

## **IMPLEMENTASI ROT 13 DAN VIGENERE CIPHER UNTUK PENGAMANAN PESAN BERBASIS WEB**

**Rizkiyatul Zakiyah<sup>1</sup>, Muhlis Tahir<sup>2</sup>, Susi Muslimah<sup>3</sup>, Tsasya Salsabila<sup>4</sup>, Edi Purwanto<sup>5</sup>, Sri Yuliani Susanti<sup>6</sup>**

[rizkiyatulzakiyah8@gmail.com](mailto:rizkiyatulzakiyah8@gmail.com) [muhlis.tahir@trunojoyo.ac.id](mailto:muhlis.tahir@trunojoyo.ac.id)  
[susimuslimah.ss550@gmail.com](mailto:susimuslimah.ss550@gmail.com) [tsasyasalsabila02@gmail.com](mailto:tsasyasalsabila02@gmail.com)  
[edipurwanto250920@gmail.com](mailto:edipurwanto250920@gmail.com) [susantiputri234@gmail.com](mailto:susantiputri234@gmail.com)

**Fakultas Ilmu Pendidikan, Universitas Trunojoyo Madura, Bangkalan**

### **Abstrak**

Keamanan merupakan hal yang harus diperhatikan saat masuk ke sosial media, ataupun aplikasi yang dianggap privasi oleh pengguna, karena semakin berkembangnya zaman, maka semakin canggih teknologi. Dengan berkembangnya teknologi, semakin banyak pula celah kejahatan yang muncul terutama pada aplikasi chatting. Oleh sebab itu keamanan dalam sistem harus mendapatkan perhatian lebih, sehingga dibutuhkan suatu pengamanan pesan yang dilakukan dengan teknik kriptografi untuk melindungi para pengguna dari serangan peretas. Teknik kriptografi bekerja dengan cara mengenkripsikan pesan asli (*plaintext*) menjadi teks yang susah dipahami (*ciphertext*) atau tidak mengandung makna. Adapun algoritma yang digunakan dalam pengenkripsian yaitu Rot 13 dan Vigenere Cipher, sebagai teknik kriptografi pengkodean username dan password agar username dan password terlihat sulit dibaca dan dipecahkan. Setelah username dan password yang telah dienkrpsi maka algoritma ini akan menyisipkan huruf rahasia.

**Kata Kunci:** *Keamanan, Vigenere Cipher, Rot 13, Kriptografi.*

**Abstract**

Security is something that must be considered when entering social media, or applications that are considered private by users, because as time goes by, the technology becomes more sophisticated. With the development of technology, more and more crime loopholes have emerged, especially in chat applications. Therefore security in the system must receive more attention, so that a message security is needed that is carried out with cryptographic techniques to protect users from hacker attacks. Cryptographic techniques work by encrypting the original message (plaintext) into text that is difficult to understand (ciphertext) or has no meaning. The algorithms used in encryption are Rot 13 and Vigenere Cipher, as cryptographic techniques for encoding usernames and passwords so that usernames and passwords look difficult to read and crack. After the username and password have been encrypted, this algorithm will insert secret letters.

**Keywords:** Security, Vigenere Cipher, Rot 13, Cryptography.

## Pendahuluan

Komunikasi merupakan suatu kegiatan dasar dalam kehidupan manusia, yang memungkinkan manusia dapat bertukar informasi dengan manusia lainnya. Informasi tersebut selanjutnya dapat di olah menjadi informasi baru yang berguna bagi manusia itu sendiri dan orang lain. Pada masa sekarang ini manusia sudah menemukan banyak alat yang dapat digunakan untuk berkomunikasi satu sama lain tanpa mengkhawatirkan jarak yang memisahkan. Kehidupan manusia sekarang ini sudah sangat dimudahkan oleh alat-alat canggih, namun bukan berarti hal tersebut tidak memiliki kekurangan. Informasi pada alat-alat komunikasi tersebut dapat dengan mudah dilihat oleh orang lain, baik penyedia layanan atau orang-orang yang berniat mendapatkan informasi untuk keperluan mereka sendiri atau biasa disebut hacker (Aditya Permana, 2018).

