IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER MENGGUNKAN PHP

Wisnu Wijaya, Rama Wahyu Husein

Program Studi Teknik Informatika, Universitas Saintek Muhammadiyah
Jl. Raya Klp. Dua Wetan, Ciracas, East Jakarta City, Jakarta 13730
fisawiznuwijaya@gmail.com, ramawahyuhusein17@gmail.com

Abstract– Information security in applications is very important, applications need security systems, because in some companies or even in countries information security is required, and important information that should not be accessed by random recipients of messages must be protected. To protect this information, an algorithm is needed that can cover important messages so that they cannot be read by parties who are not entitled to receive the information. Cryptography is one way that can be used to secure data transmission, the data sent will be converted into a certain code and can only be opened by the recipient who has the key to change the code so that the confidentiality of the message or information can be maintained. continue to be supported, and an application is needed to facilitate data processing, a cryptographic web application can be made and used to facilitate data processing.

Keywords - Cryptography, Vigenere Cipher, Encryption - Decryption, Text.

Abstrak **–** Keamanan informasi dalam aplikasi sangat penting, aplikasi membutuhkan sistem keamanan, karena di beberapa perusahaan atau bahkan di negara diperlukan keamanan informasi, dan informasi penting yang tidak boleh diakses oleh penerima pesan secara acak harus dilindungi. Untuk melindungi informasi tersebut diperlukan suatu algoritma yang dapat menutupi pesan-pesan penting agar tidak dapat dibaca oleh pihak yang tidak berhak menerima informasi. Kriptografi merupakan salah satu cara yang dapat digunakan untuk mengamankan transmisi data, data yang dikirim akan diubah menjadi kode tertentu dan hanya dapat dibuka oleh penerima yang memiliki kunci untuk mengubah kode tersebut sehingga kerahasiaan pesan atau informasi dapat dipertahankan. terus didukung, dan diperlukan aplikasi untuk mempermudah pengolahan data, dapat dibuat aplikasi web kriptografi dan digunakan untuk mempermudah pengolahan data.

Kata Kunci - Kriptografi, Vigenere Cipher, Enkripsi – Dekripsi, Text.

I. PENDAHULUAN

A. Latar Belakang

Keamanan merupakan aspek penting dari data atau informasi. Ketika Anda membutuhkan tingkat keamanan yang tinggi untuk mengirim data atau informasi. Berbagai cara digunakan untuk melindungi sebuah data agar, Salah satu kegiatan untuk melindungi data atau informasi adalah enkripsi. Kriptografi adalah ilmu yang mempelajari tentang keamanan (kerahasiaan) tulisan. Oleh karena itu, untuk melindungi data atau informasi diperlukan suatu metode mampu mengatasi masalah keamanan data. Kriptografi sendiri terbagi menjadi 2 yaitu kriptografi klasik dan kriptografi modern. Secara teknik algoritma kriptografi terdiri dari teknik substitusi dan teknik transposisi[1].[1]

Teknik kriptografi diyakini mampu mengelola masalah keamanan data atau informasi, karena selain menggunakan bahasa pemograman komputer, kriptografi menggunakan rumus-rumus matematika, mulai dari rumus sederhana hingga yang kompleks. Kriptografi memiliki dua konsep utama: enkripsi dan dekripsi. Enkripsi adalah proses pengubahan data atau informasi ke dalam format yang tidak diketahui sebagai informasi awal dengan menggunakan beberapa metode. Sejarah tercatat dalam Romawi bahwa kaisar Julius Caesar menggunakan enkripsi untuk menyampaikan pesan rahasia selama perang. Cipher Vigenre sebenarnya merupakan perpanjangan atau pengembangan dari sebuah sandi Caesar. Caesar cipher menggunakan karakter yang berbeda untuk setiap karakter dalam teks, ada perbedaan tertentu dalam urutan abjad. Misalnya, jika Anda menggeser 4 dengan pada bagian sandi Caesar, maka A menjadi E dan B menjadi F.

