ENKRIPSI DATA PENGGAJIAN DENGAN ALGORITMA CAESAR CIPHER DAN VIGENERE CIPHER PADA PT. KEMASINDO CEPAT NUSANTARA

Ismail Adi Susanto[1], **Achmad Solichin**[2]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : adisusantoismail@gmail.com [1)], achmad.solichin@budiluhur.ac.id [2)]

Abstract

PT. Kemasindo Cepat Nusantara adalah sebuah perusahaan yang bergerak dibidang pengiriman barang baik melalui darat, laut ataupun udara. PT. Kemasindo Cepat Nusantara sendiri sudah memiliki sistem penggajian yang akurat dan tepat. Untuk menjaga kerahasiaan daripada informasi tersebut maka dibutuhkan suatu sistem penggajian terenkripsi yang dapat menjaga kerahasiaan dari informasi gaji para pegawai. Kriptografi merupakan metode keamanan data yang mengubah data asli (plaintext) menjadi data yang tidak bisa dibaca (ciphertext), proses ini disebut proses enkripsi. Serta dapat mengubahnya kembali dari data yang tidak bisa dibaca (ciphertext) menjadi data yang bisa dibaca (plaintext), proses ini disebut proses dekripsi. Seiring dengan hal tersebut maka dibuatlah sebuah enkripsi database sistem penggajian. Enkripsi ini memakai algoritma Caesar dan Vigenere. Algoritma Caesar termasuk sandi subtitusi dimana setiap huruf pada teks terang (plainteks) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alphabet. Sedangkan algoritma enkripsi Vigenere sangat dikenal karena mudah dipahami dan diimplementasikan. Teknik untuk menghasilkan ciphertext bisa dilakukan menggunakan substitusi angka maupun bujursangkar Vigènere. Teknik susbtitusi Vigènere dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, hampir sama dengan kode geser. Sistem penggajian enkripsi berbasis web ini dapat diimplementasikan dengan baik.

Kata Kunci: Sistem Penggajian, Enkripsi, Dekripsi Caesar Cipher, Vigenere, Web

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan dunia teknologi dan komunikasi begitu pesat, memudahkan kita untuk melakukan pertukaran data dengan pihak lain secara cepat. Teknologi komputer juga memudahkan kita untuk menyimpan file dalam bentuk data sehingga mengurangi penggunaan kertas yang secara fisik cukup memakan tempat. Dalam dunia informasi, ada informasi yang bersifat umum, yakni informasi yang boleh dilihat atau dibaca oleh siapa saja bahkan terkadang boleh diubah. Dan ada informasi yang bersifat rahasia dimana informasi ini hanya boleh dilihat atau dibaca oleh pihak-pihak tertentu saja.

Selain sifatnya yang umum atau rahasia, ada juga informasi yang tingkat kepentingan nya tinggi, sehingga informasi itu harus utuh walau disimpan dalam waktu yang lama. Untuk menanggulangi hal tersebut dapat dilakukan pengamanan data dengan menggunakan konsep kriptografi. PT. Kemasindo Cepat Nusantara adalah sebuah perusahaan yang bergerak di bidang pengiriman barang baik melalui darat, laut ataupun udara. PT. Kemasindo Cepat Nusantara sendiri sudah memiliki sistem penggajian yang akurat dan tepat. Sistem penggajian ini sendiri dipakai untuk menghitung berapa besar gaji para karyawan yang bekerja disini. Data dari sistem ini pun bersifat rahasia. Namun tetap beresiko jika tidak dilakukan pengamanan data. Maka untuk menjaga kerahasiaan daripada informasi *database* sistem penggajian tersebut, dibutuhkan suatu aplikasi yang dapat menjaga *privacy* dari informasi *database* dari sistem penggajian tersebut.

Salah satunya dikenal dengan sebutan kriptografi Kriptografi merupakan metode keamanan data yang mempunyai dua proses yaitu enkripsi dan dekripsi. Enkripsi adalah proses mengubah data asli (*plaintext*) menjadi data yang tidak bisaatau sulit dipahami (*ciphertext*). Sedangkan dekripsi merupakan kebalikannya, yaitu mengubah kembali data yang telah dienkripsi menjadi data asli yang bisa dibaca kembali. Teknik ini memerlukan kunci atau biasa disebut dengan *key*. *Key* yang dimaksud disini adalah kunci yang dipakai untuk melakukan sebuah proses enkripsi dan dekripsi.

