

Pengamanan Data Pegawai Dengan Menerapkan Algoritma Kriptografi RSA Pada PT. Metro Cash & Credit Medan

Employee Data Security By Implementing RSA Cryptography Algorithm at PT. Metro Cash & Credit Medan

Ferdi Rahmansyah¹, Muhatri²

^aProgram Studi Informatika Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

^bProgram Studi Informatika Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

E-mail: ferdirahmansyah1@gmail.com¹, muhatri@potensi-utama.ac.id²

ABSTRAK

PT. Metro Cash & Credit Medan adalah perusahaan yang bergerak di bidang penjualan perlengkapan rumah tangga. Sistem penyimpanan data karyawan pada PT. Metro Cash & Credit Medan masih menggunakan sistem terkomputerisasi berupa penyimpanan berkas tanpa pengamanan sehingga dapat mengakibatkan kehilangan data. Perusahaan ini masih menyimpan data dalam file berbentuk berkas tanpa adanya pengamanan data. Perusahaan ini juga tidak memiliki media penyimpanan file dokumen, sehingga apabila para pegawai membutuhkan suatu file, mereka harus meminta kepada pegawai yang membutuhkan. Kemungkinan terjadinya pencurian dan penyalahgunaan data masih cukup tinggi, karena masih banyak faktor yang bisa dijadikan celah dalam hal keamanan data. Oleh karena itu, untuk menjamin keamanan data baik saat penyimpanan maupun pengiriman informasi, maka diperlukan aplikasi keamanan data untuk mengenkripsi agar data tersebut tidak bisa dengan mudah diakses orang lain yang tidak mempunyai otoritas. Permasalahan tersebut bisa diatasi dengan membangun aplikasi pengamanan data menggunakan algoritma kriptografi.

Kata Kunci : Keamanan, RSA, Pegawai, Android

ABSTRACT

PT. Metro Cash & Credit Medan is a company that operates in the field of selling household equipment. Employee data storage system at PT. Metro Cash & Credit Medan still uses a computerized system in the form of file storage without security which can result in data loss. This company still stores data in files without any data security. This company also does not have a storage medium for document files, so if employees need a file, they have to ask the employee who needs it. The possibility of data theft and misuse is still quite high, because there are still many factors that can create gaps in data security. Therefore, to ensure data security both when storing and sending information, a data security application is needed to encrypt it so that the data cannot be easily accessed by other people who do not have authority. This problem can be overcome by building a data security application using cryptographic algorithms.

Keywords : Security, RSA, Employees, Android

Info Artikel :

Disubmit: 15 Agustus 2024

Direview: 16 September 2024

Diterima : 30 Oktober 2024

Copyright © 2024 – senadimu. All rights reserved.

1. PENDAHULUAN

Kemajuan ilmu pengetahuan dan teknologi saat ini mendorong setiap orang/individu, instansi atau perusahaan baik pemerintah maupun swasta untuk senantiasa menemukan dan menggunakan teknologi sebagai alat bantu dalam menjalankan tugas – tugas dari setiap individu yang ada di dalamnya, serta membantu dalam pemecahan masalah – masalah yang dihadapi. Ancaman terhadap keamanan pesan bisa kapan saja terjadi sehingga bisa disalahgunakan oleh pihak yang tidak berwenang. Data rahasia yang akan dikirim memerlukan keamanan agar tidak dapat disalahgunakan

oleh pihak-pihak yang lain. Data yang akan disampaikan memerlukan keamanan agar hanya dapat digunakan oleh penerima yang sah [1]

PT. Metro Cash & Credit Medan adalah perusahaan yang bergerak di bidang penjualan perlengkapan rumah tangga. Sistem penyimpanan data karyawan pada PT. Metro Cash & Credit Medan masih menggunakan sistem terkomputerisasi berupa penyimpanan berkas tanpa pengamanan sehingga dapat mengakibatkan kehilangan data. Perusahaan ini masih menyimpan data dalam file berbentuk berkas tanpa adanya pengamanan data. Perusahaan ini juga tidak memiliki media penyimpanan file dokumen, sehingga apabila para pegawai membutuhkan suatu file, mereka harus meminta kepada pegawai yang membutuhkan.