Ketika *login* (masuk) pengguna harus menjaga kerahasiaan *password* atau kata sandi agar tidak mudah dibaca oleh sniffer diperlukan suatu proses pengamanan dengan melakukan enkripsi di bagian login, regist, serta nama pengguna (user) sebelum data di simpan ke dalam database sistem agar tidak dapat dibaca oleh orang yang tidak berhak (Aditya, et al., 2023).

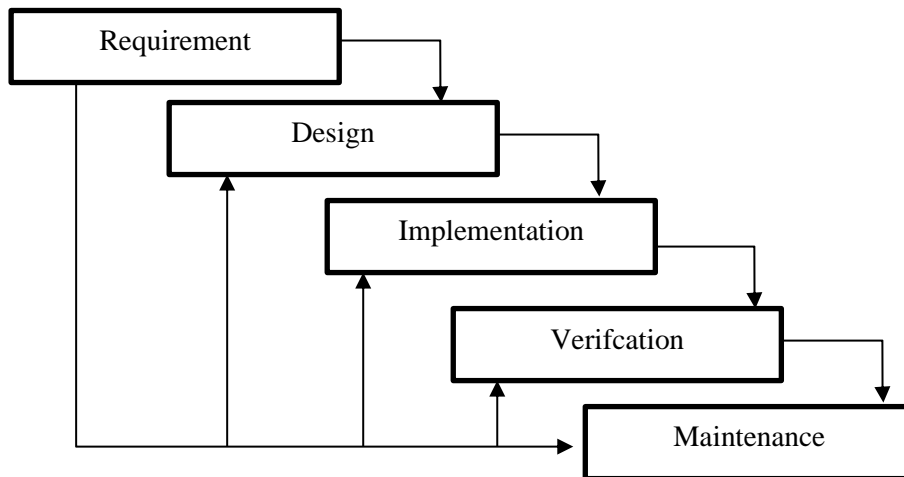
Kriptografi memiliki dua konsep yang penting, yaitu enkripsi dan dekripsi. Enkripsi mengubah informasi atau data menjadi bentuk yang hampir tidak dikenali seperti informasi awal menggunakan algoritma tertentu, sedangkan dekripsi mengubah bentuk tersamar tersebut menjadi informasi awal. Salah satu metode yang dapat dilakukan adalah metode Vigenere Cipher. Metode Vigenere Cipher menyembunyikan pesan berupa teks melalui teknik substitusi dengan mengubah setiap huruf menjadi huruf lain berdasarkan kunci yang digunakan. Metode ini dapat mengubah pesan menggunakan kombinasi 26 huruf alfabet dan memerlukan waktu cukup lama untuk memecahkan algoritma tersebut, sehingga keamanan pesan dapat terjaga (Aditya Permana, 2018).

Rot 13 merupakan enkripsi cipher yang biasa digunakan untuk sistem informasi *UNIX* yang banyak terdapat pada forum *online* yang bermanfaat untuk perlindungan. Sistem pergeseran dari metode Rot 13 dengan menggeser maju sebanyak 13 karakter. Untuk deskripsi Rot 13 dengan menggeser sebanyak 13 karakter (Jtik, et al., 2023).

## Metode

Peningkatan sistem dapat berupa membuat suatu sistem yang baru dan menggantikan sistem yang lama secara keseluruhan atau memperbaiki sistem yang telah ada sebelumnya (Rosa dan Shalahuddin, 2018). Setiap tingkatan harus diselesaikan terlebih dahulu kemudian diteruskan ketahap berikutnya agar menghindari pengulangan tahapan, sehingga system yang dibuat

terstruktur secara rapi. Metode air terjun atau yang sering disebut metode waterfall seing dinamakan siklus hidup klasik (*classic life cycle*), nama model ini sebenarnya adalah "*Linear Sequential Model*" dimana hal ini menggambarkan pendekatan yang sistematis dan juga berurutan pada pengembangan perangkat lunak, dimulai dengan spesifikasi kebutuhan pengguna lalu berlanjut melalui tahapan-tahapan perencanaan (*planning*), permodelan (*modelling*), konstruksi (*contruction*), serta penyerahan sistem ke para pengguna (*deployment*), yang diakhiri dengan dukungan pada perangkat lunak lengkap yang dihasilkan (Wahid & Aceng).



