**APLIKASI KRIPTOGRAFI MENGGUNAKAN VIGENERE CHIPER PADA DATA ORANG YANG MEMPUNYAI KEBUTUHAN KHUSUS DINAS PEMBERDAYAAN PEREMPUAN DAN PERLINDUNGAN ANAK**

**KABUPATEN MUSI RAWAS**

**Fitriana Lestari 1, Zulfauzi 2, Cindi Wulandari 3**

1,2Program Studi Informatika, Universitas Bina Insan, LubukLinggau, Indonesia

3Program Studi Sistem Informasi, Universitas Bina Insan, LubukLinggau, Indonesia

**Email:** 1fitrian\_lestari@univbinainsan.ac.id, 2zulfauzi@univbinainsan.ac.id, 3cindi\_wulandari@univbinainsan.ac.id

**Abstrak**

Masalah dalam penelitian ini adalah bagaimana untuk membuat serta merancang aplikasi kriptografi menggunakan vigenere chiper pada data orang yang mempunyai kebutuhan khusus di dinas pppa kabupaten musi rawas, dalam penelitian ini penulis menggunakan algoritma kriptografi vigenere chiper pad aplikasi yang digunakan untuk mendata kasus-kasus kekerasan yang terjadi pada perempuan dan anak secara online. Algoritma Kriptografi ini digunakan untuk mengamankan pertukaran data dan informasi yang terjadi didatabase. Hasil dari penelitian ini adalah sebuah aplikasi yang dapat digunakan untuk mendata kasus-kasus kekerasan yang terjadi pada perempuan dan anak secara online dan dilengakapin dengan algoritma kriptografi vigenere chiper. Kesimpulan dari penelitian ini adalah dengan adanya aplikasi ini dapat membantu pihak Dinas dalam mendata kasus kekerasan anak dan perempuan serta mempercepat dan mengefisiensikan proses pendataan serta pelaporan data kekerasan anak dan perempuan

**Kata Kunci :** Algoritma Kriptografi; Vigenere Chiper; Kekerasan; Waterfall.

***Abstract***

*The problem in this study is how to create and design a cryptographic application using the vigenere cipher on the data of people with special needs at the PPPA office of the Musi Rawas district, in this study the author uses the cryptographic algorithm vigenere cipher pad application that is used to record cases of violence that occur on women and children online. This Cryptographic Algorithm is used to secure the exchange of data and information that occurs in the database. The result of this study is an application that can be used to record cases of violence that occur to women and children online and is equipped with a cryptographic algorithm vigenere cipher. The conclusion of this research is that this application can help the Office in recording cases of violence against children and women as well as speed up and streamline the process of collecting data and reporting data on violence against children and women.*

***Keywords****: Cryptographic Algorithm; Vigenere Cipher; Violence; Waterfall*

# PENDAHULUAN

Pada zaman saat ini perkembangan dan pertukaran informasi menggunakan internet telah mengalami kemajuan yang sangat pesat dalam berkomunikasi seperti mengirim dan menerima data ataupun pesan, bermacam macam media seperti email, dokumen, maupun berkas pribadi tanpa memperhitungkan jarak dan waktu. Penggunaan interkonektivitas sudah menjadi kebutuhan sekunder yang sangat mendasar,karena hampir semua media yang digunakan untuk bertukar informasi sudah menggunakan interkonektivitas jaringan internet. Namun dalam pertukaran informasi tersebut terdapat beberapa aspek keamanan yang memegang peranan penting agar terhindar dari pencurian data maupun informasi oleh pihak-pihak yang tidak diinginkan [1].

Keamanan dan kerahasian pertukaran informasi sseperti database merupakan salah satu aspek penting dari sebuah pertukaran informasi. Hal tersebut terkait bagaiaman informasi tersebut dapat tersampaikan oleh pihak tertentu dan tidak dapat juga diakses oleh pihak yang tidak berhak. Oleh karena itu sangat penting untuk mencegah jatuhnya informasi kepada pihak-pihak lain yang tidak berkepentingan [2].