Permasalahan yang dibahas penulis pada penelitian ini adalah perlindungan data transaksi gaji dalam bentuk *database* pada PT. Kemasindo Cepat Nusantara yang belum terproteksi, sehingga memungkinkan pihak lain yang tidak berwenang atau tidak berkepentingan untuk dapat melihat, mengambil, dan memanipulasi informasi rahasia yang terdapat pada *database* sistem penggajian tersebut. Oleh karena itu penulis akan mengimplementasikan algoritma *Caesar Cipher* dan *Vigenere Cipher* untuk mengenkripsisi data penggajian tersebut. Berdasarkan permasalahan yang terdapat pada rumusan masalah sebelumnya, maka

tujuan yang diharapkan penulis dari penelitian ini adalah penulis dapat mengimplementasikan algoritma kriptografi *Caesar Cipher* dan *Vigenere* Cipher ke *database* sistem penggajian untuk mengamankan data rahasia perusahaan dan pegawai yang nantinya akan digunakan oleh PT. Kemasindo Cepat Nusantara untuk mengurangi kemungkinan terjadinya pencurian data atau informasi.

Agar permasalahan yang dibahas tidak meluas dan keluar dari ruang lingkup mengenai enkripsi dan dekripsi, maka diperlukan batasan masalah sebagai berikut :

a. Algoritma yang digunakan dalam penulisan penelitian ini dalah algoritma Caesar Cipher untuk password yang dienkripsi dan vigenere cipher untuk enkripsi database
b. Yang diamankan adalah database tabel penggajian dari sistem penggajian yang ada di Kemasindo Cepat Nusantara.
c. Penulisan ini membahas tentang enkripsi dan dekripsi bukan sistem penggajian yang ada di PT Kemasindo Cepat Nusantara

2. Tinjuan Pustaka

2.1 Algoritma *Caesar Cipher*

Dalam kriptografi algoritma Caesar atau sandi Caesar merupakan salah satu teknik enkripsi paling terkenal [1]. Algoritma ini termasuk sandi subtitusi dimana setiap huruf pada teks terang (plainteks) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alphabet. Algoritma ini bermula dari kaisar Romawi yaitu Julius Caesar yang menyandikan pesan yang dikirim kepada para bawahannya. Caranya dengan mengganti atau mensubtitusi setiap karakter dengan karakter lain dalam susunan abjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu *k*=3).

Algoritma ini biasa digunakan baik untuk huruf kecil maupun huruf capital tidak *case sensitive*. Ini adalah jenis substitution *cipher* dimana setiap huruf pada *plaintext* digantikan oleh beberapa surat tetap jumlah posisi down the alphabet. Misalnya, dengan pergeseran dari 3, yang akan diganti dengan D, B akan menjadi E, dan seterusnya.

Enkripsi langkah yang dilakukan oleh Kaisar *cipher* sering dimasukkan sebagai bagian dari skema lebih kompleks, seperti Vigenère *cipher*, dan masih memiliki aplikasi modern di ROT13 sistem. Seperti semua satu abjad substitution *ciphe*rs, *Caesar cipher* yang mudah rusak dan dalam prakteknya pada dasarnya tidak menawarkan keamanan komunikasi. Transformasi yang dapat diwakili oleh dua deretan alphabets the *cipher* alfabet adalah *alfabet* plain diputar kiri atau kanan oleh beberapa nomor posisi.

Algoritma ini pun mempunyai beberapa kelebihan yaitu:

a. Teknik ini adalah algoritma paling sederhana
b. Algoritma caesar cipher tertua dan paling terkenal dalam perkembangan ilmu kriptografi
c. Sangat mudah digunakan untuk keperluan penyembunyian data

Selain kelebihan, algortima ini juga menyimpan beberapa kekurangan seperti :

a. Tingkat keamanannya rendah, dikarenakan jumah kuncinya hanya 26 kunci saja
b. Teknik pemecahan kata kunci tersebut dapat dilakukan dengan cara melakukan pengecekan terhadap semua kunci yang ada yang berjumlah 26 kunci.

