ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.3 No.1 Tahun 2024
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-3 2024
Fakultas Teknik, Universitas Pelita Bangsa, Januari 2024

Implementasi Algoritma Hill Cipher untuk Pengamanan Invoice

Implementation of Hill Cipher Algorithm for Invoice Security

Ihsan Nurul Alam[1],Muhammad Alwi Nur Fathihah[2],Muhammad Iskandar[3]
Teknik Informatika Universitas Pelita Bangsa[3]
[1]ihsannoeroel276@gmail.com, [2]alwi23mhm@gmail.com, [3]m.iskandarrr07@gmail.com

Abstract

In this digital era, the use of online invoicing is very common. However, with the use of digital technology, it is possible for invoice data leaks to occur that should not occur. not happen. One way that can prevent this from happening is to encrypt the invoice, by applying the Hill Cipher method. Hill Cipher encryption is an encryption method in classical cryptography that uses matrices to convert plaintext into ciphertext and vice versa. (ciphertext) and vice versa. In this research, we as the author will explain a website that isused to encrypt a invoice file with an encrypted invoice output.

Keywords: *Hill Cipher, Online Invoice, Data Security, Cryptograpy Method*

Abstrak

Di era digital ini, penggunaan invoice secara online sangat umum dilakukan. Namun dengan penggunaan teknologi digital yang serba praktis, sangat memungkinkan terjadinya kebocoran data invoice yang seharusnya tidak terjadi. Salah satu cara yang bisa mencegah hal ini terjadi adalah dengan mengenkripsi invoice tersebut, yaitu dengan menerapkan metode Hill Cipher. Enkripsi Hill Cipher adalah sebuah metode enkripsi dalam kriptografi klasik yang menggunakan matriks untuk mengubah teks terbuka (plaintext) menjadi teks sandi (ciphertext) dan sebaliknya. Dalam penelitian ini, kami sebagai penulis akan menjelaskan sebuah website yang digunakan untuk mengenkripsi sebuah file invoice dengan output invoice yang sudah terenkripsi.

Kata kunci*: Hill Cipher, Invoice Online, Keamanan Data, Metode Kriptografi*

Pendahuluan

Keamanan dan kerahasiaan invoice merupakan aspek krusial dalam era digital saat ini, di mana risiko peretasan dan pembukaan file invoice oleh pihak yang tidak berkepentingan semakin meningkat [1]. Ancaman kebocoran informasi atau data dalam invoice dapat menimbulkan

kerugian signifikan dan berdampak fatal terutama terhadap pihak yang terlibat dalam transaksi [2]. Oleh karena itu, penelitian ini mendasarkan diri pada kebutuhan akan sistem keamanan yang efektif untuk melindungi data transaksi dalam invoice. Dalam literatur terkait, telah terungkap bahwa risiko keamanan dalam transaksi online, khususnya invoice, semakin kompleks dan meningkat [3]. Ancaman peretasan dan kebocoran data memerlukan pendekatan yang inovatif dan handal untuk menjaga kerahasiaan informasi transaksi. Sejalan dengan itu, implementasi metode enkripsi menjadi semakin penting. Salah satu solusi yang diusulkan dan menjadi fokus penelitian ini adalah penerapan metode Hill Cipher dalam mengamankan invoice. Metode Hill Cipher merupakan teknik kriptografi yang menggunakan aritmatika modulo pada matriks persegi sebagai kunci untuk enkripsi dan dekripsi [4]. Ditemukan oleh Lester S. Hill pada tahun 1929, Hill Cipher termasuk dalam jenis polygraphic cipher yang menawarkan keamanan tambahan melalui penggunaan matriks sebagai kunci enkripsi. Penggunaan metode ini diharapkan dapat meminimalisir risiko kebocoran data invoice dengan mengenkripsi string huruf menjadi bentuk string lain dengan panjang yang sama [5]. Penelitian ini bertujuan untuk mengisi celah (gap) dalam pengetahuan terkait keamanan invoice di era digital, di mana kriptografi menjadi suatu kebutuhan mendesak [6]. Dengan mengintegrasikan metode Hill Cipher dalam konteks ini, penelitian ini tidak hanya mencoba mengatasi tantangan saat ini tetapi juga memberikan kontribusi dalam pengembangan teknik keamanan invoice yang inovatif. Oleh karena itu, melalui analisis literatur, penelitian ini akan mengeksplorasi state of the art dalam keamanan invoice, mengidentifikasi celah yang perlu diisi, dan menunjukkan inovasi yang diusulkan dalam mengamankan invoice menggunakan Hill Cipher.