Prosedur dalam menjaga keamanan serta kerahasiaan data dapat dilakukan dengan menerapkan algoritma kriptografi. Algoritma kriptografi merupakan ilmu

yang mempelajari teknik-teknik matematika yang beruhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi data [3].

Didalam algoritma kriptografi itu sendiri dilakukan dengan dua proses yaitu proses enskripsi data dan proses deskripsi data. Enkripsi merupakan suatu proses untuk menyandikan sebuah pesan asli menjadi pesan yang tersandi, sedangkan deskripsi merupakan proses untuk mengembalikan pesan yang tersandi menjadi pesan asli [3].

Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Musi Rawas merupakan dinas yang mempunyai tujuan untuk melindungi serta memberikan hak-hak kepada perempuan dan anak. Adapun tujuan dari penelitian ini adalah untuk mendata orang yang mempunyai kebutuhan khusus di Dinas Pemberdayaan Perempuan Dan Perlindungan Anak Kabupaten Musi Rawas. Kebutuhan khusus disini adalah sebuah kebutuhan akan perlindungan khusus untuk perempuan dan anak dalam memenuhi serta memberikan perlindungan terhadap hak-hak nya, mengingat maraknya kasus kekerasan pada perempuan dan anak khusus nya di Kabupaten Musi Rawas masih sangat lah tinggi. Kekerasan pada perempuan dan anak dapat terjadi karena kurangnya kontrol dan pengawasan dari pihak pemerintah maupun lingkungan sekitar akan kepedulian terhadap anak anak dan perempuan yang mengalami kasus kekerasan, baik itu kekerasan fisik, maupun kekerasan secara emosional/psikologis.

Saat ini di Dinas Pemberdayaan Perempuan dan Perlindungan Anak Kabupaten Musi Rawas sudah mempunyai sebuah aplikasi yang digunakan untuk mendata anak anak dan perempuan yang mengalami kekerasan baik itu fisik maupun emosional/psikologis. Aplikasi tersebut adalah SIMFONI PPA (Sistem Informasi Online Perlindungan Perempuan dan Anak), namun penggunaan aplikasi ini hanya dilakukan oleh pihak dinas PPA Kabupaten Musi Rawas dan belum dapat digunakan secara luas untuk mayarakat umum. Proses pendataan kasus kekerasan dilakukan dengan cara menginputkan data yang ada kedalam aplikasi tersebut, data tersebut didapatkan dari laporan secara langsung masyarakat ke Dinas PPPA Kabupaten Musi Rawas maupun didapatkan dari berita yang ada.

Maka dari itu tujuan dari penelitian ini adalah untuk membuat sebuah aplikasi yang dapat digunakan untuk mendata kasus-kasus kekerasan yang terjadi pada perempuan dan anak secara online. Aplikasi ini nantinya akan ditambahkan sebuah algoritma kriptografi yang digunakan untuk mengamankan pertukaran data dan informasi yang terjadi didatabase. Algorimta kriptografi yang digunakan dalam penelitian ini adalah Vigenere Chiper. Vigenere chiper merupakan algoritma kriptografi yang menyandikan teks alfabet dengan menggunakan deretan sandi caesar berdasarkan huruf-huruf pada kata kunci [4].

## METODOLOGI PENELITIAN

## Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan adalah metode air terjun (*waterfall*). Metode air terjun (*waterfall*), sering juga disebut metode sekuensial linier (*sequential linier*) atau alur hidup klasik (*classic life*), menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau terurut dimulai dari analisis, desain pengodean, pengujian dan tahap pendukung (*support*) .

|  |
| --- |
| Pegujian  Pengodean  Desain  Analisis |

1. Metode Air Terjun (*waterfall*)

Adapun tahapan pengembangan air terjun (*waterfall*) ini terdiri dari beberapa aktifitas yang tentunya sesuai dengan tahapan yang telah dijabarkan pada alur proses pengembangan sistem. Tahapan tersebut yaitu :

1. **Analisis kebutuhan perangkat lunak**

Proses pengumpulan kebutuhan dilakukan secara interaktif untuk menspesifikasikan kebutuhan perangkat lunak agar dapat dipahami perangkat lunak seperti yang dibutuhkan oleh *user*. Spesifikasi kebutuhan perangkat lunak pada tahap ini perlu untuk didokumentasikan.