Penghitungan algoritma caesar cipher menggunaka rumus penggunaan alphabet standar yaitu :

a. Enkripsi
   $C_1 = (P_1 + K) \bmod 26$
b. Dekripsi
   $P_1 = (C_1 - K) \bmod 26$

Disertakan pula rumus enkripsi dan dekripsi caesar cipher untuk penggunaan tabel ASCII yaitu :

a. Enkripsi
   $C_1 = (P_1 + K) \bmod 256$
b. Dekripsi
   $P_1 = (C_1 - K) \bmod 526$

Jenis-jenis proses penghitungan algoritma caesar cipher pun bermacam-macam seperti:

a. Algoritma Subtitusi Menggunakan *Cesar Cipher*
   Langkah-langkah yang dilakukan untuk membentuk *ciphertext* dengan caesar cipher yaitu dengan cara memnentukan besarnya pergeseran karakter yang digunakan dalam membentuk ciphertext ke plaintext serta menukarkan karakter pada plaintext menjadi ciphertext engan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.
b. Algoritma Subtitusi Menggunakan *Cipher Key*
   Algoritma *cipher* key merupakan metode yang menggunakan sebuah kata sebagai kata kunci yang disubtitusikan kedalam abjad. Dimana pesan yang akan disampaikan sama namun menggunakan kata kunci yang tidak sama.

2.2 Studi Literature

Tabel 1. Studi Literatur

No	Judul Junal	Penulis	Tahun Penerbit dan ISSN	Kesimpulan
1.	Enkripsi Dan Dekripsi Teks Menggunakan Algoritma *Improved Caesar Cipher*	Agus Susanto, Fridariyani, Abdul Rahman [2]	2014 – STMIK Global Informatika MDP – 2407-1102	Penerapan Algoritma Improved Caesar *Cipher* untuk enkripsi dan dekripsi teks ini dapat meningkatkan keamanan teks.

2.	Kriptografi Dengan Algoritma Grass Caesar	Ana Wahyuni [4]	2016 – Fakultas Ilmu Komputer Universitas AKI – 2087-0868	Algoritma Grass Caesar dapat digunakan untuk mengirim pesan atau data rahasia via Internet. Penambahan pola grass meningkatkan keamanan transmisi data/ pesan tersebut.
3.	Analisis Kombinasi Metode *Caesar Cipher*, *Vernan Cipher* dan *Hill Cipher* Dalam Proses Kriptografi	Khairani Puspita, M. Rhifky Wayahdi [6]	2015 – STMIK Amikom Yogyakarta – 2302-3805	Penelitian ini mengkombinasikan algoritma *Caesar Cipher*, *Vernam Cipher*, dan *Hill Cipher* sehingga enkripsi sulit dipecahkan.
4.	Implementasi Algoritma Caesar, *Cipher* Disk Dan Scytale Pada Aplikasi Enkripsi Dan Dekripsi Pesan Singkat, LumaSMS	Yusuf Triyuswoyo, Ferina Ferdianti, Donny Ajie Baskoro, Lia Ambarwati, Septiawan [7]	2014 - Jurusan Management Sistem Informasi, Universitas Gunadarma – 2302-3740	Aplikasi keamanan pesan singkat dengan menggunakan tiga algoritma kriptografi klasik, yaitu: Caesar, *Cipher* Disk (Vigenere) dan Scytale. Dari hasil uji tes tingkat keamanan, aplikasi ini mampu melindungi isi pesan singkat yang dikirimkan melalui jaringan operator seluler.
5.	Implementasi Algoritma Caesar *Cipher* Dan Hill *Cipher* Pada Database Sistem Inventori TB Mitra Jepara	Egar Dika Santosa [5]	2015 – Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dian Nuswantoro - 3520 - 9102	Fungsi Algoritma Caesar *cipher* dan Hill *cipher* dapat di implementasikan kedalam koding bahasa pemrograman PHP dengan baik

Kesimpulan dari semua studi literature dan referensi serta tinjauan pustaka bahwa implementasi untuk algoritma *caesar cipher* dan vigenere dapat dilakukan dengan berbagai kondisi. Dan implementasi ini akan meningkatkan keamanan data dari sistem yang digunakan di perusahaan Kemasindo Cepat Nusantara. Meskipun tergolong algoritma sederhana namun *caesar cipher* dan vigenere lumayan hebat dalam hal pengamanan data.

