Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 65-72
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Kriptografi Untuk Keamanan Data Penjualan Barang Pada Toko Azis Menggunakan Algoritma RSA CRT

Rosa Romayanti Purba[1], Azlan[2], Jufri Halim[3]
[1,2,3] Sistem Informasi, STMIK Triguna Dharma
Email: [1]rosapurba71@gmail.com, [2]Azlansaja19@gmail.com, [3,*]halim.jufri1972@gmail.com
Email Penulis Korespondensi: rosapurba71@gmail.com

Article History:
Received Dec 31th, 2024
Revised Jan 18th, 2025
Accepted Jan 31th, 2025

Abstrak

Toko Azis adalah toko yang menyediakan barang-barang kebutuhan yang digunakan dalam kehidupan sehari-hari. Selama ini, Toko Azis memiliki data penjualan barang yang tersimpan di komputer, yang mana data penjualan barang ini sangat penting bagi pihak toko dan sangat rentan untuk disalahgunakan. Saat ini pihak manajeman toko belum mampu menemukan cara agar data tersebut bisa aman, dan tidak disalahgunakan. Dalam menyelesaikan masalah yang ada di Toko Azis salah satu cara yang tepat adalah mengamankan data penjualan barang tersebut dengan menggunakan algoritma RSA-CRT. Kriptografi dibuat untuk membantu pihak toko dan manajemen dalam mengamankan data penjualan barang agar tidak disalahgunakan. Algoritma RSA-CRT merupakan salah satu metode yang dapat digunakan dalam pengamanan data penjualan barang. Algoritma RSA-CRT merupakan salah satu algoritma yang keamanannya cukup kuat dalam mengamankan data. Hasil penelitian ini berupa aplikasi yang dapat mengamankan data penjualan barang yang berbentuk file (.*csv) yang nantinya berguna untuk meningkatkan keamanan data penjualan barang di Toko Azis
Kata Kunci: RSA, CRT, Kriptografi, Keamanan, Data Penjualan

Abstract

Azis Shop is a shop that provides necessities used in daily activities. So far, Azis Store has had goods sales data stored on the computer, which is very important for the shop and is very vulnerable to misuse. Currently, store management has not been able to find a way to ensure that this data is safe and not misused. In solving the problems at Toko Azis, one of the right ways is to secure the sales data for the goods using the RSA-CRT algorithm. Cryptography was created to help stores and management secure sales data so that it is not misused. The RSA-CRT algorithm is one method that can be used to secure goods sales data. The RSA-CRT algorithm is an algorithm whose security is quite strong in securing data. The results of this research are in the form of an application that can secure goods sales data in the form of .csv files which will later be useful for increasing the security of goods sales data at the Azis Store.
Keywords: *RSA, CRT, Cryptography, Security, Sales Data*

1. PENDAHULUAN

Keamanan data merupakan salah satu hal yang penting saat ini. Dikarenakan setiap keputusan atau kebijakan yang diambil harus berdasarkan data yang sesuai dengan fakta. Dunia semakin berkembang seiring dengan majunya teknologi informasi. Dan komunikasi sekarang menjadi tidak terbatas. Dengan banyaknya kemudahan untuk melakukan pengaksesan informasi tersebut, maka diperlukan pengamanan terhadap data-data yang ada.

Setiap toko pasti memiliki banyak data transaksi yang tersimpan di dalam *database*. Salah satunya adalah data penjualan. Begitu juga dengan Toko Azis yang sudah menerapkan teknologi komputer dalam menyimpan data penjualan. Namun komputer tersebut tidak hanya dikendalikan oleh satu orang saja, melainkan setiap karyawan bisa memakai komputer tersebut. Dengan begitu rentan terjadinya penyadapan, manipulasi, pemalsuan data, dan pencurian informasi selama masa kerja. Kasus manipulasi data penjualan ini pernah terjadi di Toko Azis. Pihak karyawan dengan sengaja mengubah jumlah total penjualan dalam perhari hanya untuk mendapatkan keuntungan pribadi. Tentu hal ini sangat merugikan pihak toko dan juga merugikan Manajer Departemen selaku pihak yang bertanggung jawab atas data penju alan tersebut. Untuk menjaga data tersebut dari manipulasi dan penyalahgunaan, maka dibutuhkan suatu sistem yang dapat melindungi data penjualan tersebut agar tidak bisa dimanipulasi oleh pihak yang tidak bertanggung jawab.