1. ***Desain***

Desain perangkat lunak adalah proses multi langkah yang fokus pada desain pembuatan program perangkat lunak termasuk struktur data , arsitektur perangkat lunak, representasi antar muka, dan prosedur pengodean.

1. **Pembuatan kode program**

Desain harus dituangkan kedalam program perangkat lunak. Hasil dari tahap ini adalah program komputer sesuai dengan desain yang telah dibuat pada tahap desain.

1. **Pengujian**

Pengujian fokus pada perangkat lunak dari segi lojik, fungsional, dan memastikan semua bagian telah diuji. Hal ini dilakukan untuk meminimalisir kesalahan (*error*) dan memastikan keluaran yang dihasilkan sesuai yang diinginkan.

## Proses Enskripsi dan Deskripsi Agortima Kriptografi Vigenere Chiper

Sandi Vigenère merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi. Setiap huruf teks terang digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi Caesar dengan geseran 3, A menjadi D, B menjadi E and dan seterusnya. Sandi Vigenère terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda [7].

Model matematika dari enkripsi pada algorotma *Vigenere cipher* ini adalah seperti berikut :

Ci = Ek (Mi) = (Mi + Ki) mod 26

Dan model matematika untuk deskripsi adalah :

Mi = Dk (Ci) = (Ci – Ki) mod 26

Keterangan :

C : cipherteks

M : Plainteks

K : Kunci

Sebagai contoh perhitungan manual yang akan penulis lakukan dalam implementasi Algortima Kriptografi Vigenere Chiper penulis mencotohkan penggunan pada tabel pengguna pada database di dalam aplikasi ini dilihat pada tabel 14 dibawah ini. Dari setiap field yang ada nantinya setiap data yang tersimpan pada tabel pengguna akan dilakukan enskripsi dan deskripsi

1. Pesan Asli

|  |  |  |
| --- | --- | --- |
| **No** | ***Field*** | **Pesan Asli / Plaintext** |
| 1 | id\_Pengguna | 1 |
| 2 | nama\_Pengguna | fitri |

Pada tabel 3. 8 diatas penulis menggunakan kunci huruf infor, maka proses enskripsi nya adalah sebagai berikut :

Model Matematika Enskripsi :

**Ci = Ek (Mi) = (Mi + Ki) mod 26**

Nama Pengguna

C1 = ( f + i ) Mod 26

C1 = (5 + 8) Mod 26

C1 = (13) Mod 26

C1 = n

C2 = (i + n) Mod 26

C2 = (8 + 13) Mod 26

C2 = (21) Mod 26

C2 = v

C3 = (t + f) Mod 26

C3 = (19 + 5) Mod 26

C3 = (24) Mod 26

C3 = y

C4 = (r + o) Mod 26

C4 = (17 + 14 ) Mod 26

C4 = (31 – 26 )

C4 = 5

C4 = f

C5 = (i + r) Mod 26

C5 = (8 + 17) Mod 26

C5 = (25) Mod 26

C5 = z

1. Pesan Tersandi

|  |  |  |
| --- | --- | --- |
| **No** | ***Field*** | **Pesan Tersandi / Chipertext** |
| 1 | id\_ Pengguna | 1 |
| 2 | nama\_pasien | nvyfz |

Sedangkan Model Matematika Deskripsi adalah sebagai berikut :