Ada berbagai jenis algoritma yang digunakan untuk melindungi data atau informasi. seperti Caesar, Compound Abjad, DES, IDEA, RSA dan sebagainya Sedangkan penelitian ini menggunakan metode Caesar Cipher dengan alfabet majemuk dalam kriptografi. Caesar Cipher merupakan sistem enkripsi berbasis substitusi. Enkripsi dan dekripsi metode Caesar menggunakan operasi pindah. Cara kerja operasi move adalah dengan mengganti huruf dengan huruf alfabet yang ada di kiri atau kanan huruf. Sedangkan compound alphabetic cipher adalah cipher, secara teknis algoritma kriptografi terdiri dari teknik substitusi dan teknik transposisi

Karena Vigenre terdiri dari beberapa Caesar cipher dengan nilai pergeseran berdasarkan arti yang

berbeda, penulis merancang perangkat lunak untuk mempelajari cipher Vigenere. Oleh karena itu, penulis menulis dengan judul "IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER".[2]

B. Batasan Masalah

Adapun batasan masalah penulisan disertasi ini sebagai berikut:

1. Perancangan aplikasi enkripsi ini hanya dapat mengenkripsi dan mendekripsi dalam tulis, bukan audio atau gambar.
2. Membuat aplikasi vigenere cipher berbasis web menggunakan aplikasi XAMPP menggunakan Program HTML dan PHP.

C. Tujuan dan Manfaat Penelitian

Menghasilkan suatu aplikasi yang memiliki suatu fasilitas untuk melindungi data atau menyembunyikan sebuah informasi dan pesan yang menggunak kriptografi vinegere cipher, mengetahui bagaimana cara merancang Program Kriptografi dengan Metode Caesar Chiper.

D. Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dan penulisan peneltian adalah sebagai berikut:

1. Penulis, dapat menambah pemahaman tentang kriptografi khususnya mengenai metode vigenere cipher.
2. Bagi pengguna, untuk meningkatkan pemahaman pengguna tentang kata sandi Vigenere bagi pengguna dan bagi pengguna bisa menyandikan pesan rahasia yang dikirim menggunakan aplikasi ini tanpa takut dibaca oleh orang yang tidak berwenang.

II. LANDASAN TEORI

A. Kriptografi

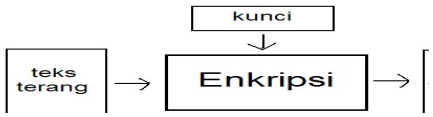
Kriptografi berasal dari bahasa Yunani. Bahasa Yunani merupakan suatu kombinasi atau gabungan dari dua kata cryptos dan graphein. cryptos berarti tersembunyi atau rahasia, dan graphein berarti menulis. Arti dari kriptografi adalah menulis secara rahasia untuk menyampaikan pesan yang perlu dirahasiakan.[3]

Kriptografi menurut (Onno, 2000) adalah bidang ilmu yang mempelajari penggunaan persamaan matematika untuk melakukan proses keamanan data. Kriptografi yang dimaksud adalah untuk melindungi suatu isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak mengetahui isi data. data tersebut diubah menjadi data password yang terlihat berbeda dari data aslinya menggunakan teknik atau algoritma tertentu yang disebut dengan proses enkripsi. Data tersebut akan diubah menjadi data password yang berbeda dengan data aslinya. Mereka yang memenuhi syarat untuk menerima data mengetahui dan memiliki algoritma.[4]

Kriptografi adalah studi tentang bagaimana menjaga keamanan data atau pesan Anda saat dikirim dari pengirim ke penerima tanpa campur tangan pihak ketiga. Menurut buku Bruce Scheiner, Applied Cryptoraphy, Kriptografi dapat menjaga keamanan pesan Anda. Konsep enkripsi sendiri masih sangat sederhana, tetapi telah lama digunakan di Mesir dan Roma. Prinsip yang mendasari Kriptografi sebagai berikut:[5]