Kemungkinan terjadinya pencurian dan penyalahgunaan data masih cukup tinggi, karena masih banyak faktor yang bisa dijadikan celah dalam hal keamanan data. Oleh karena itu, untuk menjamin keamanan data baik saat penyimpanan maupun pengiriman informasi, maka diperlukan aplikasi keamanan data untuk mengenkripsi agar data tersebut tidak bisa dengan mudah diakses orang lain yang tidak mempunyai otoritas. Permasalahan tersebut bisa diatasi dengan membangun aplikasi pengamanan data menggunakan algoritma kriptografi.

Keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Masalah keamanan sering berada di urutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting [2]

Kriptografi adalah ilmu yang mempelajari tentang bagaimana menjaga kerahasiaan suatu pesan, agar isi pesan yang ditampilkan tersebut aman sampai ke penerima pesan. Kriptografi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi naskah acak yang sulit dibaca (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi. Dalam kriptografi terdapat banyak algoritma, salah satunya adalah algoritma RSA. RSA (Rivest Shamir Adleman) merupakan algoritma tandatangan digital yang terkenal dan banyak digunakan. Algoritma ini menjadi unggul karena mudah untuk diimplementasikan dan sangat kuat. Pada RSA, algoritma enkripsi dan dekripsi identik, sehingga proses pemberian tanda tangan digital dan verifikasi juga identik [3]

Dalam kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Pesan terenkripsi disebut *plaintext*. Disebut demikian karena informasi ini dapat dengan mudah dibaca dan dipahami oleh siapa saja. Algoritma yang digunakan untuk mengenkripsi dan mendekripsi *plaintext* melibatkan penggunaan beberapa bentuk kunci [4].

2. METODE

Dalam pengumpulan data-data yang diperlukan dalam penyusunan penelitian ini, maka peneliti menggunakan beberapa tahapan yaitu :

a. Wawancara

Pada bagian ini dilakukan proses wawancara langsung dengan manajemen PT. Metro Cash & Credit Medan untuk mendapatkan informasi – informasi seperti: sistem yang sedang berjalan, dan kelemahan dari sistem yang ada sehingga perlu dibuatkan sistem yang baru pada PT. Metro Cash & Credit Medan. Proses wawancara dilakukan kepada HRD pada PT. Metro Cash & Credit Medan yaitu bapak Jerfy Ariandy. Adapun pertanyaan yang diajukan adalah :

- 1) Bagaimana sistem keamanan data pegawai pada PT. Metro Cash & Credit Medan?
Jawab : sistem keamanan data pegawai pada PT. Metro Cash & Credit Medan masih di simpan dengan menggunakan buku dan arsipan.
- 2) Apa saja kendala yang terjadi dalam keamanan data pegawai pada PT. Metro Cash & Credit Medan?

Jawab : kendala yang terjadi dalam keamanan data pegawai pada PT. Metro Cash & Credit Medan sering terjadi kehilangan data dan tidak dapat di jaga keamanannya.

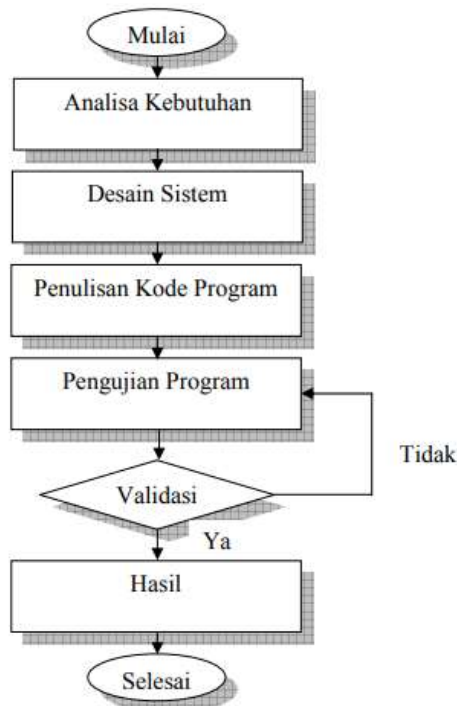
3) Apakah data pegawai dapat di jaga kerahasiannya dengan baik pada PT. Metro Cash & Credit Medan?

