-CRT's lowest encryption time is 9.83 x 10^4 ms and the highest is 22.5 x 10^4 ms, for the lowest decryption of 0.17 x 10^4 and the highest is 0.28 x 10^4 ms. The results of the study foundthatrabin-p algorithm are more efficient than the RSA-CRT algorithm due to the average time of the Rabin-p algorithm encryption process. 9.93 x 10^5 ms while the RSA-CRT algorithm is 16.7 x 10^5 ms and the average processing time of the Rabin-p algorithm decryption is 0.10 x 10^5ms while the theRSA-CRT algorithm is 0.22 x 10^5 ms.

Keywords: Cryptography, Efficiency, Execution Time, Rabin-p, RSA-CRT

ANALISIS PERBANDINGAN EFISIENSI ALGORITMA KUNCI PUBLIK RABIN-P DAN ALGORITMA KUNCI PUBLIK RSA-CRT PADA PENGAMANAN PESAN

Oleh:

Robi Hidayat
NIM: 09021381722088

ABSTRAK

Kriteria penting algoritma kriptografi yang baik adalah praktis dan efisien. Dipilih kriptografi Rabin-p dan RSA-CRT untuk dibandingkan karena algoritma ini memiliki kemiripan dalam proses pembangkitan kunci. Penelitian bertujuan untuk menganalisis efisiensi antara Rabin-p dan RSA-CRT terhadap pengukuran waktu eksekusi komputasi dan kompleksitas algoritma. Penelitian menggunakan lima sampel uji file teks berformat .txt dengan isi teks pesan 100 – 500 kata dan diulang sebanyak 10 kali percobaan tiap sampelnya. Hasil penelitian menghasilkan rata-rata kecepatan waktu enkripsi terendah Rabin-p sebesar 6,6 x 10^3 ms dan tertinggi 12,5 x 10^4 ms, untuk nilai waktu terendah dekripsi 0,09 x 10^4 ms dan tertinggi 0,11 x 10^4. Rata-rata kecepatan waktu enkripsi terendah RSA-CRT sebesar 9,83 x 10^4 ms dan tertinggi 22,5 x 10^4 ms, untuk terendah dekripsi 0,17 x 10^4 dan tertinggi 0,28 x 10^4 ms. Hasil penelitian menyimpulkan bahwa algoritma Rabin-p lebih efisien dibandingkan algoritma RSA-CRT dikarenakan rata-rata waktu proses enkripsi algoritma Rabin-p sebesar 9,93 x 10^5 ms sedangkan algoritma RSA-CRT sebesar 16,7 x 10^5 ms dan waktu rata-rata proses dekripsi algoritma Rabin-p adalah 0,10 x 10^5ms sedangkan algoritma RSA-CRT adalah 0,22 x 10^5 ms.

Kata Kunci: Efisiensi, Kriptografi, Rabin-p, RSA-CRT, Waktu eksekusi

KATA PENGANTAR

Bismillahirrahmamanirrahim. Alhamdulillahirrabbil'alamin. Puji dan syukur penulis panjatkan kepada Allah SWT. Atas segala rahmat, nikmat, dan karunia-Nya lah penulis dapat menyelesaikan penyusunan skripsi ini dengan judul **"ANALISIS PERBANDINGAN EFISIENSI ALGORITMA KUNCI PUBLIK RABIN-P DAN ALGORITMA KUNCI PUBLIK RSA-CRT PADA PENGAMANAN PESAN**". Shalawat diiringi salam tak lupa penulis hadiahkan kepada baginda Nabi Muhammad SAW. Semoga penulis, ibu dan ayah penulis, kakek dan nenek penulis, saudara penulis, sahabat dan teman penulis, guru, dosen dan kaum muslimin & muslimat mendapat syafaat Beliau di Yaumil Mahsyar kelak. Aamiin ya Rabbal'Alamin. Skripsi ini disusun dan diajukan untuk memenuhi syarat perolehan gelar sarjana (S.Kom) pada Fakultas Ilmu Komputer di Universitas Sriwijaya.