- Confidentiality (kerahasiaan), yaitu Memastikan isi pesan terkirim dijaga kerahasiaannya dan tidak diketahui oleh pihak lain (kecuali diizinkan oleh pengirim, penerima/pihak), merupakan layanan yang biasanya dilakukan dengan memodifikasi data untuk membuat algoritma matematika yang bersifat sulit untuk dibaca atau dipahami.
- Integritas data (*data integrity*) adalah layanan yang berhubungan dengan identifikasi. Otentikasi (*Authentication*) pihak-pihak yang terlibat dalam transmisi data dan otentikasi data/informasi asli.
- *Authentication* adalah koneksi dengan kontak. Otentikasi kedua pihak yang terlibat dalam transmisi data dan otentikasi keaslian data.
- *Availability*, yaitu dimana pengguna yang memiliki hak akses atau pengguna yang berwenang memiliki akses terhadap tempat dan waktu serta tidak terikat oleh siapapun
- *Non-Repodiation* anti-denial adalah layanan yang dapat mencegah pihak lain menolak operasi sebelumnya.[6]

Kriptografi sendiri terdiri dari dua bagian utama, yaitu enkripsi dan dekripsi. Seperti dijelaskan di atas, pada sebuah proses enkripsi dapat mengubah plaintext menjadi ciphertext (dengan suatu kunci tertentu), sehingga sangat sulit untuk mengakses informasi isi pesan jika kunci tersebut hanya kita yang mengetahui.



Gambar 1. Proses Enkripsi dan Dekripsi

Peran kunci sangat penting dalam proses enkripsi dan dekripsi (bukan hanya algoritma yang digunakan), sehingga rahasia terungkap, mengungkapkan isi pesan. dan cara melakukan proses kriptografi sebagai berikut:

1. Plaintext adalah data atau informasi asli yang terbuka dalam lingkup enkripsi dan dapat dibaca dan dipahami secara langsung untuk melindungi data tersebut. Menjadi sumber data untuk proses enkripsi.
2. *Key* adalah kata yang digunakan untuk melakukan proses enkripsi dan dekripsi. Kuncinya memiliki dua bagian. Yaitu, kunci privat atau biasa disebut kunci privat (secret), dan kunci publik (open). Keamanan kriptografi tergantung pada perilaku algoritma.
3. Ciphertext adalah hasil teks terenkripsi. Kebalikan dari teks terenkripsi adalah teks biasa, yang merupakan input untuk enkripsi. Proses mengubah plaintext menjadi ciphertext disebut enkripsi. Ini digunakan untuk enkripsi teks, sedangkan kebalikannya disebut dekripsi. Anda tidak bisa hanya membaca teks yang disandikan. Untuk membaca teks terenkripsi, Anda perlu mengetahui kunci dan algoritma yang digunakan untuk mengenkripsi teks. Cara kedua adalah dengan melakukan kriptanalisis. Ini untuk memecahkan kode metode tertentu.
4. Algoritma, yaitu metode melakukan enkripsi dan dekripsi.[7]

Enkripsi adalah pesan asli, yang disebut plaintext diproses dan diubah menjadi kode yang tidak bisa dimengerti.Sebuah cipher atau kode dapat diartikan sebagai enkripsi, seperti yang kita lihat dalam kamus saat ketika kita tidak memahami suatu kalimat atau kata. Berbeda dengan enkripsi, ia menggunakan algoritma yang dapat mengkodekan sebuah data dan mengubah teks asli menjadi format terenkripsi atau kode.

Dekripsi adalah kebalikan dari enkripsi. Pesan atau kalimat yang dapat dienkripsi dan dikembalikan dalam bentuk aslinya menggunakan algoritma yang telah ditentukan.

Algoritma digunakan untuk melakukan proses dekripsi berbeda dengan proses enkripsi, dan algoritma kedua harus mengubah hasil enkripsi menjadi dekripsi. Adapun langkah Proses dasar kriptografi dibagi menjadi dua bagian, yaitu enkripsi dan dekripsi. Dalam Kriptografi Klasik dan Kriptografi Modern, algoritma kriptografi (chiper) berbasis karakter yang disebut enkripsi dan dekripsi dilakukan untuk setiap karakter dalam sebuah pesan. Semua algoritma klasik memiliki sistem kriptografi simetris dan telah digunakan jauh sebelum penemuan kriptografi kunci publik. Kriptografi klasik mengacu pada kriptografi kunci simetris. Pada prinsipnya, algoritma kriptografi klasik dapat dibagi menjadi dua jenis cipher, yaitu:[8]

1. Cipher substitusi (substitution cipher)

   Cipher substitusi, suatu unit pada plainteks digantikan oleh satu unit cipherteks, satu karakter, sepasang karakter, atau sekelompok dua karakter atau lebih.