3. Metodologi Dan Penyelesaian Masalah

3.1 Metode Penelitian

Beberapa metode penelitian yang digunakan oleh penulis dalam penyusunan penelitian ini meliputi :

a. Analisis Data
   Tahapan ini digunakan untuk menganalisa algoritma kriptografi Caesar dan Vigenere dengan cara mencari dan membaca-baca buku refrensi serta memanfaatkan situs search engine seperti google, dan melihat pembahasan analisis data yang sudah ada di internet
b. Wawancara
   Adalah suatu cara untuk memperoleh data dengan cara tanya jawab langsung ke user untuk mengetahui permasalahan yang dihadapi dan mendiskusikan aplikasi yang diharapkan dapat memecahkan masalah tersebut.
c. Perancangan Sistem
   Tahapan ini dilakukan dengan cara merancang sistem yang akan dibangun dan mengimplementasikan langsung algoritma Caesar Cipher dan algoritma Vigenere Cipher ke dalam sebuah sistem penggajian berbasis web

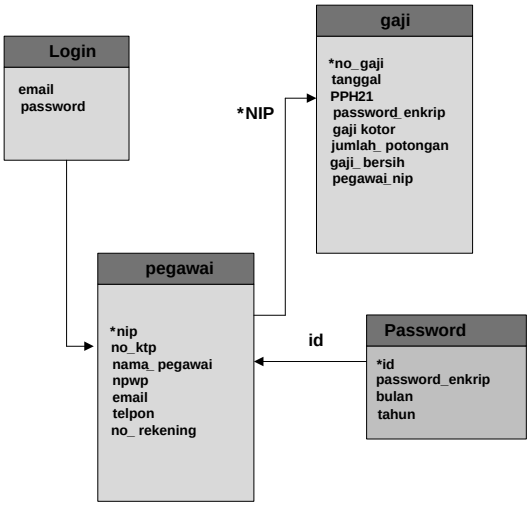
3.2 Analisis dan Penyelesaian Masalah

Dari permasalahan yang telah diuraikan diatas , diperlukan adanya sebuah sistem penggajian yang dapat menjaga kerahasiaan informasi atau data yang menyangkut gaji karyawan. Sehingga data gaji karyawan tidak dapat dilihat secara sembarangan. Sistem penggajian tersebut akan dienkripsi databasenya dengan cara mengimplementasikan algoritma Caesar Cipher dan Vigenere Cipher. Dengan adanya sistem penggajian enkripsi ini diharapkan suatu informasi atau data rahasia yang bersifat penting dapat disimpan dan tidak

disalahgunakan oleh pihak yang tidak bertanggung jawab.

3.3 Perancangan Database

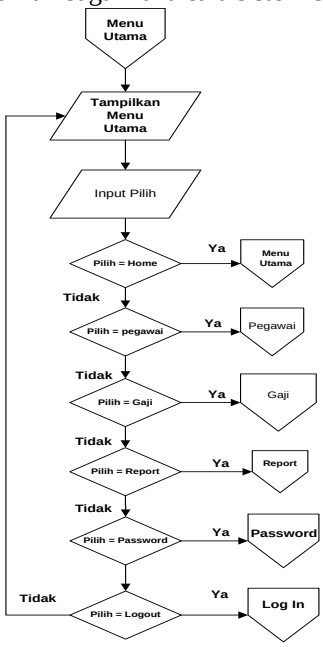
Dalam hal perancangan sistem penggajian kriptografi berbasis web ini diperlukan perancangan database untuk menampung data gaji serta pegawai perusahaan dan database inilah yang nantinya akan dienkripsi.



Gambar 1 : LRS

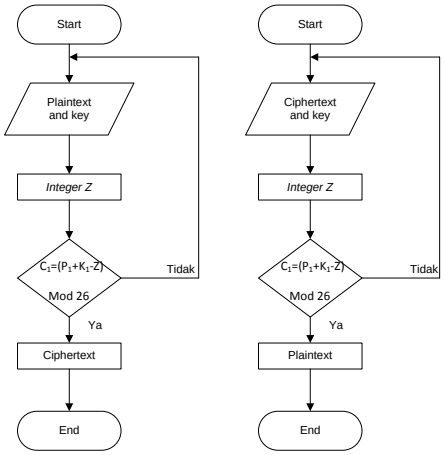
3.4 Flowchart Dan Algoritma

Flowchart adalah suatu alur proses yang menggambarkan bagaimana cara sistem berjalan.