Menurut Ashari Arief dan Ragil Saputra, Kriptografi adalah suatu ilmu yang mempelajari teknik matematika yang berhubungan dengan keamanan informasi seperti kerahasiaan data, integritas data, otentikasi entitas, dan otentikasi asal data[1]. Kriptografi dapat didefinisikan sebagai seni maupun ilmu yang menghasilkan pesan yang rahasia. Sebuah pesan asli yang disebut sebagai *plaintext* disandikan menjadi pesan yang tersandi yang disebut sebagai *ciphertext* melalui proses enkripsi dan *ciphertext* dipulihkan menjadi *plaintext* kembali melalui proses dekripsi[2]. Hasil pengujian ini menyajikan

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 65-72
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

aplikasi yang bisa mengamankan data penjualan barang pada Toko Azis dengan cara menyandikan isi *file* dan mengubah tipe data dari *file* (.*csv) menjadi file (.*txt).

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Dalam penelitian ini, penulis melakukan metode pengumpulan data sebagai berikut :

a. Observasi
b. Dalam penelitian ini dilakukan dengan tinjauan langsung ke Toko Azis. Di Toko Azis tersebut dilakukan analisis masalah yang ada kemudian diberikan resume atau rangkuman masalah apa saja yang terjadi selama ini terkait keamanan data penjualan barang.
c. Wawancara
d. Setelah itu dilakukan wawancara kepada pihak-pihak yang terlibat dan menanyakan apa yang menjadi masalah selama ini. Yaitu tentang terjadinya manipulasi data penjualan barang pada Toko Azis yang dilakukan oleh salah satu karyawan demi kepentingan pribadi.
e. Studi Pustaka
f. Di dalam penelitian ini banyak menggunakan jurnal-jurnal ISSN dan diharapkan jurnal-jurnal tersebut dapat membantu peneliti atau penulis dalam menyelesaikan permasalahan yang ada di Toko Azis.

2.2 Kriptografi

Kriptografi merupakan seni dan ilmu penyandian pesan sehingga tidak dapat lagi dipahami. Metode ini menjaga kerahasiaan pesan. Keamanan data adalah masalah kriptografi. Hal ini mencakup pembuatan proses berbasis algoritma matematika yang menyediakan sejumlah fungsi keamanan informasi utama[3]. Enkripsi dan dekripsi adalah dua proses dalam kriptografi. *Plaintext* adalah nama yang diberikan untuk pesan terenkripsi. Disebut demikian karena siapapun dapat membaca dan memahami informasi ini. Perhitungan yang digunakan untuk mengacak dan mendekode *plaintext* meliputi penggunaan beberapa jenis kunci. *Cryptext* mengacu pada pesan eksplisit yang menyertakan *ciphertext*[4].

2.3 Keamanan Data

Data adalah deskripsi dari objek dan kejadian yang kita temui. Data bisnis adalah deskripsi objek (sumber daya) dan kejadian (transaksi) yang terjadi di dalam perusahaan[5]. Data dalam penelitian ini adalah segala bentuk fakta, data, dan segala bentuk informasi yang digali dari penelitian subjek[6]. Dari pengertian di atas dapat disimpulkan bahwa data adalah kumpulan fakta tentang suatu objek, peristiwa, atau kegiatan yang disimpan atau direkam. Dengan berkembangnya teknologi di bidang komunikasi dan perpesanan maka informasi tersebut harus aman dan rahasia.

2.4 Algoritma RSA-CRT

RSA merupakan algoritma kriptografi kunci publik atau sering disebut kunci asimetrik (kunci enkripsi dan kunci dekripsi berbeda)[7]. Dalam kriptografi menggunakan algoritma RSA terdapat tiga proses yaitu proses pembangkitan kunci publik dan kunci privat, proses enkripsi, dan proses dekripsi[8]. Kunci publik boleh diketahui oleh siapa saja dan digunakan untuk proses enkripsi. Sedangkan kunci pribadi hanya pihak - pihak tertentu saja yang boleh mengetahuinya dan digunakan untuk proses dekripsi[9]. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima[10].