Metode Penelitian

Pengumpulan Data

Pengumpulan data dilakukan dengan mengidentifikasi informasi-informasi transaksi pada invoice yang memerlukan keamanan dan enkripsi. Data yang diambil melibatkan detail barang, harga, nama penagih, dan nama pembayar. Selain itu, pengumpulan data juga mencakup kunci enkripsi yang diperlukan dalam metode Hill Cipher.

Implementasi Algoritma Hill Cipher

Hill Cipher adalah suatu teknik enkripsi simetris yang menggunakan konsep matriks untuk mengubah teks terbuka (plaintext) menjadi teks sandi (ciphertext) dan sebaliknya. Ditemukan oleh Lester S. Hill pada tahun 1929, metode ini dikategorikan sebagai cipher poligrafik yang mampu mengenkripsi blok-blok teks sekaligus, berbeda dengan cipher monografik yang hanya mengenkripsi satu karakter atau satu simbol pada satu waktu. Langkah-langkah implementasi Hill

Cipher diintegrasikan ke dalam aplikasi web menggunakan framework Flask. Proses implementasi mencakup:

a. Pemilihan Kunci

- Pilih sebuah matriks kunci persegi 2×2 yang bersifat inversible.
- Pastikan matriks kunci memiliki determinan yang relatif prima dengan ukuran alfabet yang digunakan.

b. Konversi Plainteks ke Matriks

- Konversi setiap huruf dalam plainteks menjadi angka sesuai dengan alfabet yang digunakan (misalnya, A=0, B=1, ..., Z=25).
- Susun angka-angka tersebut menjadi matriks kolom.

c. Perkalian Matriks

- Matriks plainteks dikalikan dengan matriks kunci menggunakan aritmatika modulo (mod 26), yang dapat melibatkan operasi modulo untuk menghindari nilai yang sangat besar.
- Hasil perkalian menjadi matriks cipher.

d. Konversi Matriks Cipher ke Ciphertext

Ubah matriks cipher kembali ke teks sesuai dengan alfabet yang digunakan.

Enkripsi dan Dekripsi Data Transaksi

Pada tahap ini, data transaksi (informasi barang, harga, nama penagih, dan nama pembayar) dienkripsi menggunakan algoritma Hill Cipher sesuai dengan kunci yang telah dimasukkan oleh pengguna. Setelah itu, data tersebut dapat disimpan atau dibagikan secara aman. Selanjutnya, aplikasi juga mendukung dekripsi data transaksi yang telah dienkripsi, sehingga pengguna dapat melihat informasi transaksi dalam bentuk semula.

Generate PDF dan Output

Hasil enkripsi atau dekripsi data transaksi kemudian disajikan dalam bentuk file PDF menggunakan pustaka FPDF. File PDF tersebut dapat diunduh oleh pengguna sebagai bukti transaksi yang aman dan terenkripsi. Proses ini melibatkan konversi teks hasil enkripsi menjadi format PDF, yang dapat dilihat dan diunduh oleh pengguna.

Analisis Keamanan dan Performa

Metode penelitian ini mencakup analisis keamanan terhadap hasil enkripsi yang dihasilkan oleh Hill Cipher. Dilakukan evaluasi performa untuk memastikan bahwa proses enkripsi dan dekripsi dapat dilakukan dengan cepat dan efisien tanpa mengorbankan tingkat keamanan. Pengujian keamanan juga dilakukan untuk mengidentifikasi potensi kerentanan atau kelemahan.

Hasil dan Pembahasan

a. Proses Enkripsi Hill Cipher

Awal dari proyek ini melibatkan tahap krusial, yaitu pemilihan matriks kunci Hill Cipher 2x2 yang memenuhi kriteria inversibilitas. Pemilihan matriks kunci ini mengharuskan kita untuk memastikan determinannya relatif prima dengan ukuran alfabet yang digunakan, sebuah langkah kritis untuk meningkatkan tingkat keamanan. Setelah itu, teks plainteks invoice diubah menjadi representasi numerik sesuai dengan alfabet yang ditetapkan. Kemudian, angka-angka ini diatur dalam bentuk matriks kolom yang sesuai dengan ukuran matriks kunci Hill Cipher. Proses krusial berikutnya adalah perkalian matriks plainteks dengan matriks kunci, menggunakan aritmatika modulo untuk menghindari nilai yang berlebihan. Hasilnya adalah matriks cipher, yang kemudian diartikan kembali menjadi teks terenkripsi sesuai dengan alfabet.

