JURNAL OTOMASI
Volume 5, Nomor 1, Mei 2025, Page 15-21
E-ISSN 2807-3436
Available Online at http://ojs.polmed.ac.id/index.php/JOM

PERANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA CAESAR CIPHER DIKOMBINASIKAN DENGAN METODE MERKLE HELLMAN KNAPSACK

Indah Astary [1], Suriati [2], Putri Harliana [3,*]
[1,2] Program Studi Teknik Informatika, Fakultas Teknik Komputer, Universitas Harapan Medan, Medan, Indonesia
[3] Program Studi Teknik Informatika, Fakultas Teknik Komputer, Universitas Negeri Medan, Medan, Indonesia
Email: [1] indahastary8@gmail.com

Abstract

The security of text data is something that needs to be considered in maintaining the confidentiality of the data itself, especially if the text data is only known to certain parties. There are many approaches taken to realize the confidentiality of the data, starting from physical security or protection to the form *of a math-based algorithm that makes the data unreadable. Data security using encryption and decryption is known as cryptography, as a science or art to secure messages or data by disguising the message so that it can only be read by the sender and recipient of the message. Data security on network traffic is something that everyone wants to maintain privacy, so that data is sent safely from interference by irresponsible people, which is hidden using cryptographic algorithms. Application testing in encryption and decryption produces ciphertext in the* form *of a series of numbers and produces the same* input *plaintext as the* output *plaintext of the decryption process. This encryption is more secure than cryptographic methods that produce encryption in text* form*. The usual way to strengthen security is to use cryptography so that people will not suspect if the message has been encrypted and people will still think that the file does not contain a secret message. One of the techniques used in cryptography is the Caesar cipher algorithm combined with the Knapsack Merkle Hellman method.*

Keywords: *Algorithm, Data, Cryptography, Encryption, Decryption*

Abstrak

Keamanan suatu data teks merupakan hal yang perlu diperhatikan dalam menjaga kerahasiaan data itu sendiri, terutama bila data teks tersebut hanya boleh diketahui pihak yang tertentu saja. Terdapat banyak cara pendekatan yang dilakukan untuk mewujudka kerahasiaan data tersebut dimulai dari pengamanan atau perlindungan secara fisik hingga kedalam bentuk algoritma berbasis matematika yang membuat data menjadi tidak terbaca. Pengamanan data menggunakan enkripsi dan dekripsi dikenal dengan nama kriptografi, sebagai sebuah ilmu atau seni untuk mengamankan pesan atau data dengan cara menyamarkan pesan tersebut sehingga hanya dapat dibaca oleh pengirimdan penerima pesan. Keamanan data pada lalu lintas jaringan adalah suatu hal yang diinginkan semua orang untuk menjaga privasi , supaya data dikirim aman dari gangguan orang yang tidak bertanggung jawab, yang disembunyikan menggunakan algoritma kriptografi. Pengujian aplikasi dalam enkripsi dan dekripsi menghasilkan chipertext berupa deretan angka dan menghasilkan plaintext input yang sama dengan plaintext output dari proses dekripsi. Enkripsi ini lebih aman dibandingkan metode kriptografi yang menghasilkan enkripsi dalam bentuk teks. Cara yang biasa digunakan untuk memperkuat keamanan yaitu dengan menggunakan kriptografi sehingga orang tidak akan curiga jika pesan tersebut sudah di enkripsi dan orang akan tetap mengira jika file itu tidak mengandung pesan rahasia. Salah satu teknik yang digunakan pada kriptografi merupakan algoritma Caesar cipher dikombinasikan dengan metode Knapsack Merkle Hellman.

Kata Kunci: Algoritma, Data, Kriptografi, Enkripsi, Dekripsi

1. PENDAHULUAN

Dalam dunia digital saat ini, data memiliki peran sangat penting dan dapat dimanfaatkan untuk hal baik maupun buruk, seperti penyalahgunaan pembayaran online menggunakan data orang lain. Penelitian oleh Dedi Leman (2020) mengimplementasikan algoritma Merkle Hellman

Knapsack, yang menggunakan logika XOR dan tergolong asimetris, untuk pengamanan data. Metode ini dinilai aman karena memerlukan nilai pengirim dan penerima, serta diimplementasikan dalam aplikasi berbasis Visual Basic. Namun, kekurangannya adalah aplikasi ini hanya beroperasi secara *offline*. Di sisi lain, kelebihannya terletak pada hasil perhitungan yang memuaskan sesuai kebutuhan sistem.