RSA adalah algoritma asimetris yang dianggap memiliki keamanan cukup bagus dilihat dari sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Namun, walaupun tingkat keamanannya cukup tinggi, proses enkripsi dan dekripsinya membutuhkan waktu cukup lama bergantung pada besarnya kunci yang dipilih. Oleh karena itu, algoritma ini dimodifikasi menggunakan Chinese Remainder Theorem (CRT) untuk mempercepat proses dekripsi file. CRT adalah algoritma yang berfungsi untuk mengurangi perhitungan aritmatika modular dengan modulus besar sehingga proses dekripsi akan lebih cepat[11]. CRT (Chinese Remainder Theorem) adalah suatu teori matematis yang digunakan untuk mengkonversi eksponensial modular yang berukuran besar menjadi eksponensial modular yang relatif lebih kecil[12].
Berikut ini implementasi dari Algoritma RSA-CRT :

1. Proses pembangkit kunci

Proses pertama adalah pembentukan kunci publik dan kunci privat dengan langkah-langkahnya sebagai berikut:

a. Menentukan 2 bilangan prima secara sembarang untuk menentukan p dan q, dimana nilai $p \neq q$.
b. Hitung nilai modulus (n)

$$n = p.q \quad (1)$$

Hitung nilai $\emptyset(n)$

$$\emptyset(n) = (p - 1) \times (q - 1) \quad (2)$$

d. Memilih e sebagai kunci publik yang relatif prima dengan $\emptyset(n)$ (3)
e. Menentukan nilai d dengan rumus :

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 65-72
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

d= (1+(k x 2952))/5 k= 1, 2, 3… (4)

f. Menentukan nilai dP

dP=e -1 mod (p-1) = d mod (p-1) (5)

g. Menentukan nilai dQ

dQ=e -1 mod (q-1) =d mod (q-1) (6)

h. Menentukan nilai qInv

qInv=(k x q mod p)=1 k= 1, 2, 3… (7)

2. Proses Enkripsi

Proses Enkripsi adalah mengubah *plaintext* (M) menjadi *ciphertext* (C) menggunakan kunci publik. Proses enkripsinya sebagai berikut :

C= M^e (mod n) (8)

3. Proses Dekripsi

Proses Dekripsi adalah mengembalikan *ciphertext* (C) menjadi *plaintext* (M). Proses dekripsinya sebagai berikut:

a. Menentukan nilai m1

m1 = c dP mod p (9)

b. Menentukan nilai m2

m2 = c dQ mod q (10)

c. Menentukan nilai h

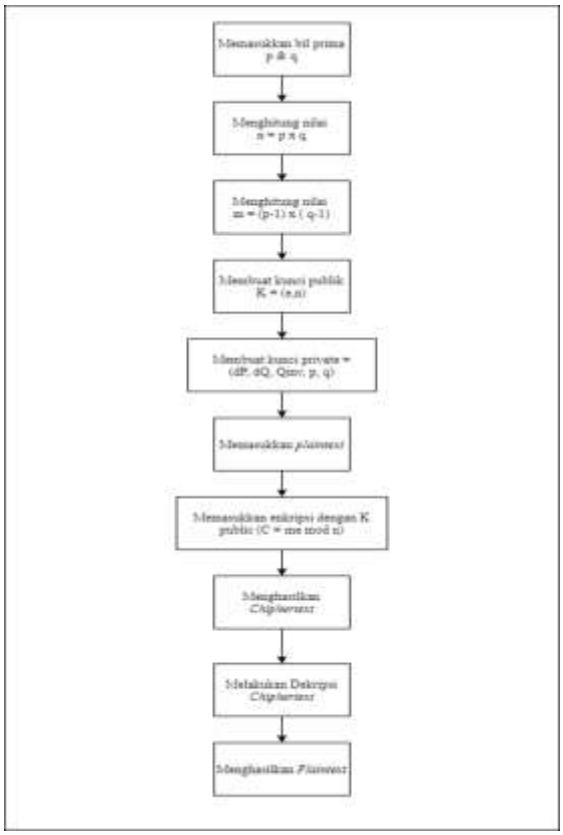
h = qInv (m1-m2) mod p (11)

d. Menghitung hasil dekripsi

M = m2 + h x q (12)

2.4 Kerangka Kerja Algoritma RSA-CRT

Metode yang digunakan untuk mengamankan data penjualan barang di Toko Azis adalah metode Rivest Shamir Adleman (RSA) – CRT. Berikut kerangka kerja dari metode RSA-CRT :



Gambar 1. Kerangka Kerja Algoritma RSA-CRT

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 65-72
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