Jawab : untuk saat ini data kerahasiaan data pegawai masih sering tidak terjaga dengan baik.

b. Penelitian perpustakaan

Peneliti melakukan penelitian perpustakaan untuk mengumpulkan teori berupa buku dan jurnal untuk referensi pada penelitian ini.

Berikut adalah alir diagram metode penelitian yang digunakan dalam penulisan proposal ini :



Gambar 1. Diagram Alir Metodologi Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahapan ini peneliti mengumpulkan data-data yang berkaitan dengan penelitian. Peneliti juga menentukan software dan hardware yang akan digunakan untuk membuat penelitian. Berikut adalah software yang digunakan untuk pembuatan sistem :

- a. Sistem operasi windows 8
- b. Java
- c. Android Studio

Berikut adalah hardware yang digunakan untuk penerapan sistem :

- a. Laptop/ Computer
- b. Hardisk
- c. Mouse

Berikut adalah bahan bacaan yang digunakan untuk teori :

- a. Buku
- b. Jurnal

2. Desain Sistem

Untuk mendesain sistem peneliti menggunakan beberapa pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Dalam penulisan kode program, peneliti menggunakan bahasa pemrograman Java dengan

database Firebase.

4. Pengujian Program

Pengujian program dilakukan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik. Pengujian dengan teori menggunakan blackbox testing dan pengujian dengan praktek menggunakan Java

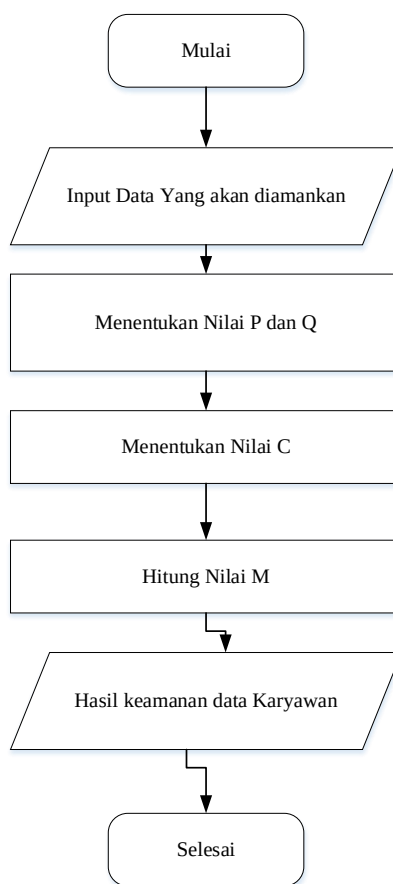
5. Hasil

Pada tahapan ini aplikasi keamanan data pegawai menggunakan metode RSA sudah dapat berjalan dengan baik dan penelitian ini menghasilkan pemahaman mengenai metode RSA.

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

Berikut ini merupakan flowchart dari metode RSA sebagai berikut :



Gambar 2. Flowchart Metode RSA

Studi Kasus

Akan dilakukan enkripsi menggunakan algoritma RSA terhadap plaintext $M = \text{KEUANGAN}$. Pertama-tama plaintext tersebut diubah menjadi format ASCII sebagai berikut :

Tabel 1. Tabel ASCII Karakter "KEUANGAN":

Huruf	ASCII
K	75
E	69

Huruf	ASCII
U	85
A	65
N	78
G	71
A	65
N	78

Data yang Sudah Ditetapkan:

$p=61$, $q=53$

$n=p \times q=61 \times 53=3233$

$\phi(n)=(p-1) \times (q-1)=3120$

Eksponen publik $e=17$

Eksponen privat $d=2753$

Enkripsi dengan Kunci Publik

Enkripsi dilakukan dengan menggunakan rumus:

$$C = M^e \bmod n$$

di mana:

- M adalah nilai ASCII dari huruf
- $e=17$ adalah eksponen publik
- $n=3233$

1. Huruf "K" (ASCII = 75):

$$C = 75^{17} \bmod 3233$$

Langkah perhitungan:

$$75^{17} = 169518829100544703125$$

$$C = 169518829100544703125 \bmod 3233 = 2201$$

Jadi, ciphertext untuk "K" adalah 2201.