Untuk selanjutnya penulis mengucapkan banyak terima kasih kepada pihak-pihak yang telah membantu dalam penyelesaian skripsi ini, yaitu :

1. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
2. Ibu Alvi Syahrini Utami, M.Kom, selaku Ketua Jurusan Teknik Informatika, Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. Abdiansah, M. Kom., M. Cs. Selaku Dosen Pembimbing I sekaligus Dosen Pembimbing Akademik penulis, yang telah sangat banyak membantu dalam membimbing, mengarahkan, membantu, memberi masukkan dan saran dalam penyelesaian skripsi ini.
4. Ibu Mastura Diana Marieska, M.T selaku Dosen Pembimbing II penulis, yang telah sangat banyak membantu dalam membimbing, mengarahkan, membantu, memberi masukkan dan saran dalam penyelesaian skripsi ini.
5. Bapak Osvari Arsalan, M.T dan Bapak Kanda Januar Miraswan, M.T, selaku Dosen Penguji penulis, yang telah memberi saran dan masukkan agar penulisan skripsi ini dapat menjadi lebih baik.
6. Seluruh Dosen yang telah mengajarkan penulis dengan memberikan informasi, pembelajaran, ilmu berharga dalam dunia perkuliahan penulis.
7. Mba Wiwin Juliani, selaku Admin jurusan Teknik Informatika Billingual, yang membantu dalam proses administrasi selama perkuliahan penulis.
8. Orang tuaku; H. Mulyadi Syafei dan Hj. Khuroifatisibti, S.Pd., yang sangat berperan dalam membantu penulis, dengan mendo'akan dan memberi dukungan baik dalam segi moril maupun materi kepada penulis.
9. Keluarga Besarku yang telah memberikan dukungan, hiburan, arahan, bahkan materi yang membuat penulis sangat terbantu dalam menyelesaikan perkuliahan dan skripsi ini.
10. Rusmansyah Putra dan Ahmad Emir Alfatah, selaku teman sekelas penulis di jurusan Teknik Informatika yang sangat baik untuk meluangkan waktunya membantu dalam proses penyelesaian perangkat lunak untuk skripsi penulis. Semoga Allah SWT meridhoi dan membalas kebaikanmu.

11. Bunga Ayu Ferdiyanti, selaku teman sekelas penulis di jurusan Teknik Informatika ini yang sangat baik mau membantu dalam perihal pengurusan berkas-berkas maupun materil yang dibutuhkan. Semoga Allah SWT meridhoi dan membalas kebaikanmu.
12. Stefany Naomi, Zhafirah Rahmadini, Sausan Syahirah, Bella Haprinda, M. Imam Renaldy Gumay, selaku teman seperjuangan dalam menyelesaikan pengerjaan skripsi bersama. Semoga Tuhan meridhoi dan membalas kebaikan kalian.
13. dr M. Ilham Dendy, Sp.PD., Shinta Octavia,S.E., M. Fadhly Dody, S.Tr. Ak., Destry, S.T., Adinda Dwi, S.T., Dhenada, S.Sos. teman rasa keluarga bagi penulis yang selalu mendukung, memotivasi, dan menghibur penulis untuk menyelesaikan penelitian ini. Semoga kebaikan kalian dibalas dan diridhoi oleh Allah SWT.
14. Primus Anindi, Yosua P. Siahaan, Josua Sihombing, Medita Deviana, Andreas Sianturi, Julia, Tazkiya selaku teman dari Belisario Choir yang selalu men-*support* penuh penulis. Semoga Tuhan membalas kebaikan kalian.
15. Teman – teman Teknik Informatika angkatan 2017.
16. Teman seperjuangan Ikatan Bujang Gadis Kampus Sumatera Selatan 2021.

Kakak dan adik tingkat penulis di Fakultas Ilmu Komputer yang memberikan banyak informasi dan dukungan saat pemberkasaan untuk menyelesaikan skripsi ini.

