# PENGGUNAAN *DIGITAL SIGNATURE* DENGAN ALGORITMA *HYBRID CRYPTOSYSTEM* ELGAMAL, RSA, DAN FUNGSI *HASH* MD5 PADA APLIKASI *FILE AUTHENTICITY VERIFICATION* BERBASIS JAVA

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


Oleh :

Zora Cahya Ardiya Prameswari

NIM : 09021281823056

**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA**

**2023**

## LEMBAR PENGESAHAN SKRIPSI

# PENGGUNAAN DIGITAL SIGNATURE DENGAN ALGORITMA HYBRID CRYPTOSYSTEM ELGAMAL, RSA, DAN FUNGSI HASH MD5 PADA APLIKASI FILE AUTHENTICITY VERIFICATION BERBASIS JAVA

Oleh :

Zora Cahya Ardiya Prameswari
09021281823056

Palembang, 10 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 **Jumat** tanggal **23 Desember 2022** telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Zora Cahya Ardiya Prameswari
N I M : 09021281823056
Judul : Penggunaan *Digital Signature* dengan Algoritma *Hybrid Cryptosystem* ElGamal, RSA, dan Fungsi *Hash* MD5 pada Aplikasi *File Authenticity Verification* Berbasis Java

dan dinyatakan **LULUS**.

1. Ketua

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

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 | : Zora Cahya Ardiya Prameswari |
| NIM | : 09021281823056 |
| Program Studi | : Teknik Informatika Bilingual |
| Judul Skripsi | : Penggunaan *Digital Signature* dengan Algoritma *Hybrid Cryptosystem* ElGamal, RSA, dan Fungsi *Hash* MD5 pada Aplikasi *File Authenticity Verification* Berbasis Java |

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, 10 Januari 2023


Zora Cahya Ardiya Prameswari
NIM. 09021281823056

# MOTTO DAN PERSEMBAHAN

- *No matter what people say, just keep going and believe in yourself.*
- "*Do not go where the path may lead, go instead where there is no path and leave a trail*." - Ralph Waldo Emerson

Kupersembahkan karya tulis ini kepada:

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

**JAVA BASED FILE AUTHENTICITY VERIFICATION APPLICATION USING DIGITAL SIGNATURE WITH HYBRID CRYPTOSYSTEM OF ELGAMAL, RSA, AND MD5 HASH FUNCTION**

**By:**

**Zora Cahya Ardiya Prameswari**
**09021281823056**

## ABSTRACT

Elgamal and RSA algorithms are asymmetric cryptographic algorithms. Elgamal's advantage is the complexity of discrete logarithms while RSA's is the complex factorization of large numbers. MD5 is a hash function with a speed greater than SHA256. Digital signature is a cryptographic technique used to sign digital documents. Hybrid Cryptosystem utilizes different algorithms to take advantage of each algorithm. This research goals are to implement hybrid cryptosystem using Elgamal, RSA, and MD5 and to measure the performance. MD5 is used to encrypt plaintext into text of 16 bytes. Elgamal is used for first layer encryption and second layer decryption. RSA is used for second layer encryption and first layer decryption. In this study, the software successfully detected 100% data manipulation. In the AE test, Elgamal's average AE value is 49.77%, 46.88% for RSA and 50.009% for hybrid. These values are considered good because still in the range of good AE values. In processing time test, the encryption and verification processing time without Elgamal and RSA is faster, with a difference of 190 ms for encryption using 1024 *bit* key and 430 ms using 2048 *bit* key, and 20 ms for verification using 1024 *bit* key and 120 ms using 1024 *bit* key. File size affects encryption and verification processing time. However, the processing time for files of different sizes is affected by the size of generated key. The usage of 1024 *bit*s key and 2048 *bit*s key increases the encryption time by 17% and the verification time by 179%. The software manages to detect changes, with a good average AE value of 50.009%. However, it hasn't been any faster than without using the hybrid.