**Mi = Dk (Ci) = (Ci – Ki) mod 26**

Nama Pengguna

M1 = (n -i) Mod 26

M1 = (13 – 8) Mod 26

M1 = (5) Mod 26

M1 = f

M2 = (v -n) Mod 26

M2 = (21 – 13) Mod 26

M2 = (8) Mod 26

M2 = i

M3 = (y -f) Mod 26

M3 = (24 – 5) Mod 26

M3 = (19) Mod 26

M3 = t

M4 = (f - o) Mod 26

M4 = (5 -14) Mod 26

M4 = (17) Mod 26

M4 = r

M5 = (z - r) Mod 26

M5 = (25 -17) Mod 26

M5 = (8) Mod 26

M5 = i

## HASIL DAN PEMBAHASAN

Dari perancangan sistem yang ada, dihasilkan sebuah aplikasi kriptografi menggunakan vigenere chiper pada data orang yang mempunyai kebutuhan khusus di dinas pemberdayaan perempuan dan perlindungan anak Kabupaten Musi Rawas.

Didalam sistem tersebut terdapat beberapa menu diantaranya yaitu :

1. Halaman *Login* User dan admin, sebagai tampilan awal pada saat user membuka halaman awal system



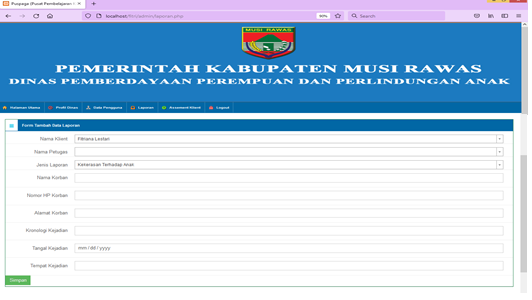
1. Halaman *Login* User
2. Halaman Awal Sistem untuk Admin dan pengguna atau masyarakat, halaman akan tampil setelah admin berhasil melakukan *login* yang befungsi untuk admin melakukan pengolahan data system



1. Tampilan Halaman Awal Sistem Untuk Admin dan Masyarakat
2. Halaman Input Data Pengguna, halaman ini dapat digunakan oleh admin untuk menambahkan data pengguna baik masyarakat maupun admin dan akan masuk ke d*atabase* sistem.



1. Halaman Input Data Pengguna
2. Halaman Laporan, halaman ini dapat digunakan oleh admin ataupun masyatakat untuk membuat laporan data kekerasan terhadap perempuan dan anak di Kabupaten Musi Rawas dan akan masuk kedatabase sistem.



1. Halaman Laporan
2. Halamn Assement Klient, halaman ini dapat digunakan oleh admin untuk melakukan assesment klient langsung kelapangan untuk mengecek kondisi korban secara langsung.



1. Halaamn Assement Klient

# KESIMPULAN

Dari hasil pembasahan tentang aplikasi yang telah dibangun. Maka dapat ditarik kesimpulan yaitu :

1. Dengan adanya aplikasi ini dapat membantu pihak Dinas dalam mendata kasus kekerasan anak dan perempuan
2. Mempercepat dan mengefisiensikan proses pendataan serta pelaporan data kekerasan anak dan perempuan
3. Dapat menjaga kemanan data pada database karena dalam pengamanan databasenya menggunakan algoritma kriptografi Vigenere Chiper.

# DAFTAR PUSTAKA

[1] N. Y. Setyawati, A. N. Khofid, A. U. . Rundi, and V. Wati, “Modifikasi Kriptografi Klasik Kombinasi Metode Vigenere Cipher dan Caesar Cipher,” *J. Smart Syst.*, vol. 1, no. 1, pp. 1–8, 2021, doi: 10.36728/jss.v1i1.1601.

[2] V. C. Hardita and E. W. Sholeha, “Penerapan Kombinasi Metode Vigenere Cipher, Caesar Cipher Dan Simbol Baca Dalam Mengamankan Pesan,” *J. SAINTEKOM*, vol. 11, no. 1, pp. 34–43, 2021, doi: 10.33020/saintekom.v11i1.202.