2. Cipher transposisi (transposition cipher)

   Suatu karakter plaintext dapat diubah secara berurutan, algoritma ini mengubah urutan karakter kedalam teks. Nama lain dari metode ini adalah permutasi atau scrambling. Karena itu mengubah setiap karakter dalam teks yang sama sebagai permutasi karakter. (Munir. 2006).[9]

A. Algoritma Caesar Cipher

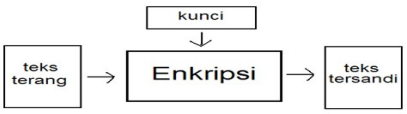
1. Algoritma

Algoritma dalam kriptografi dibagi menjadi dua yaitu algoritma simetris dan algoritma asimetris, berikut adalah pengertian dari algoritma tersebut, yaitu:

Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses dekripsi. Algoritma kriptografi simetris terbagi dalam dua kategori: stream cipher dan block cipher. Dalam algoritma aliran, proses pengkodean berorientasi pada data 1-bit/byte. Dalam algoritma blok, proses pengkodean difokuskan pada pengumpulan bit/byte data (per blok). Contoh algoritma kunci simetris termasuk Data Encryption Standard (DES), Blowfish, Twofish, MARS, International Data Encryption Algorithm (IDEA), 3DES (DES diterapkan tiga kali), dan Advanced Encryption Standard (AES).[10]

Algoritma asimetris adalah menggunakan kunci yang berbeda untuk enkripsi dan dekripsi. Sementara kunci enkripsi dapat didistribusikan secara publik dan disebut sebagai kunci publik, kunci dekripsi disimpan untuk penggunaan pribadi dan disebut sebagai kunci pribadi. Oleh karena itu kriptografi ini disebut juga dengan enkripsi kunci publik, contoh algoritma yang menggunakan kunci asimetris antara lain Riverst Shamir Adleman (RSA) dan Elliptic Curve

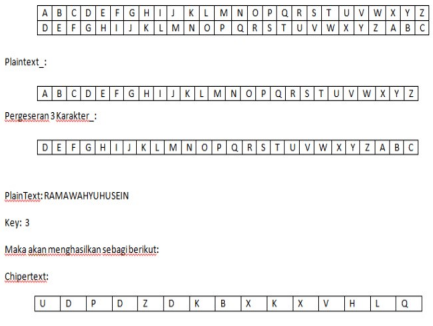
Cryptography (ECC). Dalam kriptografi asimetris, setiap aktor sistem informasi memiliki pasangan kunci, kunci publik dan kunci privat, di mana kunci publik dan kunci privat didistribusikan, kunci publik disimpan untuk diri mereka sendiri. Artinya, untuk R mengirim pesan ke M, R dapat menggunakan kunci publik M untuk menyandikan pesan, dan untuk M membaca surat itu, ia harus mendekripsi isi surat dengan kunci pribadi. Dengan demikian, kedua belah pihak dapat menjamin asal usul surat dan keaslian surat tersebut.[11]



Gambar 2 Proses Enkripsi Dan Dekripsi Algoritma Asimetris

1. Vigenere Cipher

Algoritma kriptografi klasik diperkenalkan abad ke-16 atau sekitar tahun 1986. Algoritma kriptografi ini diterbitkan seseorang diplomat dan kriptolog dari Prancis yaitu Blaise de Vigenere, sebenarnya algoritmanya sudah dijelaskan sebelumnya dalam buku La Chifra del Sigue. Giovan Battista Belaso, sebuah buku tertulis oleh Giovan Battista Belaso pada tahun 1553. Prinsip operasi sandi Vigenere mirip dengan sandi Caesar, yang mengenkripsi plainteks pada pesan dengan menggeser huruf dalam pesan ke nilai kunci dalam urutan abjad.[12]



Gambar 3. Proses Enkripsi pergeseran 3 karakter

Sebagai contoh Caesar cipher pada gambar diatas jika terdapat plainteks: RAMAWAHYUHUSEIN maka jika dienkripsi dengan nilai kunci 3 maka akan menghasilkan Chipertext: UDPDZDKBXKXVHLQ

Dari cipherteks yang didapat kita akan lihat bahwa huruf R dienkripsi menjadi U, huruf A dienkripsi menjadi huruf D, dan seterusnya dimana huruf pada pesan digeser sejauh nilai kunci.