**Keywords:** Cryptography, Hybrid cryptosytem, Digital Signature, MD5, Elgamal, and RSA.

**PENGGUNAAN *DIGITAL SIGNATURE* DENGAN ALGORITMA *HYBRID CRYPTOSYSTEM* ELGAMAL, RSA, DAN FUNGSI *HASH* MD5 PADA APLIKASI *FILE AUTHENTICITY VERIFICATION* BERBASIS JAVA**

**Oleh:**

**Zora Cahya Ardiya Prameswari**
**09021281823056**

## ABSTRAK

Algoritma Elgamal dan RSA adalah algoritma kriptografi asimetris. Kelebihan Elgamal adalah kerumitan pada logaritma diskrit sedangkan RSA adalah faktorisasi bilangan besar yang kompleks. MD5 merupakan fungsi *hash* dengan kecepatan lebih besar dari SHA256. *Digital signature* adalah teknik kriptografi untuk menanda tangani dokumen digital. *Hybrid Cryptosystem* adalah kriptografi yang memanfaatkan algoritma yang berbeda untuk memanfaatkan keunggulan tiap algoritma. Penelitian bertujuan untuk menerapkan *hybrid cryptosytem* menggunakan Elgamal, RSA, dan MD5 serta mengukur performa algoritma *hybrid*. MD5 digunakan untuk mengenkripsi *plaintext* menjadi 16 *bytes*. Elgamal digunakan untuk enkripsi lapisan pertama dan dekripsi lapisan kedua. RSA digunakan untuk enkripsi lapisan kedua dan dekripsi lapisan pertama. Pada penelitian ini, perangkat lunak berhasil mendeteksi perubahan *file* sebanyak 100%. Pada pengujian Avalanche, nilai AE rata – rata Elgamal adalah 49.77%, 46.88% untuk RSA dan 50.009% untuk *hybrid.* Rata – rata ini termasuk dalam *range* nilai AE yang baik. Pada pengujian waktu pemrosesan, waktu pemrosesan enkripsi dan verifikasi tanpa Elgamal dan RSA lebih cepat, dengan selisih 190 ms untuk enkripsi menggunakan kunci berukuran 1024 *bit*, 430 ms untuk enkripsi menggunakan kunci berukuran 2048 *bit*, 20 ms untuk verifikasi menggunakan kunci berukuran 1024 *bit*, dan 120 ms untuk verifikasi menggunakan kunci berukuran 1024 *bit*. Ukuran *file* mempengaruhi waktu pemrosesan. Namun, untuk *file* dengan ukuran yang berbeda dipengaruhi besar kunci yang dibangkitkan. Kunci dengan ukuran 1024 *bit* dan 2048 *bit* meningkatkan waktu enkripsi sebesar 17% dan waktu verifikasi sebesar 179%. Perangkat lunak berhasil mendeteksi perubahan, dengan rata – rata nilai AE yang baik sebesar 50.009%. Namun, belum lebih cepat daripada tanpa menggunakan *hybrid*.

**Kata Kunci:** Kriptografi, *Hybrid cryptosytem, Digital Signature*, MD5, Elgamal, dan RSA.

# KATA PENGANTAR

*Alhamdulillahi rabbil 'alamin*. Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan kesehatan, serta tak lupa shalawat dan salam senantiasa tercurahkan kepada junjungan Nabi Muhammad SAW. Syukur selalu dipanjatkan kepada Allah SWT atas limpahan nikmatnya, baik dari segi kesehatan fisik maupun mental, sehingga penulis dapat menyelesaikan skripsi dengan judul "**Penggunaan *Digital Signature* dengan Algoritma *Hybrid Cryptosystem* Elgamal, RSA, dan Fungsi *Hash* MD5 pada Aplikasi *File Authenticity Verification* Berbasis Java**", yang diajukan untuk menyelesaikan pendidikan program Strata-1 pada jurusan teknik informatika Universitas Sriwijaya.

Pada skripsi ini, penulis mendapatkan banyak dukungan serta bantuan dari banyak pihak. Maka dari itu, pada kesempatan kali ini penulis ingin mengucapkan terimakasih banyak kepada pihak – pihak yang telah memberi dukungan, yaitu kepada:

1. Allah SWT yang telah memberi rahmat dan karunia-Nya sehingga skripsi ini dapat diselesaikan tepat waktu.
2. Nabi Muhammad SAW yang telah menjadi suri tauladan bagi umat manusia, terutama penulis sehingga penulis memiliki motivasi untuk melaksanakan dan menyelesaikan skripsi.
3. Orang tua yang paling saya sayangi, Papa Hendry M Nur, Mama Erna Arvita, kedua saudara lelakiku Marvell Chandriqa Alcafi dan M Rajhendra

Waranggana Pinggala, serta seluruh keluarga besar yang telah memberikan doa, dukungan, serta semangat yang tidak pernah putus.

4. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Alfarissi, M.Comp.Sc. dan Bapak Muhammad Qurhanul Rizqie, M.T., Ph.D. selaku pembimbing yang telah membimbing, memotivasi, serta membantu penulis dalam penyelesaian skripsi ini.
7. Ibu Nabila Rizky Oktadini, M.T. selaku pembimbing Akademik yang selalu membimbing dan memberikan saran selama masa perkuliahan penulis.
8. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Sahabat – sahabat saya, Arya Pradata, Cindy Wijaya, Dhiya Calista, Ihtiar Alfath Raden Pangestu, Defita Auli Ramadhia, Pretty Fujianti Febrivia, dan teman – teman lain yang tidak dapat penulis sebutkan satu – persatu, yang telah memberi dukungan, saran, dan bantuan yang tidak pernah berhenti selama ini.
10. Muhammad Arif Rahman selaku rekan yang selalu memberikan dukungan, saran, bantuan, dan semangat, serta motivasi penulis dalam penyelesaian skripsi.

11. Dan untuk semua pihak yang telah banyak membantu pengerjaan tugas akhir ini yang tidak dapat penulis sebutkan satu – persatu.

Semoga bantuan yang telah diberikan kepada penulis mendapatkan imbalan yang setimpal dari Tuhan Yang Maha Esa. Akhir kata, penulis menyadari bahwa tugas akhir ini masih jauh dari kata sempurna. Seperti kata pepatah, “tak ada gading yang tak retak”, begitu pula dengan penulisan tugas akhir ini. Untuk itu, penulis terbuka terhadap kritik dan saran yang membangun dalam penyempurnaan penelitian ini. Semoga penelitian ini dapat memberikan banyak manfaat bagi banyak pihak, *Aamiin*.

Palembang, 10 Januari 2023

Zora Cahya Ardiya Prameswari

# DAFTAR ISI

Halaman

# DAFTAR TABEL

Halaman

## DAFTAR GAMBAR

Halaman

# BAB I

# PENDAHULUAN

## 1.1 Pendahuluan

Bab pendahuluan akan membahas hal – hal umum mengenai penelitian yang berupa latar belakang penelitian, rumusan masalah, tujuan dari penelitian, manfaat yang didapat dari penelitian, batasan masalah penelitian dan sistematika penulisan.

## 1.2 Latar Belakang

Kemajuan teknologi adalah hal yang tidak bisa dihindari karena berdampingan dengan kemajuan ilmu pengetahuan yang ada. Perkembangan zaman yang semakin maju mempengaruhi perkembangan teknologi dengan pesat di era digital. Hal ini mengakibatkan penggunaan teknologi yang terus meningkat memicu tenaga kerja pada bidang teknologi informasi untuk terus mengembangkan perangkat lunak agar dapat digunakan dengan mudah dan nyaman.

Komputer telah menjadi bagian dari kehidupan sehari – hari. Teknologi yang semakin maju memudahkan penggunaan komputer yang mengakibatkan banyaknya manusia yang menggunakan komputer untuk menyelesaikan masalah sehari – hari. Namun, kemajuan teknologi juga dapat membawa pengaruh buruk, salah satunya adalah munculnya ancaman baru, yaitu kejahatan siber. Kejahatan siber adalah semua kegiatan yang menggunakan jaringan komputer untuk melakukan kejahatan. Beberapa contoh kejahatan siber yang sering terjadi adalah *phising*, *online harrashment*, pembajakan, dan penipuan.

Perkembangan teknologi yang terus berlanjut mengakibatkan munculnya banyak peluang kejahatan siber dengan cara – cara baru. Pakar teknologi informasi ditantang untuk terus menciptakan solusi yang akan menutup celah terjadinya kejahatan siber. Salah satu solusi dari tantangan ini adalah pengamanan data, yaitu tindakan untuk melindungi sistem, jaringan, dan program dari serangan siber yang mencakup setiap aspek keamanan informasi dari keamanan fisik perangkat keras, keamanan logis dari perangkat lunak, hingga kontrol administratif dan akses.