2. Huruf "E" (ASCII = 69):

$$C = 69^{17} \bmod 3233$$

Langkah perhitungan:

$$69^{17} = 1041273502979112415329$$

$$C = 1041273502979112415329 \bmod 3233 = 1313$$

Ciphertext untuk "E" adalah 1313.

3. Huruf "U" (ASCII = 85):

$$C = 85^{17} \bmod 3233$$

Langkah perhitungan:

$$85^{17} = 418211942557747392265625$$

$$C = 418211942557747392265625 \bmod 3233 = 2535$$

Ciphertext untuk "U" adalah 2535.

4. Huruf "A" (ASCII = 65):

$$C = 65^{17} \bmod 3233$$

Langkah perhitungan:

$$65^{17} = 8650415919381337933$$

$$C = 8650415919381337933 \bmod 3233 = 2790$$

Ciphertext untuk "A" adalah 2790.

5. Huruf "N" (ASCII = 78):

$$C=78^{17} \bmod 3233$$

Langkah perhitungan:

$$78^{17}=82724026188633676417793$$

$$C=82724026188633676417793 \bmod 3233 =2591$$

Ciphertext untuk "N" adalah 2591.

6. Huruf "G" (ASCII = 71):

$$C=71^{17} \bmod 3233$$

Langkah perhitungan:

$$71^{17}=16448102661888121144271$$

$$C=16448102661888121144271 \bmod 3233 =1730$$

Ciphertext untuk "G" adalah 1730.

7. Huruf "A" (ASCII = 65):

Karena "A" sudah dienkripsi sebelumnya, ciphertext-nya adalah:

$$C=2790$$

8. Huruf "N" (ASCII = 78):

Ciphertext untuk "N" sudah dihitung:

$$C=2591$$

Hasil Enkripsi:

Setelah dienkripsi, teks "KEUANGAN" berubah menjadi deretan ciphertext:

- **2201 1313 2535 2790 2591 1730 2790 2591**

Dekripsi dengan Kunci Privat

Dekripsi dilakukan dengan menggunakan rumus:

$$M=C^d \bmod n$$

di mana:

- C adalah nilai ciphertext
- d=2753 adalah eksponen privat
- n=3233

Dekripsi setiap ciphertext untuk mendapatkan kembali teks asli.

1. Ciphertext 2201 (untuk "K"):

$$M=2201^{2753} \bmod 3233$$

Dengan menggunakan metode eksponensiasi modular:

$$M=75$$

Ini mengembalikan huruf "K".

2. Ciphertext 1313 (untuk "E"):

$$M=1313^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=69$$

Ini mengembalikan huruf "E".

3. Ciphertext 2535 (untuk "U"):

$$M=2535^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=85$$

Ini mengembalikan huruf "U".

4. Ciphertext 2790 (untuk "A"):

$$M=2790^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=65$$

Ini mengembalikan huruf "A".

5. Ciphertext 2591 (untuk "N"):

$$M=2591^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=78$$

Ini mengembalikan huruf "N".

6. Ciphertext 1730 (untuk "G"):

$$M=1730^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=71$$

Ini mengembalikan huruf "G".

7. Ciphertext 2790 (untuk "A"):

$$M=2790^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=65$$

Ini mengembalikan huruf "A".

8. Ciphertext 2591 (untuk "N"):

$$M=2591^{2753} \bmod 3233$$

Hasilnya adalah:

$$M=78$$

Ini mengembalikan huruf "N".