[3] S. S. Informasi, F. Teknik, U. Pamulang, J. P. No, and K. Tangerang, “IMPLEMENTASI ALGORITMA VIGENERE CHIPER DAN LEAST SIGNIFICANT BIT ( LSB ) UNTUK MENYEMBUNYIKAN,” vol. XVI, no. 2, pp. 42–53.

[4] M. I. Afand and Nurhayati, “Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android,” *30. IT J.*, vol. 8, no. 1, pp. 2252–746, 2020.

[5] M. Siregar, H. F., Siregar, Y. H., & Melani, “Perancangan Aplikasi Komik Hadist Berbasis Multimedia Helmi,” *JurTI (Jurnal Teknol. Informasi),* vol. 2, no. 2, pp. 113–121, 2018.

[6] M. S. Novendri, A. Saputra, and C. E. Firman, “Aplikasi Inventaris Barang Pada MTS Nurul Islam Dumai Menggunakan PHP Dan MySQL,” *Lentera Dumai*, vol. 10, no. 2, pp. 46–57, 2019.

[7] N. Laila and A. S. R. Sinaga, “Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra,” *Sci. Comput. Sci. Informatics J.*, vol. 1, no. 2, p. 47, 2019, doi: 10.22487/j26204118.2018.v1.i2.11221.

[8] N. Azis, “Perancangan Aplikasi Enkripsi Dekripsi Menggunakan Metode Caesar Chiper dan Operasi XOR,” *Ikraith-Informatika*, vol. 2, no. 1, pp. 72–80, 2018.

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

[10] Marlina, Masnur, and M. Dirga.F, “Aplikasi E-Learning Siswa Smk Berbasis Web,” *J. SINTAKS Log. Vol.*, vol. 1, no. 1, pp. 2775–412, 2021.

[11] J. Karman and A. Nurhasan, “Perancangan Sistem Keamanan Data Inventory Barang Di Toko Nanda Berbasis Web Menggunakan Metode Kriptografi Vigenere Cipher,” *J. Teknol. Inf. MURA*, vol. 11, no. 1, pp. 29–36, 2019, doi: 10.32767/jti.v11i1.451.

[12] A. Z. Hasibuan, M. S. Asih, and H. Harahap, “Penerapan QR Code dan Vigenere Cipher Dalam Sistem Pelaporan Juru Parkir Ilegal,” *J. Sist. Inf.*, vol. 5341, no. April, pp. 2579–5341, 2019.

[13] D. R. P. Hafiz Benizar, “RANCANG BANGUN SISTEM INFORMASI LAPORAN PENGAWASAN PROYEK BERBASIS WEB PADA PT.HUTAN ALAM,” *J. Manaj. Inform.*, vol. 7, no. 1, pp. 11–20, 2017.

[14] M. T. Ely Rosely, Ir., M.B.S. Supriadi, Rd. Yayuana Sabrina Asniar, S.T., “Aplikasi Pengelolaan Pelelangan Jasa Konstruksi Bangunan di Kantor Zidam III Siliwangi,” *J. Teknol. Inf.*, vol. 2, no. 2, pp. 45–50, 2015.

[15] R. R. Widagdo and M. S. A.K.T Dundu, “PERANCANGAN SISTEM INFORMASI MANAJEMEN BERBASIS WEBSITE DALAM PROYEK KONSTRUKSI (STUDI KASUS : PEMBANGUNAN KANTOR MAKODAM 13 MERDEKA DI MANADO),” *J. Sipil Statik*, vol. 3, no. 11, pp. 767–774, 2015.

[16] A. . Rosa and M. Shalahuddin, *Rekayasa Perangkat Lunak Terstruktur dan berorientasi Objek*. Bandung: Informatika, 2018.