**Sumber: (Pressman, 2012)**

#### 1. Requirement

Tahap ini pengembang sistem diperlukan komunikasi yang bertujuan untuk memahami perangkat lunak yang diharapkan oleh pengguna dan batasan perangkat lunak tersebut. Perangkat lunak *xampp* dan *sublime text* yang digunakan untuk merancang aplikasi serta perangkat keras seperti laptop untuk membangun sebuah aplikasi.

#### 2. Design

Pada tahap ini, pengembang membuat desain sistem yang dapat membantu menentukan sebuah desain dari aplikasi pengamanan pesan *berbasis web* dengan menggunakan algoritma Rot 13 dan Vigenere Cipher. Serta menggunakan pemodelan UML yaitu use case diagram, class diagram, activity diagram, dan sequence diagram untuk perancangan sistem.

#### 3. Implementation

Pada tahap ini, sistem pertama kali dikembangkan di program aplikasi pengamanan pesan, peneliti menggunakan metode Rot 13 dan Vigenere Cipher dengan menggunakan bahasa php dan html pada software *sublime text*.

#### 4. Verification

Pada tahap ini, sistem dilakukan verifikasi dan pengujian apakah sistem sepenuhnya atau sebagian memenuhi persyaratan sistem aplikasi pengamanan pesan dengan Algoritma Rot 13 dan Vigenere Cipher secara keseluruhan. Seperti pengujian fungsional dan pengujian kemampuan aplikasi dalam mengamankan pesan apakah sudah berjalan dengan baik.

#### 5. Maintenance

Ini adalah tahap akhir dari metode *waterfall*, peneliti telah menyelesaikan seluruh penelitian baik teori maupun aplikasi yaitu “Implementasi Rot 13 dan Vigenere Cipher untuk Pengamanan Pesan Berbasis We

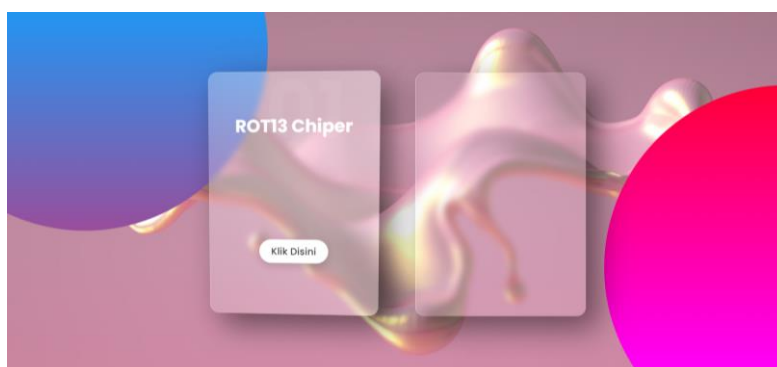
## Hasil dan Pembahasan

### a. Perancangan Sistem

Hasil penelitian berupa uraian yang menunjukkan fakta atau data terkait hasil penelitian. Komputer sebagai sarana penyimpanan data, informasi, dan dokumen penting dan rahasia. Peningkatan keamanan dengan menggunakan pemanfaatan teknologi dengan pemanfaatan ilmu kriptografi yakni Rot 13 dan Vigenere Chiper. Sistem enkripsi ini sudah digunakan sejak masa Romawi untuk mengenkripsi serta menyandikan pesan militer resmi dan rahasia. Enkripsi ini terbilang sederhana namun mampu membentuk cipher dengan penukaran karakter pada planteks menjadi tepat satu karakter pada chiperteks. Proses halaman home dengan sistem Rot 13 dan Vigenere Chiper digunakan untuk mengenkripsi password, sehingga melalui proses enkrip terlebih dahulu sebelum akhirnya dilakukan pencocokan data pada web. Perancangan antarmuka dimuat untuk membuat antarmuka yang mudah dimengerti dan pengguna mampu mengoperasikan web dengan interaktif.