]Algoritma Caesar cipher sangat sederhana, sehingga sangat beresiko di pecahkan, karena hanya satu huruf dari plaintext yang dibutuhkan untuk menentukan kunci yang akan digunakan. Cipher Vigenere, yang menggunakan metode substitusi alfabet, tidak memiliki masalah ini karena setiap huruf dalam pesan yang dienkripsi dengan sandi Vigenere ini akan digeser dengan nilai yang berbeda tergantung pada kunci yang diberikan. Kunci yang digunakan pada sandi vigenere berbeda dengan kunci yang digunakan pada sandi Caesar. Jika pada sandi Caesar kuncinya hanya satu nilai, maka pada sandi Vigenere kunci tersebut berupa rangkaian huruf. Suatu kunci yang dapat diuntaikan kata untuk mengenkripsi suatu huruf dari plaintext dengan kunci yang berbeda. Pada panjang kunci yang digunakan lebih pendek dari panjang plainteks, maka kunci akan mengulang sampai suatu panjang kunci sama panjang plainteks. Algoritma ini meminimalkan kemungkinan pemecahan ciphertext jika satu huruf dari plaintext diketahui. Suatu proses enkripsi secara matematis yang dapat digunakan operasi modul dengan cara mengubah huruf menjadi angka, misalanya A = 0, B = 1 sampai dengan Z = 25. Setelah itu, prosesnya sama seperti pada Caesar cipher dimana setiap huruf pada plainteks akan digeser sejauh nilai kunci pada posisinya yang sesuai. Pergeseran huruf-huruf tersebut dapat Dipetakan dalam bentuk pemetaan tabel 26x26 antar karakter huruf pada plaintext dan huruf-huruf pada kunci.

Gambar 2 Tabel *Vigenere Cipher*

Algoritma ini akan meminimalkan kemungkinan pecahnya ciphertext jika diketahui satu huruf plaintext. Model matematis enkripsi pada algoritma cipher *Vigenere* adalah sebagai berikut: Sebuah sandi (E_n) "huruf" x dengan digeser n ditulis secara matematis.

$$E_n(x) = (x + n) \mod 26.$$

Sedangkan suatu pemerosesan dalam pemecahan kode dekripsi, menjadi hasil dekripsi (D_n) adalah Dimana:

$$D_n(x) = (x - n) \mod 26.$$

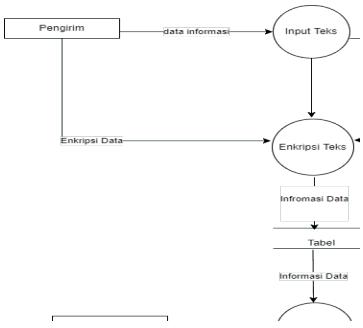
Pada setiap huruf yang sama diganti dengan huruf yang sama di semua pesan, itulah sebabnya sandi Caesar dapat diklasifikasikan substitusi monoalfabetic, sebagai lawannya adalah substitusi polialfabetik.

B. PHP

[14]PHP atau Hypertext Preprocessor adalah salah satu bahasa pemrograman open source yang sangat cocok atau dikhususkan untuk pengembangan web dan dapat ditanamkan pada sebuah script HTML. Bahasa PHP bisa Dikatakan untuk menggambarkan beberapa bahasa pemrograman seperti c, java dan perl yang mudah dipelajari. php adalah pemrosesan data di server, akan menerjemahkan script program, hasilnya akan dikirim ke pelanggan yang membuat permintaan. Pengertian lain dari PHP adalah singkatan dari Hypertext Preprocessor, yang merupakan bahasa pemrograman berbasis kode (script) yang digunakan untuk memproses data dan mengirimkannya ke web browser dalam bentuk kode HTML". Menurut Kustiyaningsih (2011: 114), "PHP (atau secara resmi PHP: Hypertext Preprocessor) adalah skript siserver yang ditambahkan ke HTML". Sistem kerja dari PHP diawali dengan permintaan yang beasal dari halaman website oleh browser. Berdasarkan URL atau alamat situs web di Internet, browser akan mencari alamat dari server web, mengidentifikasi halaman yang benar, dan meneruskan semua informasi yang dibutuhkan oleh server web. Jika file tidak berisi script PHP maka request pengguna akan langsung ditampilkan di browser, namun jika file berisi script PHP maka proses akan dilanjutkan di modul PHP sebagai mekanisme yang menerjemahkan script. PHP dan mengolah script tersebut sehingga dapat diubah menjadi kode html lalu ditampilkan ke browser user.