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab ini membahas latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian serta batasan masalah. Bab ini juga akan memberikan penjelasan umum mengenai keseluruhan penelitian.

1.2 Latar Belakang Masalah

Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial, hal ini tak terlepas dari peran komputer digital dan elektronik. Informasi atau pesan dapat dikirim dalam hitungan detik meskipun menempuh jarak yang sangat jauh. Pesan juga dapat disimpan dalam kurun waktu yang lama tanpa perlu memikirkan pemakaian media penyimpanan yang besar dan khawatir jika pesan mengalami kerusakan.

Namun seiring perkembangan teknologi, media elektronik juga dapat menjadi ancaman yang disebabkan oleh kemudahan akses informasi serta lemahnya sistem keamanan. Berdasarkan data dari Badan Siber dan Sandi Negara Republik Indonesia (BSSN RI) (*Rekapitulasi Insiden Web Defacement*, 2020) terdapat 88.414.296 kasus serangan siber yang terjadi pada bulan Januari sampai bulan April 2020 dengan 43% dari total keseluruhan kasus merupakan aktivitas serangan berupa *information gathering*. Menurut *Risk Based Security* (2020) menerbitkan laporan pelanggaran data bahwa pada tiga bulan pertama tahun 2020 sektor

informasi menduduki peringkat pertama sebagai sektor yang melaporkan pelanggaran data terbanyak dengan 215 laporan dari 1.473 atau 14,5% dari total keseluruhan. Ini menandakan pesan atau informasi yang seharusnya bersifat rahasia dapat diakses oleh orang yang tidak berhak. Oleh karena itu, dibutuhkan pengamanan untuk melakukan pencegahan atas sampainya informasi ke tangan yang tidak berhak. Banyak hal yang dapat dilakukan untuk meningkatkan keamanan, salah satunya dengan menyandikan isi pesan menjadi suatu kode – kode yang tidak dimengerti atau yang sering dikenal dengan teknik kriptografi.

Banyaknya pilihan jenis metode kriptografi dalam melindungi keamanan data, membuat pengguna bingung menentukan jenis metode kriptografi yang ideal untuk digunakan. Faktor seperti tujuan, waktu proses, keamanan kunci sampai kerumitan algoritma juga menjadi bahan pertimbangan untuk memilih metode kriptografi. Pada penelitian ini akan digunakan dua algoritma kriptografi, yaitu algoritma Rabin-p dan RSA-CRT untuk dijadikan sebagai objek perbandingan pada penelitian ini.

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk mendapatkan kunci *private*. Namun ukuran *private key* yang terlalu besar akan mengakibatkan proses dekripsi yang cukup lambat, terutama untuk ukuran pesan yang besar. Untuk itu dibutuhkan penggunaan teorema *Chinese Remainder Theorem* (CRT) pada proses dekripsi pesan yang mampu membantu kinerja algoritma RSA menjadi lebih baik. CRT akan memperpendek ukuran bit dan terbukti sistem kriptografi RSA-

CRT memiliki waktu komputasi yang lebih singkat daripada sistem kriptografi RSA biasa yaitu sekitar 4 kali lebih cepat (Yulianti, 2020)

Algoritma Rabin-p diperkenalkan oleh Michael O. Rabin pada tahun 1979. Rabin-p dinamai rabin dengan tambahan yang melambangkan bahwa skema yang diusulkan hanya menggunakan satu prima sebagai kunci dekripsi. Algoritma Rabin-p merupakan turunan dari Algoritma Rabin, dimana Algoritma Rabin turunan dari Algoritma RSA (Mubaroka, 2018).