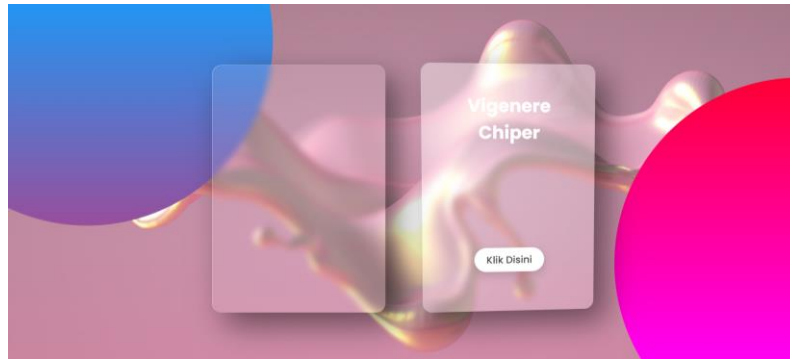
### b. Implementasi Sistem

Setelah dilakukan implementasi ke dalam bahasa pemrograman html, CSS dan PHP berikut ini adalah rincian dari hasil implementasi pada sistem



**Gambar 1. Tampilan awal Rot 13**

Tampilan awal Rot 13 merupakan tampilan yang akan muncul pada saat aplikasi dibuka. Jika aplikasi tersebut digunakan maka tampilan pada halaman depan akan muncul sesuai dengan gerakan pada kursor aplikasi. Tampilan yang ada pada gambar tersebut merupakan tampilan yang ditujukan untuk menghubungkan pada Rot 13. Tulisan pada aplikasi akan muncul dan menghilang otomatis sesuai dengan kursor yang kita arahkan pada aplikasi tersebut.



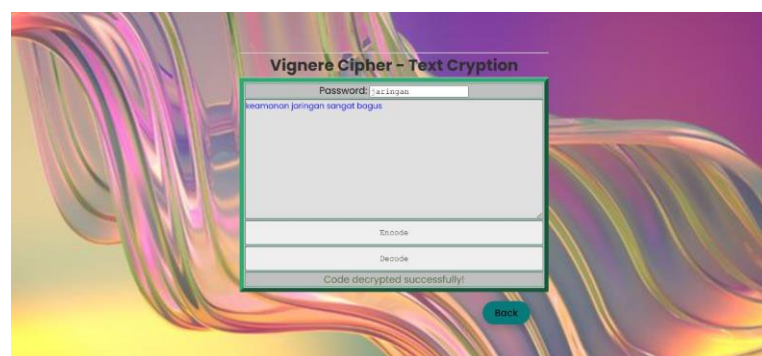
**Gambar 2. Tampilan awal Vigenere Chiper**

Pada tampilan awal Vigenere Chiper merupakan tampilan yang akan menghubungkan pada aplikasi Vigenere Chiper. Tampilan ini secara otomatis akan terhubung Vigenere Chiper dan membuka pada halaman selanjutnya.

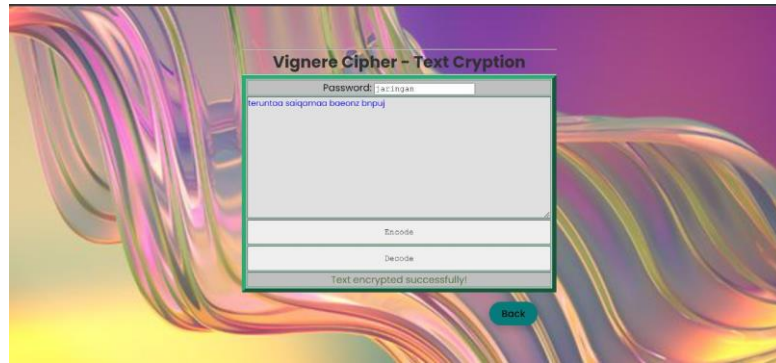


**Gambar 3. Tampilan Rot 13**

Tampilan Rot 13 merupakan tampilan pada aplikasi yang akan muncul pada saat aplikasi tersebut digunakan. Penggunaan aplikasi tersebut berfungsi untuk memasukkan plaintext yang akan di enkripsi menjadi chipertext. Pada bagian ini kita dapat mencari plaintext dan mereset kembali jika akan mengulang kembali plaintext yang akan kita cari. Kemudian pada tampilan tersebut juga terdapat tombol back yang akan mengembalikan pada tampilan awal Rot 13. Pada tampilan ini chipertext dapat kita lihat dalam satu halaman aplikasi, sehingga masih bisa melihat plaintext yang akan kita enkripsi pada aplikasi tersebut.