Hasil Dekripsi:

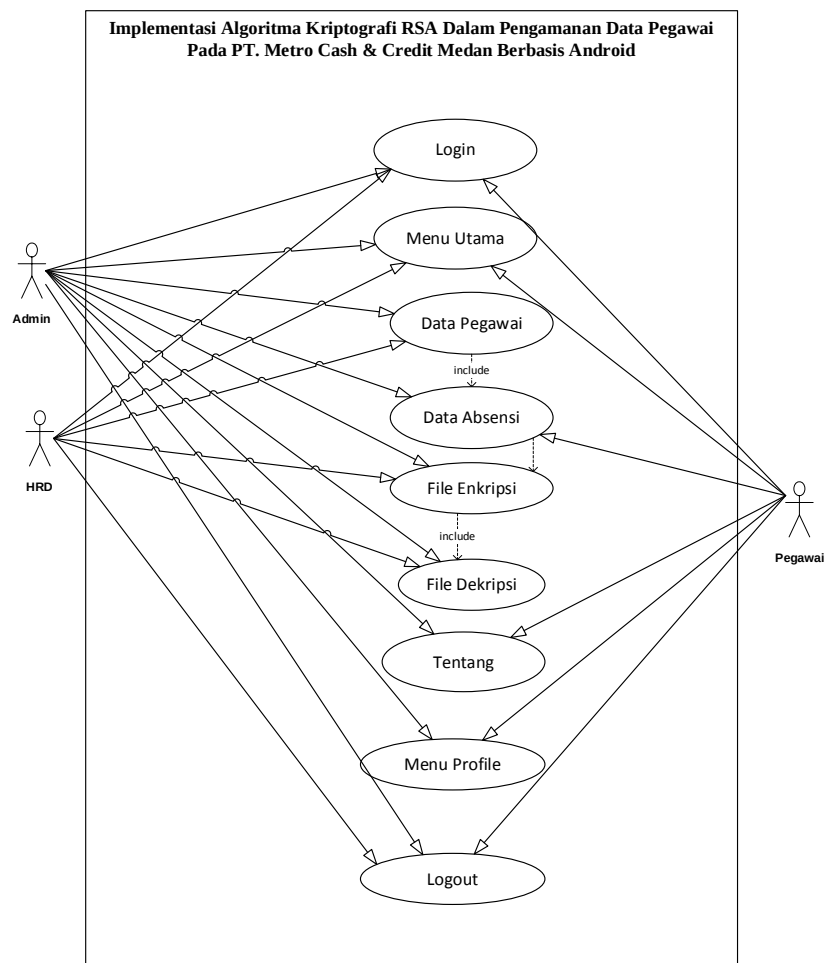
Setelah dekripsi, maka mendapatkan kembali teks asli:

- **KEUANGAN**

Kesimpulan:

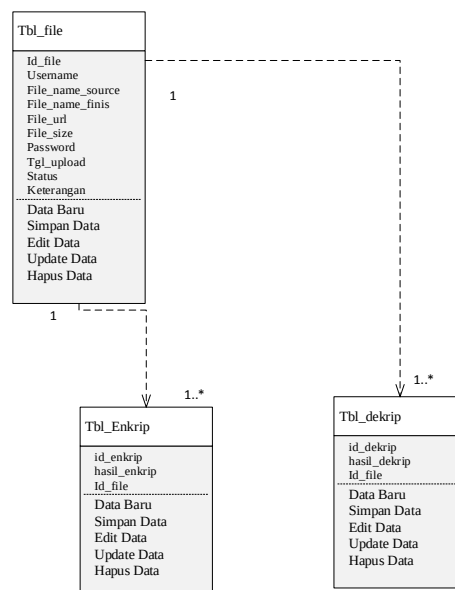
- **Enkripsi** mengubah teks "KEUANGAN" menjadi deretan ciphertext 2201 1313 2535 2790 2591 1730 2790 2591 menggunakan kunci publik.
- **Dekripsi** menggunakan kunci privat mengembalikan ciphertext tersebut menjadi teks asli "KEUANGAN".