Pada penelitian terkait yang menjadi rujukan utama penelitian ini, dilakukan percobaan perbandingan antara algoritma RSA dengan algoritma Rabin-p. Didapatkan hasil bahwa tingkat keamanan keduanya relatif sama dengan mengandalkan kekuatan sulitnya memfaktorkan bilangan yang besar. Pada penelitian ini juga menyebutkan bahwa algoritma Rabin-p memiliki waktu proses komputasi yang lebih cepat dibandingkan algoritma RSA. Hal ini didasari karena proses perhitungan enkripsi dan dekripsi algoritma RSA memiliki nominal yang lebih besar dibanding besaran nominal pada algoritma Rabin-p (Purwasito, 2017)

Penelitian tersebut menjadi dasar dari penelitian ini, bedanya pada penelitian ini yang akan dibandingkan adalah algoritma Rabin-p dengan algoritma RSA yang telah ditambahkan dengan *Chinese Remainder Theorem* (CRT). Oleh karena itu penelitian ini bertujuan untuk mengetahui efisiensi dari kedua algoritma tersebut dengan melihat dari aspek kecepatan komputasi melalui hasil nilai *execution time* yang dibandingkan dengan analisis algoritma dari proses enkripsi dan dekripsi pesan teks. Berdasarkan dari uraian latar belakang diatas peneliti ingin melakukan

penelitian yang berjudul "***Analisis Perbandingan Efisiensi Algoritma Kunci Publik Rabin-p dan Algoritma Kunci Publik RSA-CRT pada Pengamanan Pesan***".

1.3 Rumusan Masalah

Berdasarkan latar belakang tersebut, fokus permasalahan yang akan dibahas pada penelitian ini adalah

1. Bagaimana pengembangan aplikasi perangkat lunak perbandingan algoritma Rabin-p dan algoritma RSA-CRT pada pengamanan pesan?
2. Bagaimana perbandingan efisiensi dari algoritma Rabin-p dan algoritma RSA-CRT ditinjau dari analisis algoritma dan *execution time*?

1.4 Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah:

1. Mengembangkan aplikasi perangkat lunak perbandingan algoritma Rabin-p dan algoritma RSA-CRT pada pengamanan pesan.
2. Menganalisis nilai hasil perbandingan kecepatan waktu eksekusi dan analisis kompleksitas algoritma Rabin-p dan algoritma RSA-CRT pada proses enkripsi dan dekripsi pesan.

1.5 Manfaat Penelitian

1. Penelitian ini diharapkan dapat menambah informasi ilmiah dibidang kriptografi khususnya algoritma Rabin-p dan algoritma RSA-CRT.
2. Hasil penelitian ini diharapkan dapat menjadi bahan referensi bacaan dan studi banding bagi peneliti lain yang ingin membahas topik yang terkait dengan penelitian ini

1.6 Batasan Masalah

1. Pesan yang digunakan berbentuk teks yang berekstensi *txt*.
2. *Plaintext* dan *ciphertext* yang dibuat berdasarkan kode ASCII (256 karakter).
3. Implementasi berupa enkripsi dan dekripsi pesan saja dan tidak melakukan kriptanalisis.
4. Hanya menghitung *execution time* dalam *millisecond* (ms).
5. Pengembangan aplikasi ini diimplementasikan dengan menggunakan bahasa java.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini terdiri dari beberapa bagian utama sebagai berikut :

BAB I. PENDAHULUAN

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

BAB II. KAJIAN LITERATUR

Pada bab ini akan membahas mengenai dasar-dasar teori yang digunakan dalam penelitian, mulai dari penjelasan mengenai sistem kriptografi sampai semua yang digunakan pada tahapan alasisis, perancangan, dan implementasi.

BAB III. METODOLOGI PENELITIAN

Pada bab ini akan dibahas mengenai tahapan yang akan dilakukan pada penelitian. Untuk setiap tahapan rencana penelitian dideskripsikan secara rinci dengan mengacu kepada kerangka kerja. Pada akhir bab akan diisi dengan perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini akan dibahas mengenai perancangan pengembangan perangkat lunak perbandingan algoritma kriptografi Rabin-p dan algoritma kriptografi RSA-CRT serta pengujian perangkat lunak.

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada bab ini dijelaskan hasil pengujian berdasarkan langkah-langkah yang telah direncanakan. Analisis diberikan sebagai basis dari kesimpulan yang diambil dalam penelitiani ini.