**Gambar 4. Tampilan Vigenere Chiper**



**Gambar 5. Tampilan Vignere Chiper**

Pada tampilan Vignere Chiper merupakan tampilan yang akan muncul pada saat vignere chiper digunakan. Tampilan dapat mengubah plaintext untuk di enkripsi dan deskripsi menjadi sebuah chipertext. Pada tampilan tersebut terdapat password yang dapat diisi sesuai dengan kebutuhan kita. Kemudian pada tampilan tersebut menjadi dua halaman, sehingga jika kita telah menenkripsi ataupun mendeskripsi sebuah plaintext hasil dari chipertext akan otomatis pada halaman selanjutnya. Jika plaintext telah berhasil kita proses maka akan muncul notifikasi succsessfully. Tampilan tersebut akan kembali ada tampilan awal Vigenere cipher jika kita telah memilih tombol back pada tampilan aplikasi.

Rot 13 adalah algoritma enkripsi sederhana yang menggunakan sandi abjad-tunggal dengan pergeseran  $k=13$  (huruf **A** diganti dengan **N**, huruf **B** diganti dengan **O**, dan seterusnya). Enkripsi ini merupakan penggunaan dari sandi Caesar dengan geseran 13. Pada percobaan aplikasi ROT 13 terdapat, plaintext : HELLO dan menghasilkan chipertext: URYYB.

Vigenere Cipher merupakan teknik menyandikan pesan dengan sandi Caesar menggunakan karakter pada kunci yang digunakan. Kunci yang digunakan pada algoritma ini berupa kunci simetris dan karakter pada kunci tersebut akan dipakai berulang apabila karakter pada pesan belum terproses semua dengan menggunakan modifikasi pada plaintext. Pada percobaan aplikasi Vignere Chiper terdapat, plaintext : KEAMANAN JARNGAN SANGAT BAGUS dan menghasilkan chipertext : TERUNTAA SAIQAMAA BAEONZBNPUJ.

Kriptografi modern selain memanfaatkan algoritma juga menggunakan kunci (*key*) untuk memecahkan masalah tersebut. Proses enkripsi dan dekripsi dilakukan dengan menggunakan kunci ini. Setiap anggota memiliki kuncinya masing-masing yang digunakan untuk proses enkripsi dan dekripsi yang akan dilakukannya. Dalam aplikasi web dibutuhkan mekanisme yang dapat melindungi data dari pengguna yang tidak berhak dan tidak bertanggung jawab. Mekanisme ini dapat diimplementasikan dalam bentuk sebuah proses login yang biasa nya terdiri dari tiga tahapan yakni identifikasi, otentifikasi dan otorisasi pada algoritma Rot 13 dan Vigenere Chiper.

## Kesimpulan

Dalam menjaga kerahasiaan *password* pada pesan implementasi sistem pengamanan pesan berbasis web dengan menggunakan algoritma Rot 13 dan vignere cipher berhasil diterapkan. Sistem ini bertujuan untuk membantu meningkatkan keamanan pesan dan memberikan kemudahan bagi pengguna dengan menggunakan algoritma vignere cipher dan Rot 13. Sistem dapat bekerja dengan mengubah kata atau kalimat ke dalam bentuk enkripsi (mengubah *plaintext* ke dalam bentuk *chipertext*) dan dekripsi (mengubah *chipertext* ke dalam bentuk *plaintext*). Dari contoh kriptografi dengan metode algoritma Rot 13, ketika memasukkan *plaintext* HELLO maka menghasilkan *chipertext* URYYB dan contoh kriptografi vignere chiper,

ketika memasukkan *plaintext* KEAMANAN JARNGAN SANGAT BAGUS, maka menghasilkan *chipertext* TERUNTAA SAIQAMAA BAEONZBNPUJ. Dalam hal ini sistem sangat bermanfaat untuk pengguna dalam menentukan *password* yang akan digunakan dan keamanan pesan meningkat.