Proses Enkripsi pada Website

Fase selanjutnya melibatkan interaksi pengguna dengan antarmuka website. Pengguna memasukkan data transaksi melalui interface yang disediakan, dan data tersebut kemudian diolah dan diatur formatnya agar sesuai dengan kebutuhan enkripsi Hill Cipher. Matriks kunci Hill Cipher yang telah dipilih diterapkan untuk mengenkripsi data transaksi, menghasilkan matriks cipher sebagai representasi terenkripsi dari invoice. Langkah berikutnya adalah mengintegrasikan matriks cipher ke dalam template invoice menggunakan library fpdf, yang menghasilkan file PDF invoice terenkripsi. Pengguna dapat mengunduh file invoice terenkripsi ini untuk digunakan dalam transaksi, memberikan tingkat keamanan yang tinggi terhadap kerahasiaan informasi transaksi. Dengan menggabungkan proses enkripsi Hill Cipher dan fungsionalitas website, solusi yang holistik dan efisien telah tercipta untuk menjaga kerahasiaan informasi pada invoice.

Teknik Dekripsi Hill Cipher

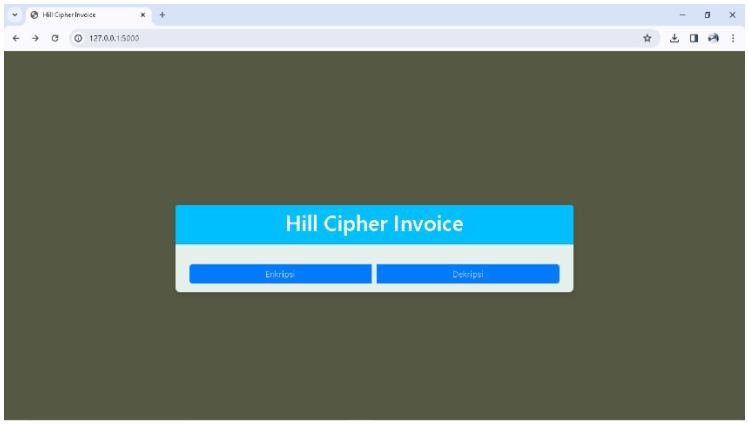
Dekripsi adalah proses pembuatan kembali data dari pesan yang di enkripsi. Proses dekripsi pada Hill Cipher pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu. Berikut ini tahapan-tahapan algoritma dekripsi Hill Cipher :

1. Menentukan nilai determinan matriks kunci K = [$a\ b\ c\ d$] det K = [$a\ b\ c\ d$] = ad-bc 2. Menentukan invers modulo = det * b mod n=1 Keterangan : det = nilai determinan kunci matriks b = bilangan positif atau negatif mod = sisa bagi untuk mencari nilai b digunakan rumus : n(k) + 1/det, dengan cara menentukan nilai K menggunakan bilangan positif 0,1,2,3…. dst dan negatif -1,-2,-3,…. dst sampai hasil perhitungan mendapatkan nilai bilangan positif atau negatif. 3. Menentukan invers matriks kunci (Mk) K = [$a\ b\ c\ d$] K-1 = [$d\ -b\ -c\ a$].

b. Tampilan dan Menu Website

1. Tampilan Menu Utama

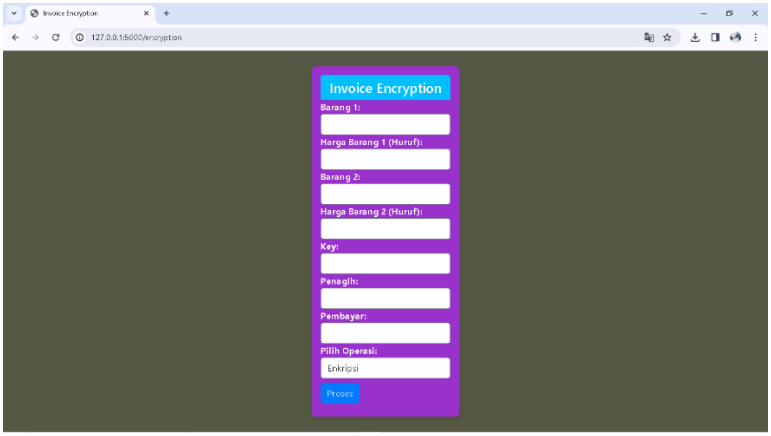
Pada halaman utama ini user memilih menu enkripsi atau dekripsi.