III.HASIL DAN PEMBAHASAN

1. Perancangan Sistem



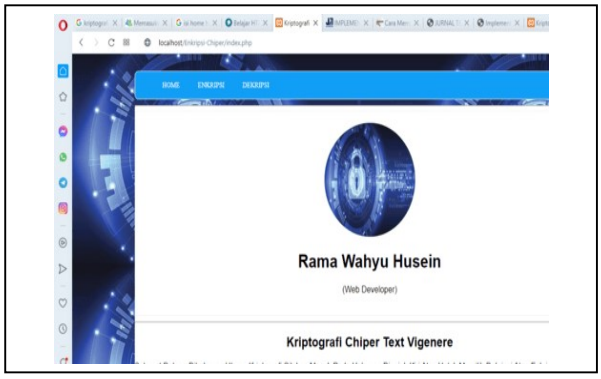
Gambar 4 DFD

Tunjukkan gambar sistem umum. Dimana didalam sistem ada tiga proses yaitu enkripsi data, enkripsi dan input teks. Pada gambar diatas proses dalam sistem diawali dengan pemasukan data yang harus dirahasiakan (enkripsi). Setelah memasukkan data atau informasi selesai, maka dilakukan proses enkripsi. Data atau informasi yang dihasilkan dari enkripsi tersebut kemudian dikirim ke penerima. Setelah penerima menerima data atau informasi, data atau informasi yang dikirim didekripsikan maka akan tau jenis teks tersebut berisi pesan apa yang dapat kita baca jika proses masih dalam bentuk enkripsi maka kita tidak dapat membacanya dengan jelas.

2. Implementasi Sistem dan Hasil

Pada penelitian ini dibuat sebuah aplikasi kriptografi dengan menggunakan metode Caesar cipher vigenere yang didalam tahap pembuatan aplikasi berbasis web tersebut.

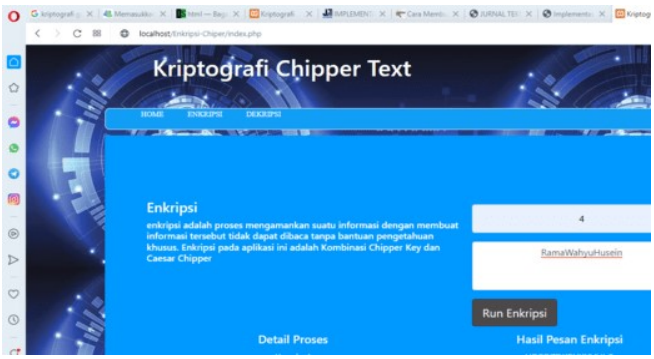
1. Halaman Utama



Gambar 5 Halaman Utama

Halaman utama ini berisi menu-menu enkripsi dan dekripsi yang dapat dipilih oleh pengguna. Halaman utama dari aplikasi kriptografi chipper.

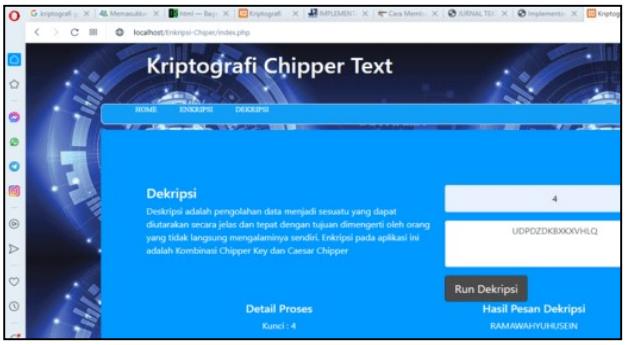
2. Halaman Enkripsi



Gambar 6 Enkripsi Teks

Pada halaman ini, pengguna dapat memasukkan data dan melakukan proses enkripsi teks. Pada halaman aplikasi web enkripsi.