## Daftar Referensi

- Aditya, F., Rizky, M., Saputra, R. A., & Abei, F. (2023). *Sistem Login Menggunakan Caesar Chipper Berbasis Web Login System Using Web-Based Caesar Chipper*. 2(1), 267–271.
- Aditya Permana, A. (2018). Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. *Jurnal AL-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, 4(3), 110–115.
- Alasi, T. S., & Fitriani, P. (2022). Peningkatan Keamanan untuk Password menggunakan Algoritma Vigenere Cipher. In *Jurnal Mantik Penusa* (Vol. 6, Issue 1).
- Cahya Hardita, V., Wahyu Sholeha, E., Raya Jl Obos No, P. G., Raya, P., Tengah, K., Informasi, T., Negeri Tanah Laut Jl Yani NoKm, P. A., Pelaihari, K., Tanah Laut, K., & Selatan, K. (n.d.). *PENERAPAN KOMBINASI METODE VIGENERE CIPHER, CAESAR CIPHER DAN SIMBOL BACA DALAM MENGAMANKAN PESAN*.
- Faris, F. A. E. F., Febi, F. Y., Iwan, I. I., & Pizaini, P. (2023). Kombinasi algoritma kriptografi vigenere cipher dengan metode zig-zag dalam pengamanan pesan teks. *Jurnal CoSciTech (Computer Science and Information Technology)*, 4(1), 182–192. <https://doi.org/10.37859/coscitech.v4i1.4787>
- Helmi Sahara. (2018). Implementasi Pengamanan Pesan Chatting menggunakan Metode Vigenere Cipher dan Cipher Block Chaining. *MEANS (Media Informasi Analisa Dan Sistem)*.
- Jtik, J., Teknologi, J., Milian, Y. C., & Sulisty, W. (2023). *Model Pengembangan Keamanan Data dengan Algoritma ROT 13 Extended Vernam Cipher dan Stream Cipher*. 7(2).
- Manullang, A. S., Puspasari, R., & Verina, W. (n.d.). Penyandian Database Menggunakan Metode Base64 Dan Rot13 Database Encoding Using Base64 and ROT13 Methods. In *Penyandian Database Menggunakan ...* (Vol. 283).
- Mu'alimin Arrijal, I., Efendi, R., & Susilo, B. (2016). PENERAPAN ALGORITMA KRIPTOGRAFI KUNCI SIMETRIS DENGAN MODIFIKASI VIGENERE CIPHER DALAM APLIKASI KRIPTOGRAFI TEKS. In *Jurnal Pseudocode* (Vol. 1). [www.ejournal.unib.ac.id](http://www.ejournal.unib.ac.id)
- RH. Sianipar. (2016). *Kompilasi Proyek Kriptografi dengan Visual Basic.Net*. Penerbit Andi.
- Roger S.Pressman. (2012). *Rekayasa Perangkat Lunak (Pendekatan Praktisi)*. Andi Offset.
- Susanto, I. A., & Solichin, A. (2018). *ENKRIPSI DATA PENGGAJIAN DENGAN ALGORITMA CAESAR CIPHER DAN VIGENERE CIPHER PADA PT. KEMASINDO CEPAT NUSANTARA* (Vol. 1, Issue MARET).

- Veny Cahya Hardita, & Eka Wahyu Sholeha. (2021). PENERAPAN KOMBINASI METODE VIGENERE CIPHER, CAESAR CIPHER DAN SIMBOL BACA DALAM MENGAMANKAN PESAN. *SAINTEKOM (Sains, Teknologi, Komputer, Dan Manajemen)*, 11.
- Wahid, A. A. (n.d.). (2020). *Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi. Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK*
- Yazid, M. F., & Haryanto, E. V. (n.d.). *Perancangan Aplikasi Penyandian File Teks Dengan Menggunakan Algoritma ROT13 Dan Rail Fence Cipher Designing a Text File Encryption Application Using the ROT13 Algorithm and Rail Fence Cipher.*