BAB VI. KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari penelitian yang telah dilakukan serta berisi saran yang diharapkan dapat membantu untuk keperluan pengembangan penelitian berikutnya.

1.8 Kesimpulan

Pada bab ini telah dibahas secara umum mengenai latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah serta sistematika penulisan terkait penelitian yang akan dilakukan.

4.3 Kesimpulan

Pada bab ini telah jelaskan mengenai analisis perancangan, implementasi serta pengujian perangkat lunak perbandingan metode kriptografi Rabin-p dan metode kriptografi RSA-CRT pada pengamanan pesan. Proses pengembangan perangkat lunak menggunakan metode *Rational Unified Process* (RUP) telah dilaksanakan dengan baik sesuai dengan rancangan yang telah dijabarkan serta telah memenuhi evaluasi pengujian *black box*.

DAFTAR PUSTAKA

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.

Asbullah, M. A., Ariffin, M. R. K., & Mahad, Z. (2016). Analysis on the Rabin-p cryptosystem. In *AIP Conference Proceedings* (Vol. 1787, No. 1, p. 080012). AIP Publishing LLC.

Asbullah, M. A., & Kamel, M. R. (2019). Design and Analysis of Rabin-p Key Encapsulation Mechanism for CyberSecurity Malaysia MySEAL Initiative. *IJCR*, *9*(1), 19-51.

Ermedahl, A., & Engblom, J. (2007). Execution Time Analysis for Embedded Real-Time Systems.

Hansen, K., Larsen, T., & Olsen, K. (2010). On the efficiency of fast RSA variants in modern mobile phones. *arXiv preprint arXiv:1001.2249*.

Kruchten, P. (2000). *The Rational Unified Process An Introduction, Second Edition*.

Mid Year Report Data Breach (2020). Risk Based Security.

Mubaroka, M. A. (2018). Perbandingan Efisiensi Algoritma Rabin-p dan Algoritma RSA pada Pengamanan File Txt Berbasis Desktop.

Munir, R. (2006). Kriptografi. *Informatika, Bandung*.

Muzaki, Almeiza Arvin (2020). Studi Kompleksitas Algoritma Enkripsi Teks Simetri dan Asimetri.

Nasution, N. R. (2017). Kombinasi RSA-CRT dengan Random LSB untuk Keamanan Data di Kanwil Kementerian Agama Prov. Sumatera Utara. *Query: Journal of Information Systems*, *1*(01).

Panjaitan, Z., Ibnutama, K., & Suryanata, M. G. (2019). Penggunaan Chinese Reminder Theorem (CRT) pada Algoritma RSA. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, *18*(1), 41-46.

Perwitasari, R., Afawani, R., & Anjarwani, S. E. (2020). Penerapan Metode Rational Unified Process (RUP) Dalam Pengembangan Sistem Informasi Medical Check Up Pada Citra Medical Centre. *Jurnal Teknologi Informasi, Komputer, dan Aplikasinya (JTIKA)*, *2*(1), 76-88.

Purwasito, A. (2017). Analisis Pesan. *Jurnal The Messenger*, *9*(1), 103-109.

Pusparani, N. A. (2009). Analisis RSA dengan Penambahan Chinese Remainder Theorem untuk Mempercepat Proses Dekripsi.

Rahanady, T. (2012). Perbandingan Algoritma RSA dan Rabin.

Rekapitulasi Insiden Web Defacement. (2020). Badan Siber dan Sandi Negara.

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

Sulistiyorini, S., & Prihanto, A. (2019). Perbandingan Efisiensi Algoritma RSA dan RSA-CRT Dengan Data Teks Berukuran Besar. *Journal of Informatics and Computer Science (JINACS)*, *1*(02).

Sutarno, H. (2007). Enkripsi Data Sistem Kriptografi Kunci Publik Menggunakan Algoritma Diophantine. *Jurnal Pengajaran MIPA*, *9*(2), 8-20.

Yulianti, W. (2020). Perbandingan Kinerja Algoritma Elgamal dan Algoritma Rabin-p pada Pengamanan File BMP.