IMPLEMENTASI APLIKASI KRIPTOGRAFI CAESAR CIPHER DENGAN PHP

Article · January 2021

CITATIONS
0

READS
1,458

5 authors, including:

Nandana Guna
Siliwangi University
5 PUBLICATIONS **0** CITATIONS

SEE PROFILE

IMPLEMENTASI APLIKASI KRIPTOGRAFI CAESAR CIPHER DENGAN PHP

Anggi Suprayogi
187006001
Program Studi Informatika
Universitas Siliwangi

Fakhrul Rifqi Darmawan
187006097
Program Studi Informatika
Universitas Siliwangi

Muhammad Arfan Maulana W
187006095
Program Studi Informatika
Universitas Siliwangi

Nandana Surya Guna
187006103
Program Studi Informatika
Universitas Siliwangi

Rafi Dhiya Nurhaq
187006076
Program Studi Informatika
Universitas Siliwangi

I. PENDAHULUAN

Keamanan dan kerahasiaan data atau informasi merupakan salah satu aspek yang penting dari suatu data atau informasi. Dengan perkembangan teknologi saat ini, setiap orang akan mudah memperoleh data atau informasi. Apabila data atau informasi tersebut tidak di lindungi, maka secara mudah orang lain akan mengetahui data atau informasi yang dimiliki. Berbagai cara pun dilakukan untuk melindungi data atau informasi tersebut.

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. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi seperti ini disebut juga sebagai cipher abjad tunggal. Caesar cipher adalah dasar enkripsi yang sangat baik untuk dipahami sebelum membahas enkripsi berbasis karakter lainnya yang lebih rumit.

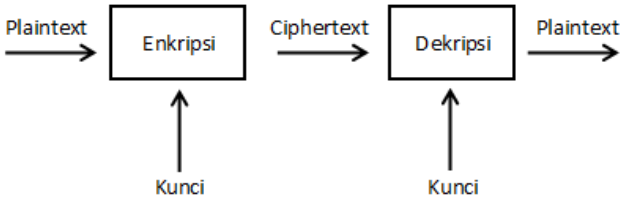
Dalam dunia kriptografi, Caesar cipher adalah salah satu teknik enkripsi paling sederhana dan paling terkenal dengan menggunakan metode subtitusi.

II. LANDASAN TEORI

A. *Kriptografi*

Kriptografi (cryptography) merupakan ilmu dan seni untuk menjaga pesan agar aman. *(Cryptography is the art and science of keeping messages secure)* "Crypto" berarti "Secret" (rahasia) dan "Graphy" berarti "Writing" (tulisan). Jadi, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan yang akan dikirim ke penerima sehingga data atau pesan tersebut aman dan tidak diketahui oleh pihak ketiga. Data atau pesan yang akan dikirim di ubah menjadi kode-kode yang tidak dipahami oleh pihak ketiga.

Kriptografi membuat data atau pesan menjadi kode-kode terlebih dahulu oleh pengirim. Proses ini dikenal dengan enkripsi. Enkripsi diartikan sebagai proses diubahnya data atau pesan yang hendak dikirim menjadi bentuk yang hampir tidak dikenali oleh pihak ketiga setelah data atau pesan itu sampai kepada penerima, maka penerima melakukan dekripsi yang merupakan kebalikan dari enkripsi. Dekripsi diartikan sebagai proses mengubah data atau pesan kembali kebentuk semula sehingga data atau pesan tersampaikan dan dimengerti oleh si penerima, datau atau pesan asli dinamakan plaintext sedangkan sesudah dikodekan dinamakan chipertext. Proses enkripsi dan dekripsi memerlukan kunci dalam mekanismenya dan biasanya berupa string atau deretan bilangan. Berikut ini contoh proses enkripsi dan dekripsi yang digunakan dalam pengiriman pesan. Proses enkripsi dan dekripsi yang digunakan dalam pengiriman pesan dapat dilihat pada Gambar 1.

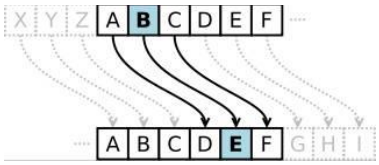


Gambar 1. Proses Enkripsi Dekripsi

B. *Caesar Cipher*

Metode penyandian ini dinamakan caesar cipher, setelah digunakan Julius Caesar untuk berkomunikasi dengan para panglimanya. Dalam kriptografi caesar cipher dikenal dengan nama seperti: shift cipher, Caesar's code atau Caesar shift.

Caesar Cipher merupakan teknik enkripsi yang paling sederhana dan banyak digunakan. Cipher ini berjenis chiper subtitusi, dimana setiap huruf pada plaintext nya diganti dengan huruf lain yang tetap pada posisi alfabet. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya, untuk proses pergeseran dapat dilihat pada Gambar 2.



Gambar 2. Proses pergeseran 3 huruf

Gambar 2 dapat dipresentasikan dengan menyelaraskan plaintext dengan chipertext ke kiri atau ke kanan sebanyak jumlah pergeseran yang diinginkan. Sebagai contoh denga jumlah pergeseran sebanyak 3.