Penelitian Murdani (2017) juga menekankan pentingnya keamanan data teks, terutama yang bersifat rahasia, dengan menggunakan algoritma Merkle Hellman Knapsack dalam Visual Basic 6.0. Aplikasi ini memudahkan pengguna dalam menghasilkan kunci, enkripsi, dan dekripsi, dengan output *ciphertext* berupa deretan angka—lebih aman dibanding metode yang menghasilkan teks terenkripsi. Keunggulannya adalah keamanan ganda yang sulit ditembus, meski terbatas pada penggunaan offline.

Untuk memperkuat keamanan, kriptografi menjadi solusi utama, salah satunya dengan algoritma Caesar Cipher yang menggunakan substitusi huruf berdasarkan pergeseran kunci. Penelitian Gurning (2014) mengimplementasikan metode ini dalam Visual Basic untuk mengamankan pesan melalui enkripsi dan dekripsi. Kombinasi teknik ini memastikan kerahasiaan pesan selama pengiriman.

Berdasarkan pembahasan tersebut, muncul gagasan untuk merancang aplikasi pengamanan data dengan menggabungkan dua algoritma berbeda, yaitu Caesar Cipher dan Merkle Hellman Knapsack. Tujuannya adalah meningkatkan keamanan pertukaran data dengan memanfaatkan kelebihan masing-masing metode, sekaligus mengatasi keterbatasan akses *offline* pada penelitian sebelumnya. Harapannya, aplikasi ini dapat memberikan perlindungan lebih kuat terhadap penyalahgunaan data di era digital.

2. METODE PENELITIAN

Penelitian ini menggunakan metodologi *Waterfall* untuk menganalisis dan merancang aplikasi pengaman data dengan kombinasi algoritma Caesar Cipher dan Knapsack Merkle Hellman. Permasalahan utama adalah bagaimana mengintegrasikan kedua algoritma untuk meningkatkan keamanan data dalam aplikasi berbasis web menggunakan PHP dan XAMPP.

Prosedur kerja diawali dengan enkripsi *plaintext* "INFORMATIKA" menggunakan Caesar Cipher (pergeseran 3), menghasilkan *ciphertext* "LQIRUPDWLND". Selanjutnya, *ciphertext* dikonversi ke biner dan dienkripsi lagi dengan Knapsack Merkle Hellman menggunakan kunci publik {93,124,279,589,567,523,404,44}, menghasilkan deretan angka acak seperti {691,1280,1258,...}. Kombinasi ini memperkuat keamanan dengan dua lapis enkripsi.

Analisis persyaratan mencakup:

1. Fungsional : Aplikasi harus mampu melakukan enkripsi dua algoritma, menampilkan hasil, menerima input, dan diakses via web.
2. Non-fungsional (PIECES) : Kinerja (hasil enkripsi/dekripsi akurat), informasi (notifikasi proses), ekonomi (kompatibel Windows 8+, hanya butuh XAMPP), kontrol (pesan error), efisiensi (input fleksibel), dan layanan (fitur enkripsi/dekripsi).

Strategi pemecahan masalah meliputi pemahaman mendalam terhadap alur kerja kedua algoritma dan implementasinya dalam *flow chart* aplikasi. Kebutuhan perangkat meliputi laptop (Intel i5, RAM 8GB) dan perangkat lunak (Sublime Text, XAMPP).

Flow chart aplikasi terdiri dari:

1. Input data melalui form.
2. Validasi dan enkripsi data.
3. Notifikasi gagal/sukses.
4. Output *ciphertext* (huruf/acak).
5. Rancangan antarmuka mencakup:
6. Textbox input *plaintext*.

7. Tombol enkripsi.
8. Textbox output *ciphertext*.

Dengan pendekatan ini, aplikasi dirancang untuk memastikan keamanan data melalui kombinasi algoritma yang robust dan antarmuka yang user-friendly.

3. HASIL DAN PEMBAHASAN

Aplikasi pengaman data dengan kombinasi algoritma Caesar Cipher dan Knapsack Merkle Hellman diimplementasikan menggunakan beberapa *software* pendukung:

1. Google Chrome: Media pengujian aplikasi.
2. Sublime Text: Teks editor untuk pemrograman.
3. XAMPP: Server lokal untuk menjalankan aplikasi berbasis web.
4. Photoshop: Desain antarmuka aplikasi.