Gambar 2. Flowchart Menu Log In

Flowchart menu utama seperti di atas adalah proses setelah pengguna melakukan log in. Kemudian setelah login maka pengguna akan masuk ke dalam menu utama sistem penggajian yang terenkripsi. Dimenu utama terdapat menu home, pegawai, gaji, report serta password dan tombol log out untuk keluar dari menu utama sistem.



Gambar 3. Flowchart Proses Enkripsi Dan Dekripsi Database Pada Algoritma Caesar Cipher

Pada gambar di atas menjelaskan proses atau alur dari enkripsi atau proses penyembunyian atau pengacakan data. Proses enkripsi dimulai dengan membaca data didatabse dan panjang data di database.

1. Tampilkan Form Menu Utama
2. ***Else If*** pilih = "*Home* ***Then***
3. Tampilkan Form Menu Utama
4. ***Else If*** pilih = "Pegawai" ***Then***
5. Tampilkan Form *List Of* Pegawai"
6. ***Else If*** pilih = "Gaji" ***Then***
7. Tampilkan Form *List Of* Gaji Pegawai
8. ***Else If*** pilih = "*Report*" ***Then***
9. Tampilkan Form *Report*
10. ***Else If*** pilih = "*Log Out*" ***Then***
11. Tampilkan Form *Log in*
12. ***End If***

Algortima di atas adalah algoritma yang menjelaskan tentang menu utama. Yang mana menjelaskan cara kerja dari menu utama sistem.

1. *Start*
2. *Select database for enkripsi*
3. *Input password*
4. Pengecekan *Password*
5. Baca pesan serta panjang pesan, baca *output* lokasi & nama *database.*
6. Mulai*enkripsi*
7. Ubah pesan dan *password* ke *caesar chiper,* ubah bits pesan ke *caesar cipher* untuk pesan dan *password*
8. Enkripsisi pesan dan *password*
9. Tulis kembali enkripsi pesan dan *password* , simpan dilokasi *output stream*
10. ***If*** *"*enkripsisi sukses*?"* ***Then***
11. Proses simpan data *databse* dari *crypto file* ke *output file.*
12. ***Else***
13. *Kembali ke baris 1*
14. ***End If***

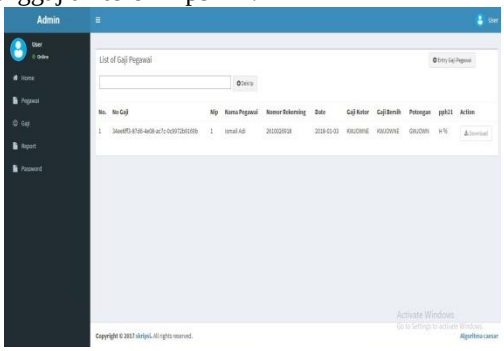
Algortima di atas adalah penjelasan tentang proses bagaimana sistem penggajian dienkripsi menggunakan algoritma caesar cipher.

4. Hasil Dan Pembahasan

4.1 Rancangan Layar

Gambar 4 : Rancangan Layar Menu Utama

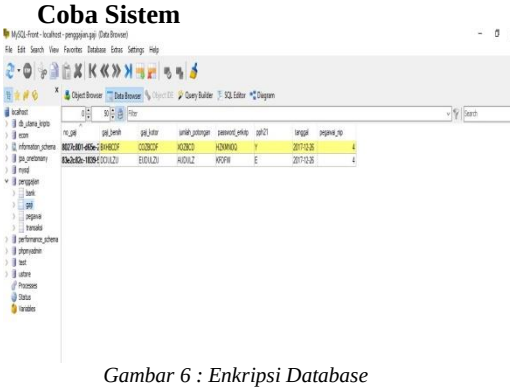
Gambar di atas adalah gambar rancangan layar menu utama, dimana rancangan utama ini memuat semua menu yang ada di sistem penggajian terenkripsi ini.