3. HASIL DAN PEMBAHASAN

3.1 Penerapan Algoritma RSA-CRT

Dalam mengamankan data penjualan, yang akan diamankan adalah *file* berbentuk *Comma Separated Values* (*.CSV). Dan dalam perhitungan manual yang dicontohkan pada skripsi ini, pesan yang di enkripsi adalah "ROSA" yang dimana kode ASCII nya adalah "82 79 83 65". Implementasinya sebagai berikut :

1. Pembangkit kunci RSA-CRT
   a. Ambil bilangan prima untuk p dan q :
      □ = 37 dan □ = 83
   b. Hitung nilai modulus (n)
      □ = □ □ □
      □ = 37 □ 83
      □ = 3071
   c. Hitung nilai Ø □ = □−1 □ (□−1)
      Ø(□) = (□ − 1) □ (□ − 1)
      Ø(□) = (37 − 1) □ (83 − 1)
      Ø(□) = 36 □ 82
      Ø(□) = 2952
   d. Memilih kunci publik yang relatif prima dengan Ø □, maka □=5
   e. Menentukan nilai □ dengan rumus :
      □ = 1+(□ □ 2952)/5 dimana k = 1, 2, 3…
      □ = 1 = 1+(1 □ 2952)/5 □ = 590,6 tidak bulat
      □ = 2 = 1+(2 □ 2952) □ = 1181 bulat
      Dari perhitungan diatas diperoleh nilai □ yang bulat adalah 1181.
   f. Menentukan nilai dP
      □□ = □ □□□ (□ − 1)
      □□ = 1181 □□□ (37 − 1)
      □□ = 1181 □□□ 36
      □□ = 29
   g. Menentukan nilai dQ
      □□ = □□□ (□ − 1)
      □□ = 1181 □□□ (83 − 1)
      □□ = 1181 □□□ 82
      □□ = 33
   h. Menentukan qInv dengan rumus :
      □□□□ = (□ □ □ □□□ □) = 1, □ = 1, 2, 3…
      □ = 1 = (1 □ 83 □□□ 37) = 9, hasilnya belum 1
      □ = 2 = (2 □ 83 □□□ 37) = 18, hasilnya belum 1
      □ = 3 = (3 □ 83 □□□ 37) = 27, hasilnya belum 1
      □ = 33 = (33 □ 83 □□□ 37) = 1
      Maka, qInv berhasil didapatkan yaitu 33.
   i. Kunci *public* dan kunci *private* RSA-CRT
      K□□□□□□ = (□, □)
      K□□□□□□ = (5, 3071)
      K□□□□□□□ = (□□, □□, □□□□, □, □)
      K□□□□□□□ = (29, 33, 33, 37, 83)
2. Proses Enkripsi

Berdasarkan perhitungan diatas, maka dapat dilakukan proses enkripsi untuk menghasilkan *ciphertext* dengan rumus C = M^e mod n, yaitu :

- R (82) = 82^5 mod 3071
  = 1244
- O (79) = 79^5 mod 3071
  = 387
- S (83) = 83^5 mod 3071
  = 996
- A (65) = 65^5 mod 3071
  = 2334

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 65-72
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

3. Proses Dekripsi
   1. Memasukkan *ciphertext*
      Ciphertext yang akan di enkripsi adalah berupa hasil enkripsi yaitu "1244 387 996 2334".
   2. Menentukan nilai m1
      Untuk mencari nilai m1 digunakan rumus m1 = C^dp mod p, dengan perhitungannya adalah :

Tabel 1. Perhitungan mencari nilai □1

Ciphertext	Rumus m1 = C^dp mod p	m1
1244	1244^29 □□□ 37	8
387	387^29 □□□ 37	5
996	996^29 □□□ 37	9
2334	2334^29 □□□ 37	28

   3. Mencari nilai m2
      Untuk mencari nilai m2 digunakan rumus m2 = C^dq mod q, dengan perhitungannya adalah :

Tabel 2. Perhitungan mencari nilai □2

Ciphertext	Rumus m2 = C^dq mod q	m2
1244	1244^33 □□□ 83	82
387	387^33 □□□ 83	79
996	996^33 □□□ 83	0
2334	2334^33 □□□ 83	65

4. Menentukan nilai h
   Untuk mencari nilai h digunakan rumus h = qInv (m1 - m2) mod p, dengan perhitungannya adalah :

Tabel 3. Perhitungan mencari nilai h

Ciphertext	Rumus h = qInv (m1 - m2) mod p	h
1244	33 (8− 82) □□□ 37	0
387	33 (5 − 79) □□□ 37	0
996	33 (9 − 0) □□□ 37	1
2334	33 (28 − 65) □□□ 37	0