Cara Kerja Aplikasi

Persiapan Server Lokal

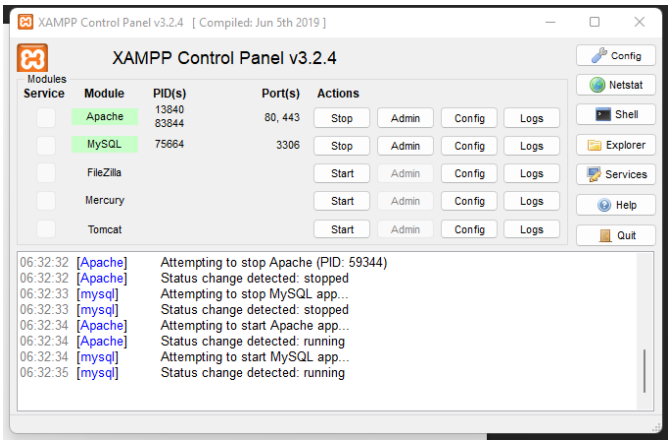
1. Instal XAMPP Control Panel dari situs resmi.
2. Aktifkan server dengan mengklik Start pada modul Apache dan MySQL.
3. Server lokal siap digunakan.

Penggunaan Aplikasi

1. Buka aplikasi melalui Google Chrome dengan memasukkan *link* lokal (misal: localhost/nama_aplikasi).
2. Jika *link* tidak valid, browser menampilkan error "404 Not Found".
3. Masukkan data teks (*plaintext*) pada kolom input yang disediakan.
4. Klik tombol Proses untuk memulai enkripsi.
5. Hasil enkripsi berupa huruf/acak (Caesar Cipher) atau deretan angka (Knapsack Merkle Hellman) akan muncul di kolom output.