3. Halaman Dekripsi



Gambar 7 Dekripsi

Pada halaman ini, pengguna dapat memasukkan teks atau data yang terenkripsi untuk melakukan proses dekripsi teks. Pada halaman aplikasi web.

IV. KESIMPULAN

Berdasarkan hasil aplikasi enkripsi menggunakan caesar cipher maka bisa diambil kesimpulan bahwa perhitungan matematis Caesar cipher dapat dilakukan dengan menggunakan kata kunci dan plaintext, bahwa dengan tidak adanya rumus pasti dalam metode kriptografi Caesar Ciper, maka dapat dikatakan bahwa Caesar Cipher sulit untuk dipecahkan. Enkripsi sangat penting dalam pengiriman pesan, apalagi pesannya sangat rahasia. Pada keamanan aplikasi menggunakan metode Vigenere Cipher yang memiliki kunci dan pesan khusus yang telah ditentukan sebelumnya.

DAFTAR PUSTAKA

[1] A. Pradipta and S. A. Yogyakarta, "Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi," *ijns.org Indones. J. Netw. Secur.*, vol. 5, p. 3, 2016.

[2] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher Dengan Php," *J. Teknol. Inf.*, vol. 1, no. 1, p. 11, 2017, doi: 10.36294/jurti.v1i1.21.

[3] N. Aziz, "Perancangan Aplikasi Enkripsi Deskripsi Menggunakan Metode Caesar Shiper dan Operasi XOR," *Ikraith-Informatika*, vol. 2(2), no. 1, pp. 72–80, 2018.

[4] R. Lingkup, K. Untuk, and M. Data, "Ruang Lingkup Kriptografi," vol. IX, no. 2, 2004.

[5] E. Juliansyah, M. T. Informatika, I. Pendahuluan, and R. L. Rivest, "Implementasi Algoritma Kriptografi Rc-6 Dalam," vol. 16, no. 02, pp. 267–269, 2017.

[6] Jumiran and F. Aminul, "Penyisipan text pada gambar menggunakan steganografi," *J. IPSIKOM*, vol. 2, no. 1, pp. 1–12, 2014.

[7] A. P. Aplikasi, "APLIKASI KRIPTOGRAFI PESAN MENGGUNAKAN ALGORITMA," vol. 10, no. 2, pp. 120–128, 2014.

[8] D. Bayu Gumelar *et al.*, "SKANIKA VOLUME 1 NO. 2 MEI 2018_____ 711 Implementasi Algoritma Kriptografi dengan Algoritma Caesar Cipher, Advanced Encryption Standard 256, Dan Rc6 untuk Aplikasi Chatting Berbasis Android," vol. 1, no. 2, pp. 711–717.

[9] Y. Permanasari, "Kriptografi Klasik Monoalphabetic," *Matematika*, vol. 16, no. 1, pp. 7–10, 2017, doi: 10.29313/jmtm.v16i1.2543.

[10] I. M. Arrijal, R. Efendi, and B. Susilo, "Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks," *Pseudocode*, vol. 3, no. 1, pp. 69–82, 2016, doi: 10.33369/pseudocode.3.1.69-82.

[11] J. T. Informatika, F. Sains, and D. A. N. Teknologi, "Implementasi Kombinasi Algoritma Asimetris Rivest Shamir Adleman Dan Algoritma Simetris Advanced Encryption Standard Pada Aplikasi Pesan Singkat," 2017.

[12] S. Nasional, T. Informatika, P. G. Medan, I. Pendahuluan, and A. L. Belakang, "Rancang Bangun Kombinasi Chaisar Cipher dan Vigenere Cipher Dalam Pengembangan Algoritma Kriptografi Klasik," pp. 234–243, 2017.

[13] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.

[14] A. Firman, H. F. Wowor, X. Najoan, J. Teknik, E. Fakultas, and T. Unsrat, "Sistem Informasi Perpustakaan Online Berbasis Web," vol. 5, no. 2, 2016.