Plaintext : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher : DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk membaca pesan yang dienkripsi penerima dapat menyelaraskan huruf chipertext yang diterima dengan plaintextyang tepat berada diatasnya. Sebagai contoh dekripsinya sebagai berikut.

Cipher : NHDPDQDQ LQIRUPDVL

Plaintext : KEAMANAN INFORMASI

Proses enkripsi pada Caesar Cipher dapat direpresentasikan menggunakan operator aritmatika modulo 26 setelah sebelumnya setiap huruf di transformasi kedalam angka, yaitu A = 0, B = 1, ... , Z = 25. Maka caesar cipher dirumuskan sebagai berikut: Proses enkripsi suatu huruf P dengan pergeseran K dapat dinyatakan secara matematis sebagai berikut:

Enkripsi: C = E(P) = (P + K) mod26

Dekripsi: P = D(C) = (C – K) mod26

Dengan C adalah ciphertext, P adalah plaintext, K adalah kunci rahasia, E(P) adalah enkripsi, dan D(C) adalah dekripsi.

Kelemaham dari caesar cipher adalah dapat dipecahkan dengan cara brute force attack, suatu bentuk serangan yang dilakukan dengan mencoba-coba berbagai kemungkinan untuk menemukan kunci. Bisa juga menggunakan exhaustive key search, karena jumlah kunci sangat sedikit (hanya ada 26 kunci).

C. PHP

PHP adalah bahasa scripting server-side, bahasa pemrograman yang digunakan untuk mengembangkan situs web statis atau situs web dinamis atai aplikasi web. PHP singkatan dati Hypertext Pre-processor, yang sebelumnya disebut Personal Home Pages.

Script sendiri merupakan sekumpulan intruksi pemrograman yang ditafsirkan pada saat runtime. Sedangkan bahasa sripting adalah bahasa yang menafsirkan skrip saat runtime. Dan biasanya tertanam ke dalam lingkungan perangkat lunak lain.

Karena PHP merupakan scripting server-side maka jenis bahasa pemrograman ini nantinya script atau program tersebut akan dijalankan atau diproses oleh server. Berbeda dengan javascript yang client-side.

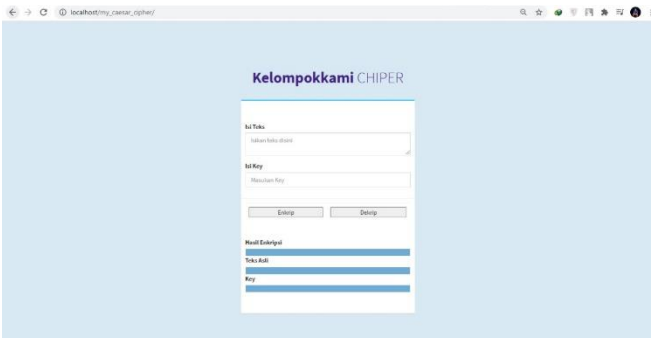
PHP adalah bahasa pemrograman umum yang berarti php dapat disematkan ke dalam kode HTML, atau dapat digunakan dalam kombinasi dengan berbagai sistem template web, sistem manajemen konten webm dan kerangka kerja web.

III. HASIL DAN PENGUJIAN

Berikut adalah gambaran hasil implementasi aplikasi kriptografi caesar cipher dengan php yang telah dibangun.

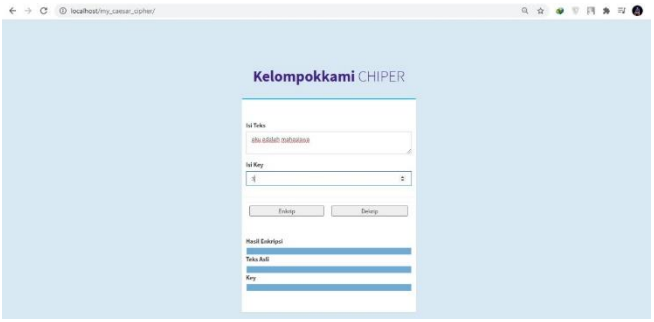
A. Aplikasi kriptografi caesar cipher

Berikut merupakan halaman utama dimana teks yang diinginkan pengirim dimasukan data nya terlebih dahulu untuk mengubah atau enkripsi data



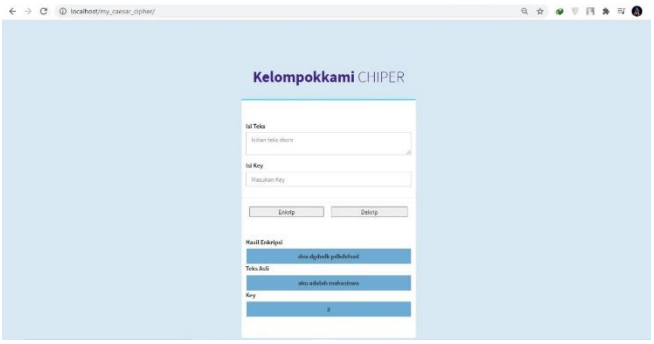
Gambar 3. Tampilan Utama

Setelah pengguna memasuki halaman utama tersebut, selanjutnya pengguna harus memasukan data untuk diubah atau enkripsi agar pihak ketiga tidak mengetahuinya.