5. Menghitung Hasil Dekripsi
   Untuk mencari nilai dekripsi digunakan rumus M = m2 + h x q dengan perhitungannya adalah :

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 65-72
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

Tabel 4. Perhitungan mencari hasil dekripsi

Ciphertext	Rumus M = m2 + h x q	Dekripsi
1244	82 + 0 □ 83	82
387	79 + 0 □ 83	79
996	0 + 1 □ 83	83
2334	65 + 0 □ 83	65

Dari proses perhitungan di atas, maka didapatkan hasil dekripsi yaitu “82 79 83 65”. Dan apabila dalam bentuk ASCII karakter yaitu “ROSA”.

3.2 Implementasi Sistem

Berikut ini merupakan implementasi dari Kriptografi Untuk Keamanan Data Penjualan Barang Pada Toko Azis Menggunakan Algoritma RSA-CRT :

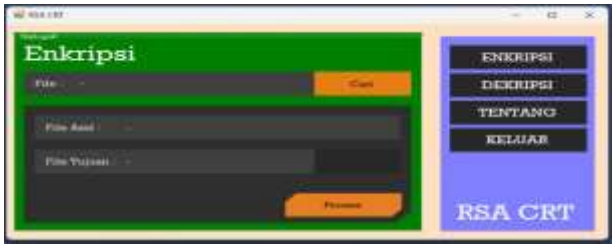
a. *Form Login*

Form Login merupakan *form* yang pertama ditampilkan untuk menghubungkan *user* ke halaman menu utama. Pada *form login* ini, *user* harus memasukkan *username* dan *password* dengan benar agar dapat membuka aplikasi dan menampilkan halaman menu utama.

Gambar 2. Tampilan *Form Login*

b. *Form* Enkripsi

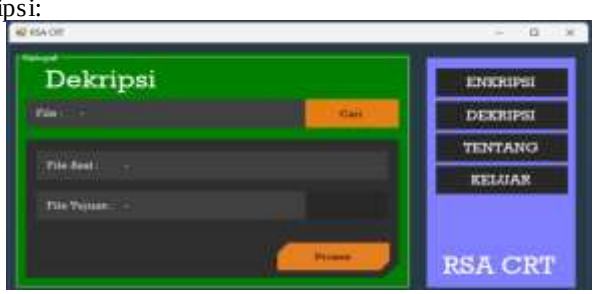
Form enkripsi digunakan *user* untuk mengenkripsi data penjualan barang yang berbentuk *file* (.* csv). Berikut tampilan dari *form* enkripsi.



Gambar 3. Tampilan *Form* Enkripsi

c. *Form* Dekripsi

Form Dekripsi digunakan *user* untuk mengdekripsi hasil enkripsi data penjualan barang yang berbentuk *file* (.*txt). Berikut tampilan dari *form* dekripsi:

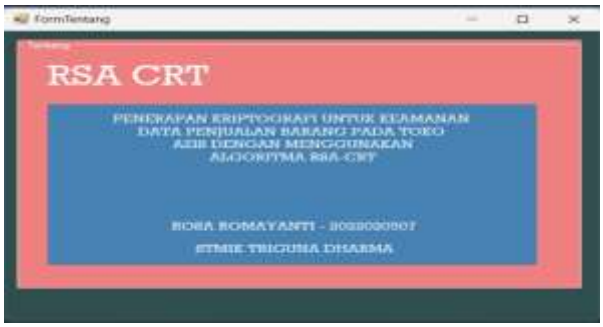


Gambar 4. Tampilan *Form* Dekripsi

Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD
Volume 8 ; Nomor 1 ; Januari 2025 ; Page 65-72
E-ISSN : 2615-5133 ; P-ISSN : 2621-8976
https://ojs.trigunadharma.ac.id/index.php/jsk/index

d. *Form* Tentang

Form tentang adalah *form* tambahan yang berisi nama aplikasi, nama pembuat aplikasi. NIRM, dan asal perguruan tinggi. Berikut tampilan *form* tentang.