Kriptografi adalah salah satu bentuk pengamanan data yang menggunakan teknik penyembunyian pesan pada implementasinya. Penyembunyian pesan pada kriptografi dilakukan dengan cara mengubah naskah asli (*plaintext*) kedalam bentuk acak (*ciphertext*) dengan menggunakan kunci enkripsi sehingga naskah asli akan sulit untuk dibaca oleh pihak yang tidak memiliki kunci dekripsi. Ada tiga fungsi dasar dalam kriptografi, yaitu enkripsi, dekripsi dan kunci. Enkripsi merupakan proses penyembunyian pesan dimana naskah asli akan diacak dengan menggunakan teknik tertentu sehingga menjadi naskah yang tidak bisa dibaca (*chipertext*). Dekripsi merupakan proses mengembalikan informasi dengan cara mengubah kembali naskah tersandi (*chipertext*) kedalam bentuk naskah asli (*plaintext*). Kunci merupakan teknik yang digunakan untuk enkripsi maupun dekripsi. Kriptografi terdiri dari dua jenis, yaitu kriptografi simetri dan asimetri. Kriptografi simetri adalah jenis kriptografi yang menggunakan kunci yang sama pada enkripsi dan dekripsinya. Sedangkan kriptografi asimetri adalah jenis kriptografi yang menggunakan dua kunci berbeda pada enkripsi dan dekripsinya. Pada kriptografi

asimetri biasanya digunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi.

Keunggulan kriptografi asimetri adalah menggunakan kunci publik dan kunci privat. Hal ini dikarenakan hanya kunci privat yang perlu dijaga kerahasiaannya, dan beberapa algoritmanya dapat digunakan untuk memberi *digital signature* pada pesan.

*Digital signature* dapat digunakan untuk membuktikan keaslian dari suatu *file* digital dengan cara memastikan bahwa *file* yang diterima tidak mengalami perubahan selama pengiriman. Menurut Septiawan (2019) *digital signature* memenuhi setidaknya 2 syarat keamanan data dan teks, yaitu *authenticity* dan *nonrepudiation*. *Digital signature* diharapkan dapat membantu menjaga keaslian data dan menjamin integritas data.

Dalam penelitian ini, akan diimplementasikan *hybrid cryptosystem* dengan menggunakan RSA dan Elgamal, serta fungsi *hash* MD5 untuk membentuk *message digest*. Pada penelitian (Agung & Ferry, 2016) menyatakan beberapa kelebihan dari *hybrid cryptosystem*, diantaranya: (1) Kecepatan pada enkirpsi asimetri akan lebih cepat seperti kecepatan pada enkripsi simetri dengan menggunakan kombinasi dari enkirpsi simetri dan asimetri. (2) Memberikan pemecahan masalah waktu enkripsi asimetri yang terbilang lama dengan menggunakan enkripsi simetri yang 100 – 1000 kali lebih cepat. (3) Masalah pendistribusian kunci dan transmisi data pada enkripsi simetri dapat dipecahkan oleh enkripsi asimetri. (4) Performa dan pendistribusian kunci dapat meningkat

tanpa adanya pengurangan keamanan dengan penggunaan kombinasi enkripsi simetri dan asimetri.

Menurut Rivera et al. (2019) Algoritma Elgamal dikenal dengan kerumitan pada logaritma diskritnya. RSA memiliki kelebihan pada faktorisasi bilangan besar yang kompleks. Kedua algoritma adalah algoritma asimetris sehingga menggunakan dua kunci berbeda pada enkripsi dan dekripsinya. MD5 digunakan untuk menghasilkan *message digest* dengan ukuran 128 *bit*. Menurut Rachmawati (2017) kompleksitas dari algoritma MD5 sama seperti SHA256. Keunggulan dari MD5 terletak pada *running time*-nya yang lebih cepat dari SHA256.

## 1.3 Rumusan Masalah

Berdasarkan latar belakang diatas, maka didapatkan rumusan masalah sebagai berikut:

1. Bagaimana cara mengimplementasikan *hybrid cryptosystem* ke *digital signature* pada aplikasi *file authenticity verification*?
2. Bagaimana performa dari sistem yang dihasilkan?

## 1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Menerapkan *hybrid cryptosystem* ke *digital signature* pada aplikasi *file authenticity verification* dengan menggunakan algoritma RSA dan ElGamal.