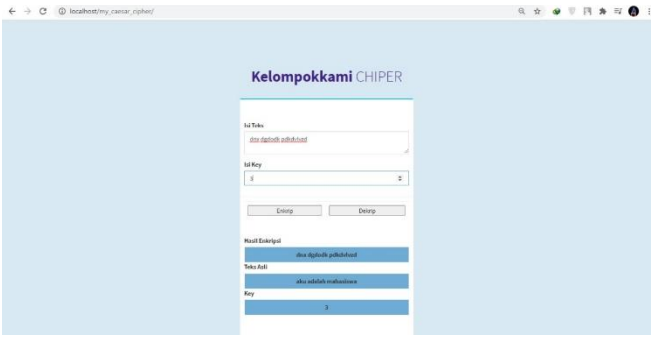
Gambar 4. Memasukan Data Untuk di Enkripsi

Pengguna memasukan data yaitu “aku adalah mahasiswa” yang nanti akan diubah atau enkripsi dengan menggunakan kunci = 3.



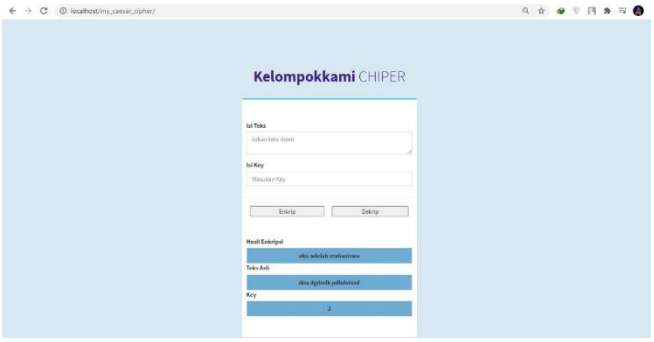
Gambar 5. Proses Enkripsi Data

Gambar diatas merupakan hasil dari proses enkripsi dari data yang pengguna inginkan yaitu “aku adalah mahasiswa”, setelah dienkripsi menjadi “dnx dgdodk pdkdvlvzd”. Hasil enkripsi tersebutlah yang tidak akan diketahui oleh pihak ketiga.



Gambar 6. Data yang akan di Dekripsi

Gambar diatas merupakan data yang akan di dekripsi oleh penerima agar mengetahui data yang telah di enkripsi oleh pengguna, tetapi penerima harus mengetahui kunci yang di digunakan pengguna.



Gambar 7. Hasil Dekripsi Data

Gambar diatas merupakan hasil dari dekripsi data yang telah dilakukan penerima agar mengetahui data yang telah dikirim oleh pengguna.

IV. KESIMPULAN

Berdasarkan hasil aplikasi berbasis Web yang telah dibuat yaitu aplikasi Caesar Cipher memiliki kesimpulan yaitu Aplikasi ini sebagai cara untuk mengimplementasikan kriptografi yaitu caesar cipher. Aplikasi ini dapat digunakan untuk mengubah data atau Enkripsi, Deskripsi informasi agar tidak diketahui oleh pihak ketiga.

Dalam penyelesaian aplikasi ini juga dapat mengetahui sampai manakah kemampuan tentang pengetahuan Caesar Cipher yang telah di pelajari, sehingga mampu diimplementasikan menjadi sebuah aplikasi yang dinamai Caesar Cipher.

REFERENSI

[1] Angriani, H., & Saharaeni, Y. (2019). Implementasi Algoritma Caesar Cipher pada Keamanan Data Sistem e-voting Pemilihan Ketua Organisasi Kemahasiswaan. *Inspiration: Jurnal Teknologi Informasi Dan Komunikasi*, *9*(2), 123. https://doi.org/10.35585/inspir.v9i2.2499

[2] Dwi Putri, Y., Rosihan, R., & Lutfi, S. (2019). Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance. *JIKO (Jurnal Informatika Dan Komputer)*, *2*(2), 87–94. https://doi.org/10.33387/jiko.v2i2.1319

[3] Jurnal, A. (2019). IMPLEMENTASI ALGORITMA CAESAR CIPHER UNTUK KEAMANAN DATA PADA KARTU UJIAN (Studi Kasus : SMK Model Patriot IV Ciawigebang Kab.Kuningan). *Buffer Informatika*, *5*(1), 1–7. https://doi.org/10.25134/buffer.v5i1.1953

[4] Sutoyo, M. N. (2016). Kombinasi Algoritma Kriptografi Caesar Chiper dan. *Mekanova*, *2*(1), 58–66.