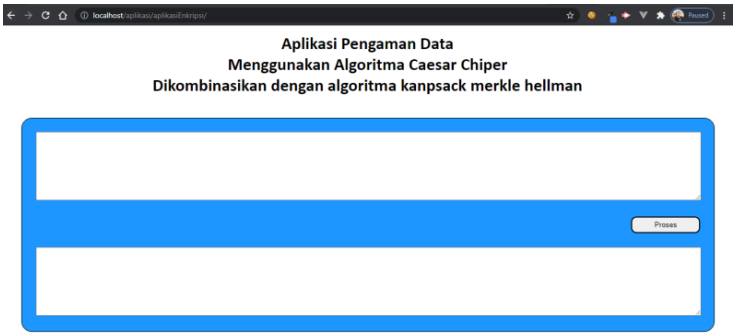
Tampilan Aplikasi dan Cara Kerja

1. XAMPP Control Panel : Digunakan untuk mengaktifkan server lokal (Apache untuk web server, MySQL untuk database).



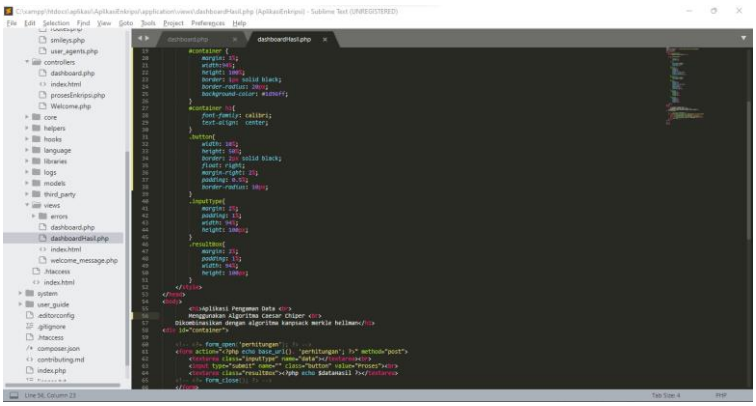
Gambar 1. Tampilan XAMPP Control Panel

2. Google Chrome : Menampilkan antarmuka aplikasi melalui *link* lokal.



Gambar 2. Tampilan Google chrome

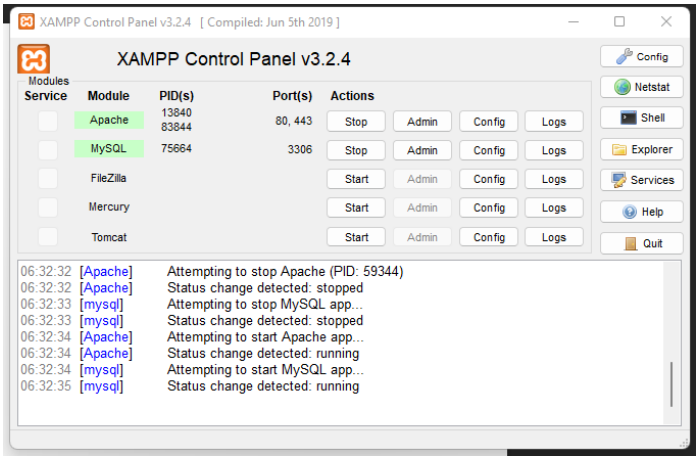
3. Sublime Text : Teks editor untuk menulis kode program dengan fitur *syntax highlighting*.



Gambar 3. Tampilan Sublime Text

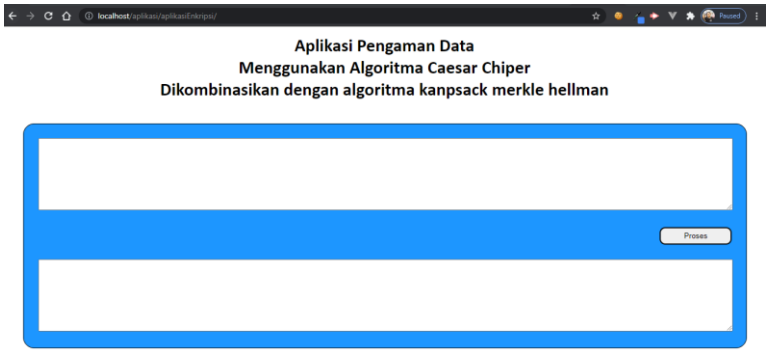
Implementasi Aplikasi

1. Hidupkan server lokal via XAMPP.



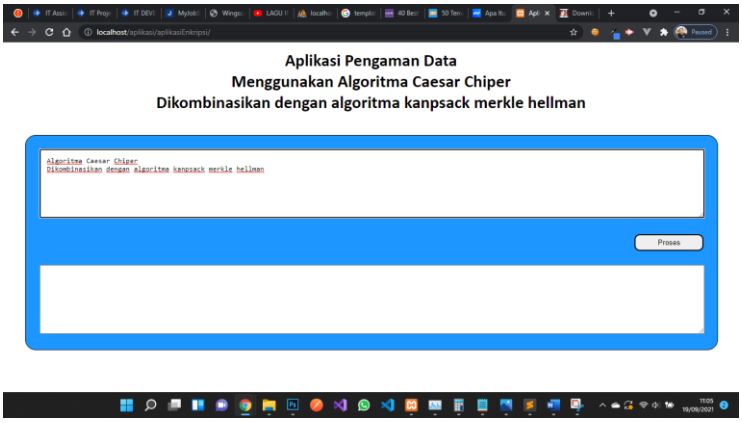
Gambar 4. Aktivasi server XAMPP

2. Akses aplikasi melalui browser dengan *link* lokal.



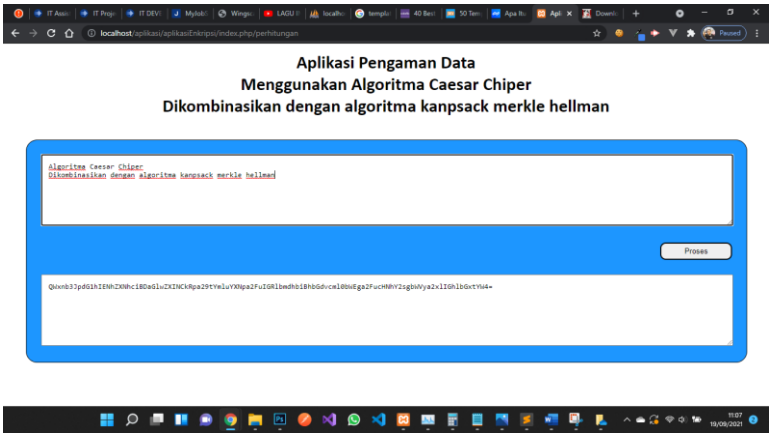
Gambar 5. Tampilan Google chrome saat mengakses aplikasi

3. Input data teks pada form dan klik Proses.



Gambar 6. Form input data

4. Hasil enkripsi ditampilkan dalam bentuk *ciphertext*.



Gambar 7. Output hasil enkripsi

Proses Enkripsi :

1. Data teks dienkripsi pertama kali dengan Caesar Cipher (contoh: "INFORMATIKA" → "LQIRUPDWLND").

2. Hasil Caesar Cipher dikonversi ke biner dan dienkripsi lagi dengan Knapsack Merkle Hellman, menghasilkan deretan angka acak (contoh: `{691, 1280, 1258, ...}`).