2. Membandingkan performa sistem dengan menggunakan *hybrid cryptosystem* dibandingkan *digital signature* tanpa menggunakan *hybrid cryptosystem*.

## 1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Meningkatkan keamanan data dengan menggunakan *digital signature*.
2. Dapat digunakan sebagai nilai untuk uji banding performa antara sistem yang menggunakan *hybrid cryptosystem* dengan yang tidak menggunakannya.

## 1.6 Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Fokus dari penelitian adalah implementasi *hybrid cryptosystem* dengan menggunakan algoritma RSA dan Elgamal serta fungsi *hash* MD5 pada *digital signature*.
2. Membandingkan performa dari segi *Avalanche Effect* dan *processing time*.
3. Tipe data yang digunakan pada penelitian ini berupa *file* teks.

## 1.7 Sistematika Penulisan

Sistem penulisan tugas akhir sesuai dengan standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya, yaitu:

**BAB I. PENDAHULUAN**

Bab Pendahuluan akan membahas tentang dasar – dasar penulisan skripsi, seperti latar belakang penelitian, rumusan masalah, tujuan dari penelitian, manfaat yang didapat dari penelitian, batasan masalah penelitian dan sistematika penulisan.

**BAB II. KAJIAN LITERATUR**

Bab Kajian Literatur akan membahas tentang dasar – dasar teori yang digunakan pada penulisan skripsi, diantaranya adalah penjelasan mengenai kriptografi, *hybrid cryptosystem*, *digital signature*, algoritma RSA (*Rivest Shamir Adlemen*), algoritma Elgamal, dan fungsi *hash* MD5.

**BAB III. METODOLOGI PENELITIAN**

Bab Metodologi Penelitian akan membahas tentang tahapan – tahapan yang dilaksanakan pada penelitian. Rincian dari tiap tahapan akan dijelaskan pada bab ini. Perancangan manajemen proyek pada pelaksanaan penelitian juga dijelaskan pada bab ini.

**BAB IV. PENGEMBANGAN PERANGKAT LUNAK**

Bab Pengembangan Perangkat Lunak akan menjelaskan tentang proses yang dilalui pada pengembangan perangkat lunak. Metode yang digunakan adalah metode agile yang memiliki beberapa tahapan dengan tingkat fleksibilitas tinggi.

**BAB V. HASIL DAN ANALISIS PENELITIAN**

Bab Hasil dan Analisis Penelitian akan membahas tentang analisis hasil yang didapat dari pengembangan perangkat lunak. Disini, kesimpulan dari penelitian bisa didapatkan.

# BAB VI. KESIMPULAN DAN SARAN

Bab Kesimpulan dan Saran akan membahas tentang kesimpulan yang didapat dari penelitian serta saran yang dapat digunakan untuk mengembangkan perangkat lunak agar menjadi perangkat lunak yang lebih baik pada penelitian selanjutnya.

## 1.8 Kesimpulan

Pada bab ini, dapat disimpulkan bahwa masalah ancaman siber dapat diselesaikan dengan cara meningkat keamanan pada data. Salah satu cara untuk meningkatkan keamanan data adalah dengan menggunakan *digital signature* yang memenuhi setidaknya 2 syarat keamanan data dan teks, yaitu *authenticity* dan *nonrepudiation.* Penerapan *hybrid cryptosystem* pada *digital signature* diharapkan bisa meningkatkan keamanan pada data dan meningkatkan performa aplikasi.

# DAFTAR PUSTAKA


Abdurrachman, T., & Suteja, B. R. (2021). Pengembangan Sistem Informasi Asosiasi Jasa Konstruksi dengan Menerapkan Tanda Tangan Digital. *JuTISI (Jurnal Teknik Informatika dan Sistem Informasi), 7*(1), 217.

Agung, H., & Ferry. (2016). Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature. *Jatisi, 3*(1), 35.

Alfatah, A. E. (2021). *Sistem Pengamanan Pesan Menggunakan Kriptografi AES dan Digital Signature Berbasis Mobile.* Palembang.

Anshori, Y., Dodu, A. Y., & Wedananta, D. M. (2019). Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital. *Techno.COM, 18*(2), 111.

Apdilah, D., & Swanda, H. (2018). Penerapan Kriptografi RSA dalam Mengamankan File Teks Berbasis PHP. *JurTI (Jurnal Teknologi Informasi), 2*(1), 46.