Sebuah *use case* digambarkan sebagai elips horizontal dalam suatu diagram UML *use case*, dapat dilihat pada gambar 2:



Gambar 2. Use Case Diagram

Rancangan kelas-kelas yang akan digunakan pada sistem yang akan dirancang dapat dilihat pada gambar 3 :



Gambar 3. *Class Diagram*

3.2. Hasil

1. Tampilan Menu Login

Tampilan login merupakan tampilan yang pertama kali muncul ketika program dijalankan. Berfungsi sebagai *form* beranda admin program. Gambar tampilan beranda dapat ditunjukkan pada gambar 4 :



Gambar 4. Tampilan *Form* Login

2. Tampilan Menu beranda

Tampilan beranda merupakan tampilan yang pertama kali muncul ketika program dijalankan. Berfungsi sebagai *form* beranda admin program. Gambar tampilan beranda dapat ditunjukkan pada gambar 5 :



Gambar 5. Tampilan *Form* Beranda

3. Tampilan *Form* data Pegawai

Form utama merupakan *interface* program menu pegawai, dimana untuk menggunakan aplikasi kriptografi ini dapat melalui *interface form* menu pegawai. Dalam *form* menu pegawai terdapat

beberapa menu yaitu, menu *file* dan menu program. Untuk lebih jelasnya tampilan *form* menu pegawai dapat dilihat pada Gambar 6 dibawah ini.

Gambar 6. Tampilan *Form* Menu Pegawai

4. Tampilan *Form* Data daftar data pegawai

Form daftar data pegawai ini berfungsi untuk merubah isi data *file* dalam bentuk *chiphertext*, menyimpan hasil enkripsi (*chiphertext*), dan keluar dari *form* data enkripsi. Berikut ini tampilan *form* data daftar data pegawai dapat dilihat pada gambar 7 berikut ini:

Gambar 7. Tampilan *Form* Data Daftar Data Pegawai

5. Tampilan *Form* Tentang

Form tentang berfungsi untuk melihat tentang aplikasi, dapat dilihat sebagai berikut ini:



Gambar 8. Tampilan *Form* Tentang

5. Tampilan *Form* Akun

Form tentang berfungsi untuk melihat tentang akun pengguna, dapat dilihat sebagai berikut ini:



Gambar 9. Tampilan *Form Akun*

4. KESIMPULAN

Berdasarkan hasil pembahasan dan uji coba yang telah dilakukan yaitu Implementasi Algoritma Kriptografi RSA Dalam Pengamanan Data Pegawai Pada PT. Metro Cash & Credit Medan Berbasis Android, dapat disimpulkan :

1. Aplikasi Telah dibangun dan dapat menjaga keamanan data pegawai Pada PT. Metro Cash & Credit Medan dengan system penyandian Metode RSA.
2. Sistem yang dibangun sudah mampu melakukan enkripsi dan dekripsi terhadap Karyawan Pada PT. Metro Cash & Credit Medan sehingga dapat Melindungi data karyawan.
3. Sistem yang dibangun mempunyai tampilan yang sangat sederhana dan mudah digunakan oleh user .

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah banyak memberikan masukan dan saran dalam penyelesaian penelitian ini.