Gambar 5 : Rancangan Layar List Of Gaji Pegawai

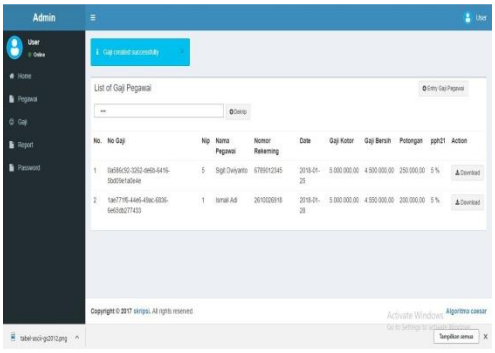
Gambar di atas adalah rancangan layar list of gaji pegawai. Menu ini berisi data gaji pegawai yang telah dienkripsi sebelumnya.

4.2 Analisa Hasil Implementasi Dan Uji Coba Sistem



Gambar 6 : Enkripsi Database

Gambar di atas menjelaskan tentang database sistem penggajian yang telah di enkripsi. Bentuk dan format database menjadi tidak terbaca karena data tersebut sudah di acak oleh algoritma caesar cipher dan vigenere cipher.



Gambar 7 : Data Gaji Yang Telah Di Dekirpsi

Gambar di atas adalah gambar layar yang berisi data sistem penggajian yang telah di didekripsi sebelumnya. Setelah didekripsi maka semua data jadi terbaca dengan jelas.

4.3 Kelebihan dan Kekurangan Sistem Penggajian

Sistem penggajian berbasis web ini mempunyai beberapa kelebihan dan kekurangan. Kelebihan sistem ini yaitu :

a. Sistem penggajian krptografi berbasis web lebih aman .
b. Sistem ini bisa dilakukan secara online karena berbasis web
c. Kerahasiaan suatu dokumen lebih terjamin dan aman.

Sedangkan untuk kekurangan dari sistem penggajian ini sendiri yaitu :

a. Kunci atau password harus benar benar diingat dan disimpan untuk melakukan dekripsi
b. Untuk proses ekripsi harus satu persatu data dan tidak langsung semuanya.
c. Untuk melakukan enkripsi password harus dibuat perbulan, tidak bisa langsung untuk satu tahun.

5. Kesimpulan

Adapun kesimpulan yang diperoleh dari perancangan, pembuatan, serangkaian uji coba dan analisa sistem informasi penggajian terenkripsi berbasis web ini, maka dapat dibuat suatu kesimpulan antara lain :

a. Dengan adanya sistem penggajian enkripsi berbasis web ini, informasi atau data gaji karyawan dapat lebih terjaga kerahasiaannya.
b. Sistem penggajian enkripsi ini memberikan suatu hal yang baru dan menarik untuk diterapkan bagi pihak-pihak yang berkepentingan.
c. Sistem penggajian ini mudah diterapkan dan digunakan bagi admin baru.
d. Implementasi algoritma caesar cipher dan vigenere bisa dilakukan.

6. Daftar Pustaka

[1] Ariyus, D., 2014. *Pengantar ilmu kriptografi: teori, analisis, dan implementasi* S. Suyantoro, ed., Yogyakarta: ANDI.

[2] Fridariyani dan Susanto, Rahman 2014. Enkripsi Dan Dekripsi Teks Menggunakan Algoritma *Improved Caesar Cipher*. STMIK Global Informatika MDP

[3] Manoj, I.V.S., 2012. Cryptography and Steganography. *International Journal of Computer Applications*, 1(12), pp.63–68.

[3] Sadikin, R., 2012. *Kriptografi untuk keamanan jaringan* Edisi Pert., Yogyakarta: ANDI.

[4] Wahyuni, Ana 2016. Kriptografi Dengan Algoritma Grass Caesar. Fakultas Ilmu Komputer Universitas AKI

[5] Santosa, Egar Dika 2015. Implementasi Algoritma Caesar Cipher Dan Hill Cipher Pada Database Sistem Inventori TB Mitra Jepara, Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dian Nuswantoro

[6] Puspita, K., & Wayahdi, M. R. (2015, February). Analisis Kombinasi Metode Caesar Cipher, Vernam Cipher, Dan Hill Cipher Dalam Proses Kriptografi. In Jurnal Seminar Nasional Teknologi Informasi dan Multimedia.

[7] Triyuswoyo, Y., Ferdianti, F., Baskoro, D. A., Ambarwati, L., & Septiawan, S. (2014). Implementasi Algoritma Caesar, Cipher Disk, Dan Scytale Pada Aplikasi Enkripsi Dan Dekripsi Pesan Singkat, Lumasms. Prosiding KOMMIT.