Hakim, Z., & Rizky, R. (2018). Analisis Perancangan Sistem Informasi Pembuatan Paspor Di Kantor Imigrasi Bumi Serpong Damai TangerangBanten Menggunakan Metode Rational Unified Process. *Jutis, 6*(2), 105.

HR, A. H. (2021). *IMPLEMENTASI FUNGSI HASH MD5 DAN KRIPTOGRAFI ALGORITMA RSA PADA PEMBUATAN TANDA TANGAN DIGITAL.* Malang.

Hulu, Y., Simbolon , N., Tarigan, E. V., Bunawolo, M., & Turnip, M. (2020). Aplikasi Sistem Informasi Manajemen Sekolah Terintegrasi dengan Pendekatan Rational Unified Process. *Jikomsi, 3*, 11-17.

Mallouli, F., Hellal, A., Saeed, N. S., & Alzahrani, F. A. (2019). A Survey on Cryptography: comparative study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms. *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud) / 2019 5th IEEE*

*International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 174.

Munir, R. (2019). *Kriptografi*. Bandung: Informatika.

Muslih, & Handoko, L. B. (2022). PENGUJIAN AVALANCHE EFFECT PADA KRIPTOGRAFI TEKS MENGGUNAKAN AUTOKEY CIPHER. *STEKOM*, (p. 130).

Prayitno, A. (2017). ANALISA DAN IMPLEMENTASI KRIPTOGRAFI PADA PESAN RAHASIA MENGGUNAKAN ALGORITMA CIPHER TRANSPOSITION. *JESIK (Jurnal Elektronik Sistem Informasi dan Komputer)*, 1 & 4.

Pudoli, A., & Kusumaningsih, D. (2017). PENGGUNAAN HYBRID CRYPTOSYSTEM UNTUK ENKRIPSI DAN DEKRIPSI PESAN MESSENGER MENGGUNAKAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) DAN ADVANCED ENCRYPTION STANDARD (AES) DENGAN FIREBASE PADA ANDROID. *Jurnal TELEMATIKA MKOM, 9*(3).

Rivera, L. B., Bay, J. A., Arboleda, E. R., Pereña, M. R., & Dellosa, R. M. (2019). Hybrid Cryptosystem Using RSA, DSA, Elgamal, and AES. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 8*(10).

Saragih, R. (2021). Digital Singnature pada File Dokumen Menerapkan Fungsi Hash dengan Metode MD5. *TIN: Terapan Informatika Nusantara, 2*(6), 8.

Seputra, K. A., & Saskara, G. A. (2020). KRIPTOGRAFI SIMETRIS RC4 PADA TRANSAKSI ONLINE BOOKING ENGINE SYSTEM. *Jurnal Pendidikan Teknologi dan Kejuruan, 17*(2), 288-289.

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), 4*(1), 1 & 4.

Sulaiman, R., & Vebu, M. (2018). Peningkatan Keamanan Pesan Berbasis Android Menggunakan Algoritma Kriptografi RSA. *Jurnal SISFOKOM, 7*(2), 117.

Sulastri, S., & Putri, R. D. (2018). Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) (SHA-256) dan Message Digest Algorithm (MD5) Penjadwalan Karyawan. *Jurnal Teknik Elektro, 10*(2), 73.

Warnilah, A. I., & Nugraha, S. N. (2018). Komparasi Algoritma Kriptografi Elgamal Dan Caesar Cipher untuk Enkripsi dan Dekripsi Pesan. *IJCIT (Indonesian Journal on Computer and Information Technology), 3*(2), 244.

Yusfrizal. (2019). RANCANG BANGUN APLIKASI KRIPTOGRAFI PADA TEKS MENGGUNAKAN METODE REVERSE CHIPER DAN RSA BERBASIS ANDROID. *Jurnal Teknik Informatika Kaputama, 3*(2), 32.

Yusuf, N. F. (2019). PENGIRIMAN PESAN DENGAN ALGORITMA KRIPTOGRAFI ELGAMAL. *Axiomath: Jurnal Matematika dan Aplikasinya, 1*(2), 14-17.

Zulfikar, M. I., Abdillah, G., & Komarudin, A. (2019). Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA). *Seminar Nasional Aplikasi Teknologi Informasi (SNATi)*, (pp. B-12). Yogyakarta.