REFERENSI

- [1] Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) untuk Mengamankan Data Keuangan. *JIKOMSI [Jurnal Ilmu Komputer Dan Sistem Informasi]*, 4(2), 75–85. <https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A>
- [2] Fitriyani A, Handayani R, & Widanengsih E. (2020). Sistem Pendukung Keputusan Pemilihan Jurusan Pada SMK YMIK Joglo Jakarta Barat Menggunakan Metode Simple Additive Weigting (SAW). *Jtksi*, 03(01), 11–19.
- [3] Janis, J. W., Mamahit, D. J., Sugiarto, B. A., Rumagit, A. M., Elektro, T., Sam, U., & Manado, R. (2020). Rancang Bangun Aplikasi Online Sistem Pemesanan Jasa Tukang Bangunan Berbasis Lokasi. *Jurnal Teknik Informatika*, 15(1), 1–12. <https://doi.org/10.35793/jti.15.1.2020.29023>
- [4] Kaban, R., Yunita, W., & Faradillah, Y. (2019). Aplikasi Pemesanan Tiket Bus Berbasis Android (Study Kasus : Pt. Als Terminal Pasar X Tanjung Beringin). *Jurnal Manajemen ...*, 32(1).
- [5] Lubis, R. S., Tulus, & Nababan, E. B. (2022). Pengamanan File Teks Menggunakan Algoritma RSA – LUC dan Algoritma Zig- Zag dalam Hybrid Crypto Sistem. *InfoTekJar : Jurnal Nasional Informatika Dan Teknologi Jaringan*, 6(2), 185–189.
- [6] Marpaung, R., & Informasi, T. (2022). *PENYIMPANAN DATA PRIBADI DENGAN METODE*. 2(11), 1–14.
- [7] Muharromin, M., Informatika, J. T., & Dharma, U. B. (n.d.). *Analisis Performance Web Application Firewall ModSecurity dan Shadow Daemon Dalam Keamanan Web Server Apache*. 393–402.
- [8] Perbawa, K. A. (2022). Application of Linear Congruential Generator (LCG) Algorithm in Android Based Mathematics Education Game Penerapan Algoritma Linear Congruential Generator (LCG) dalam Game Edukasi Matematika Berbasis Android. *Jurnal Komputer, Informasi Dan Teknologi*, 2(1), 47–56.
- [9] Ruing, M. O. I., & Ujianto, E. I. H. (2020). *Penerapan Kombinasi Algoritma Kriptografi (Caesar, Vigenere, Zig-Zag) Dan Metode Steganografi Lsb Untuk Mengamankan Pesan Ke Dalam Citra Digital*. 1–8. <http://eprints.uty.ac.id/4888/>
- [10] Setiaji, A. (2020). RANCANG BANGUN APLIKASI PEMESANAN DESAIN JERSEY BERBASIS ANDROID DENGAN MENGGUNAKAN TEKNOLOGI FIREBASE (Studi Kasus :Konfeksi Minister). *Jurnal Sistem Informasi Dan Sains Teknologi*, 2(2). <https://doi.org/10.31326/sistek.v2i2.664>

-
- [11] Sitepu, D. A., Nurhayati, & Khair, H. (2022). Implementasi Pengamanan Data Koperasi Menggunakan Algoritma Advanced Encryption Standard (AES). *CITISEE 2016 Proceedings*, 6(1), 37–40. [https://citisee.amikompurwokerto.ac.id/assets/proceedings/paper/8__Amikom_Purwokerto_Implementasi_Pengamanan_Data_Koperasi_Menggunakan_Algoritma_Advanced_Encryption_Standard_\(Aes\).pdf](https://citisee.amikompurwokerto.ac.id/assets/proceedings/paper/8__Amikom_Purwokerto_Implementasi_Pengamanan_Data_Koperasi_Menggunakan_Algoritma_Advanced_Encryption_Standard_(Aes).pdf)
 - [12] Suharya, Y. (2020). Implementasi Digital Signature Menggunakan Algoritma Kriptografi RSA Untuk Pengamanan Data Di Smk Wirakarya 1 Ciparay. *COMPUTING| Jurnal Informatika*, 7(1), 21-29.
 - [13] Rosita, A. (2021). IMPLEMENTASI VERIFIKASI TEKS MENGGUNAKAN METODE RIVEST SHAMIR ADLEMAN (RSA). *Jurnal Ilmiah Teknologi Infomasi Terapan*, 8(1), 72-77.
 - [14] Implementasi Algoritma Kriptografi Rivest Shamir Adlemen untuk Mengamankan Data Ijazah pada SMK Swasta Prama Artha Kab. Simalungun
 - [15] Rizki, M., & Ariyani, P. F. (2021). Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal. *SKANIKA: Sistem Komputer dan Teknik Informatika*, 4(2), 77-82.
 - [16] Sutejo, S. (2021). Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien. *INTECOMS: Journal of Information Technology and Computer Science*, 4(1), 104-114