Fitur Aplikasi :

1. Input Data : Kolom untuk memasukkan *plaintext*.
2. Tombol Proses : Memulai enkripsi.
3. Output : Menampilkan hasil enkripsi dalam bentuk terenkripsi ganda.

Kebutuhan Sistem :

1. Perangkat Keras : Laptop dengan prosesor Intel i5, RAM 8GB, sistem 64-bit.
2. Perangkat Lunak : XAMPP, Sublime Text, dan browser Google Chrome.

Dengan langkah-langkah di atas, aplikasi siap digunakan untuk mengamankan data melalui dua lapis enkripsi, menggabungkan keunggulan Caesar Cipher dan Knapsack Merkle Hellman.

4. SIMPULAN

Berdasarkan penelitian tersebut, metode yang digunakan memiliki kelebihan dari segi keamanan karena menerapkan sistem keamanan ganda yang sulit ditembus. Namun, di balik keunggulan ini, terdapat kekurangan berupa keterbatasan aplikasi Visual Basic (VB) yang hanya dapat diakses secara *offline*. Untuk memperkuat keamanan, salah satu cara yang sering digunakan adalah kriptografi, yang memastikan pesan tersamar sehingga orang tidak menyadari adanya pesan rahasia dalam file tersebut. Oleh karena itu, berdasarkan pembahasan sebelumnya, dapat dikembangkan sebuah aplikasi yang menggabungkan dua algoritma berbeda untuk menjaga keamanan data saat pertukaran informasi, menggabungkan keunggulan keamanan ganda dengan fleksibilitas akses yang lebih baik.

DAFTAR PUSTAKA

[1] Aprianantа, Y. J. and Wijaya, L. S. (2018) 'Penggunaan Website Dan Media Sosial Dalam Membangun Citra Positif Perguruan Tinggi', *Jurnal Komunikatif*, 7(2), pp. 187–209. doi: 10.33508/jk.v7i2.1750.

[2] Nasution, A. B. (2019) 'IMPLEMENTASI PENGAMANAN DATA DENGAN MENGGUNAKAN', 3(1), pp. 1–6.

[3] Muharam, M. and Persada, A. G. (2020) 'Implementasi Penggunaan Website Sebagai Media Informasi dan Media Pemasaran Hasil Pertanian dan Peternakan Desa Sumberejo', *Automata*, 1(2).

[4] Fadlan, M. *et al.* (2017) 'Rekayasa aplikasi kriptografi dengan penerapan kombinasi algoritma knapsack merkle hellman dan affine cipher', 4(4), pp. 268–274. doi: 10.25126/jtiik.201744468.

[5] Susanto, I. A. *et al.* (2018) 'ENKRIPSI DATA PENGGAJIAN DENGAN ALGORITMA CAESAR CIPHER DAN VIGENERE CIPHER PADA PT . KEMASINDO CEPAT NUSANTARA'.

[6] Jodi, M. R. D. (2020) 'Algoritma dan Struktur Data'. doi: 10.31219/osf.io/xmbhc.

[7] Han, E. S. and goleman, daniel; boyatzis, Richard; Mckee, A. (2019) 'Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah', *Journal of Chemical In*form*ation and Modeling*, 53(9).

[8] Mubarak, A. (2019) 'Rancang Bangun Aplikasi Web Sekolah Menggunakan Uml

(Unified Modeling Language) Dan Bahasa Pemrograman Php Berorientasi Objek', *JIKO (Jurnal In*form*atika dan Komputer)*, 2(1), pp. 19–25. doi: 10.33387/jiko.v2i1.1052.

[9] Nugroho1, A. Y. (2015) 'Pembuatan aplikasi kriptografi algoritma base 64 menggunakan php untuk mengamankan data text', *Seminar Nasional In*form*atika*.