Gambar 1: Tampilan Halaman Utama

2. Tampilan Menu Enkripsi

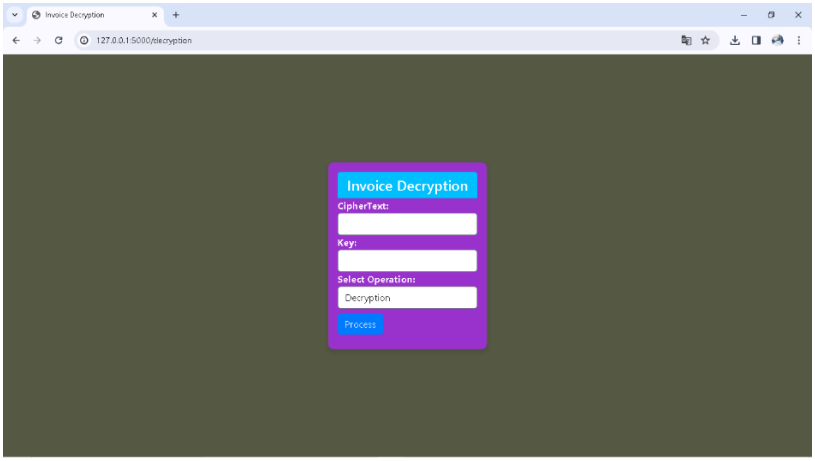
Pada menu ekripsi terdapat kolom untuk mengisi informasi barang, harga, nama penagih, dan nama pembayar yang akan di enkripsi, juga terdapat menu untuk kita menentukan key.



Gambar 2: Tampilan Halaman Enkripsi

3. Tampilan Menu Dekripsi

Pada menu deskripsi juga sama seperti pada menu enkripsi dan hasil setelah di submit akan berupa file PDF yang sudah terenkripsi.



Gambar 3: Tampilan Halaman Dekripsi

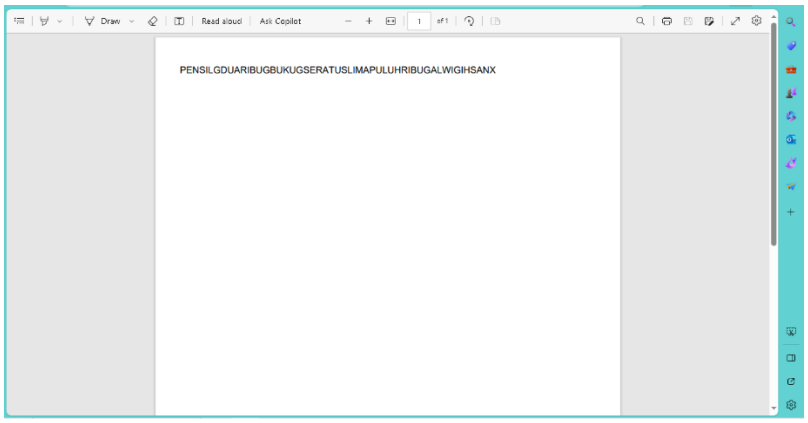
4. Hasil Enkripsi

Untuk hasil ekripsi dari invoice yang kita buat maka hasilnya akan berupa teks isi dari invoice yang sudah terenkripsi.

Gambar 4: Hasil Enkripsi

1. Hasil Deskripsi

Begitupun untuk hasil deskripsi dari invoice yang kita enkripsi maka hasilnya juga akan menjadi sebuah file pdf,untuk mendeskripsikan filenya disini masih menggunakan cara manual yakni dengan copy teks enkripsinya lalu di paste pada menu deskripsi dan setelah di submit maka hasilnya akan terunduh sebagai file pdf yang sudah di deskripsi.