Gambar 5. Tampilan *Form* Tentang

6. KESIMPULAN

Berdasarkan hasil tentang penerapan algoritma RSA-CRT untuk keamanan data penjualan barang pada Toko Azis telah dikemukakan, maka dapat diperoleh beberapa kesimpulan, yaitu penggunaan algoritma RSA-CRT telah berhasil digunakan di aplikasi dengan baik, sehingga data penjualan barang dapat terjaga, dan meningkatkan kemanan pada Toko Azis, lalu penerapan Kriptografi untuk Keamanan Data Penjualan Barang pada Toko Azis dengan menggunakan algoritma RSA-CRT dirancang melalui proses yang diawali dengan mencari masalah, lalu menemukan solusinya, kemudian merancang sebuah sistem yang dapat memecahkan masalah tersebut, serta aplikasi Kriptografi untuk Keamanan Data Penjualan pada Toko Azis menggunakan algoritma RSA-CRT yang telah dirancang tentu saja dapat diaplikasikan untuk menjaga data penjualan barang yang berbentuk *file Comma Separated Values* (*.CSV) dari pihak-pihak yang tidak bertanggung jawab dengan tujuan untuk mengambil keuntungan pribadi.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada Tuhan Yang Maha Esa yang telah memberikan rahmat dan karuniaNya sehingga penulis mampu menyelesaikan jurnal ini tepat pada waktunya. Kepada kedua orangtua atas doa dan motivasi nya serta kepada Bapak Azlan dan Bapak Jufri Halim untuk arahan dan bimbingannya selama proses pengerjaan skripsi ini. Terima kasih juga kepada seluruh pihak manajemen kampus STMIK Triguna Dharma, para bapak dan ibu dosen yang telah memberikan ilmu dan pengajaran selama masa perkuliahan, para pegawai yang ada di kampus STMIK Triguna Dharma yang telah membantu memberikan informasi ataupun dukungan lainnya, serta seluruh teman-teman yang telah memberikan dukungan dan motivasi.

DAFTAR PUSTAKA

[1] R. Herteno, W. Ramadansyah, O. Soesanto, R. A. Nugroho, and A. Rusadi, "Steganografi Untuk Pesan Terenkripsi Menggunakan Algoritma Kriptografi Rsa-Crt Di Android," *Klik - Kumpul. J. Ilmu Komput.*, vol. 6, no. 1, pp. 16–26, 2019.
[2] Y. Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," J. Inform. Kaputama, vol. 3, no. 2, pp. 29–37, 2019.
[3] Y. J. El Anwar, R. Habibi, and N. Riza, "Penerapan Metode Kriptografi Aes Untuk Mengamankan File Dokumen," J. Tekno Insentif, vol. 16, no. 2, pp. 92–104, 2022, doi: 10.36787/jti.v16i2.852.
[4] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," J. Pendidik. Sains dan Komput., vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.
[5] A. Ignasius and D. V. Shaka Yudha Sakti, "Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi," Skanika, vol. 5, no. 1, pp. 1–10, 2022, doi: 10.36080/skanika.v5i1.2118.
[6] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," J. Comput. Syst. Informatics, vol. 1, no. 2, pp. 54–60, 2020.
[7] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," J. Media Inform. Budidarma, vol. 4, no. 2, p. 413, 2020, doi: 10.30865/mib.v4i2.2037.
[8] A. Syahputra, I. Algoritma, and F. Untuk, "Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci Algoritma RSA Pada Pengamanan Data Video," vol. 10, pp. 70–77, 2021.
[9] C. N. Prabiantissa, G. E. Yuliastuti, S. Agustini, and D. H. Sulaks ono, "Proteksi Data X-Ray Paru-Paru Pasien COVID-19 menggunakan Algoritma Rivest Shamir Adleman dan Algoritma Enkripsi Rubic Cube Principle,"Pros. Semin. Nas. Sains dan Teknol. Terap. VIII, pp. 93–100, 2020, [Online]. Available: https://ejurnal.itats.ac.id/sntekpan/article/view/1221.
[10] S. Rahmadhiyanti, "Implementasi Kriptografi Rsa Untuk Peningkatan Keamanan Database E-Commerce," Pelita Inform., vol. 8, p. 4, 2019.

[11] N. C. H. Wibowo, K. Umam, A. M. I. Khaq, and F. A. Rizki, "Komparasi Waktu Algoritma RSA dengan RSACRT Base On Computer," Walisongo Journal of Information Technology,vol.2, no. 1, p. 13, 2020, doi: 10.21580/wjit.2020.2.1.5402.
[12] Z. Panjaitan, K. Ibnutama, and M. G. Suryanata, "Penggunaan Chinese Reminder Theorem (CRT) pada Algoritma RSA," J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer), vol. 18, no. 1, p. 41, 2019, doi: 10.53513/jis.v18i1.102.