Gambar 5: Hasil Dekripsi

Kesimpulan

Berdasarkan informasi yang diberikan mengenai penggunaan Hill Cipher dalam proyek pembuatan website untuk invoice terenkripsi, dapat diambil beberapa kesimpulan. Pertama, Hill Cipher merupakan metode enkripsi yang dirancang untuk memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan metode enkripsi konvensional pada masanya. Keberhasilan Hill Cipher tergantung pada pemilihan kunci yang tepat, dan metode ini cocok untuk mengamankan informasi sensitif seperti data transaksi pada invoice. Kedua, integrasi Hill Cipher pada website pembuatan invoice menunjukkan upaya untuk menyajikan solusi yang holistik dan efisien. Proses enkripsi Hill Cipher diimplementasikan secara mulus dalam alur pembuatan invoice, memastikan

bahwa data transaksi terjaga kerahasiaannya. Pengguna dapat dengan mudah menghasilkan dan mengunduh invoice terenkripsi melalui antarmuka web, menggabungkan kenyamanan pengguna dengan tingkat keamanan yang tinggi. Kesimpulannya, penggunaan Hill Cipher dalam proyek ini menunjukkan pendekatan proaktif untuk melindungi informasi transaksi pada invoice. Dengan memadukan kekuatan matematika matriks Hill Cipher dan kemudahan akses melalui website, proyek ini memberikan solusi yang dapat diandalkan dan aman dalam mengatasi risiko kebocoran informasi pada era digital saat ini.

Daftar Rujukan

[1] Desimeri L., Bosker S., and Anita S., "Penerapan Algoritma Hill Cipher dan Leeast Significant Bit (LSB) Untuk Pengamanan Pesan Pada Citra Digital*," Jurnal JISKa*, Vol. 4, No.3, pp. 1 – 11, 2020

[2] Nurharianna S., Ilham F., and Divi H., "Menerapkan Algoritma Hill Cipher dan Matriks 2×2 Dalam Mengamankan File Teks Menggunakan Kode ASCII," *Jurnal Ilmu Komputer dan Sistem Informasi*, Vol. 1, No.2, pp. 70 – 83, 2022

[3] Novita P. D., David JM Sembiring, Raheliya br. Ginting, and Meiliyani br. Ginting, Pengamanan Data dengan Kriptografi Hibrida Algoritma Hill Cipher dan Algoritma LUC serta Steganografi Chaotic," *Jurnal Ilmu Komputer dan Sistem Informasi*, Vol. 1, No.2,.2022

[4] Akbar S., M. Zarlis, Sawaluddin, and Hartama D., "Pengamanan Pesan Menggunakan Algoritma Hill Cipher Dalam Keamanan Komputer," Jurnal Mahajana Informasi, Vol. 3, No.2, 2019

[5] I. Saputri, P. Wibowo, P. Ratricia, and A. Ikhwan, "Pengamanan Pesan Menggunakan Metode Hill Chiper Dalam Keamanan Informasi," *Jurnal Bulletin of Information Technology (BIT)*, Vol. 3, No.4, pp. 341 – 349, 2022

[6] R. Wardhani, S. R. Nurshiami, and N. Larasati, "Komputasi Enkripsi Dan Dekripsi Menggunakan Algoritma Hill Cipher," *J. Ilm. Mat. dan Pendidik. Mat.*, Vol. 14, No.1, pp. 45, 2022

[7] Frinto T., Nurhayati, Abdul M., Erwin G., "Optimizing the Complexity of Time in the Process of Multiplying Matrices in the Hill Cipher Algorithm Using the Strassen Algorithm," *The 7th International Conference on Cyber and IT Service Management (CITSM 2019)* , 2019

[8] Agung A., Nono H., Arip S., "Combination of hill cipher algorithm and Caesar cipher algorithm for exam data security," *Buana Information Technology and Computer Sciences (BIT*

and CS), Vol. 1, pp. 42-45, 2020

[9] M. Abdul R., Kiswara A. S., Alfian F. H., "Primary key encryption using hill cipher chain (case study: Stie mandala pmb site)," *International Conference on Mathematics, Geometry, Statistics, and Computation (IC-MaGeStiC 2021)*, pp. 222-227, 2022

[10] Adetya M. M., Fauziatun H., Sinta D.E,.Adnan B.N., "Perancangan Sistem Keamanan Website Dengan Metode Hill Chiper," Jurnal Sains dan Teknologi (JSIT), Vol. 3, No. 1, pp. 120-129, 2023