Journal of Science and Social Research ISSN 2615 – 4307 (Print)
May 2024, VII (2): 441 – 448 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

IMPLEMENTASI ALGORITMA VIGENERE DAN ALGORITMA F5 UNTUK KEAMANAN TEKS PADA CITRA

Jihan Ulfa Deski[1], Yusuf Ramadhan Nasution[2], Aidil Halim Lubis[3]
Universitas Islam Negeri Sumatera Utara, Medan
e-mail: [1]jihanulfadeski662000@gmail.com, [2]ramadhannst@uinsu.ac.id,
[3]aidilhalimlubis@uinsu.ac.id

Abstract: *This study aims to build a web-based system that can be used to secure confidential information in the form of words, sentences and others which can be composed of a collection of letters, numbers and symbols which are stored in a text file before distributing the secret message. The information security process is carried out using the Vigenere algorithm and the F5 algorithm. The vigenere algorithm functions in the process of encrypting messages, namely changing plaintext messages into ciphertext so that it cannot be read by other unauthorized people. Meanwhile, the F5 algorithm functions to embed the ciphertext that has been generated into a digital image storage medium. The selection of digital images can make the presence of secret messages unnoticed by others. From the results of testing the resulting text file security system, it can be concluded that the process of encryption and message insertion can be carried out properly and there is no significant change in the size of the image file used as the insertion media. While the results of the PSNR test between the original image and the stego image show results above 30 dB where this value is considered good because there is no change that can be seen directly by the eye, the difference between the original image and the resulting stego image.*

Keywords: *Security, Text Files, Vigenere Algorithm, F5 Algorithm*

Abstrak: Penelitian ini bertujuan untuk membangun sebuah sistem berbasis web yang dapat digunakan untuk mengamankan sebuah informasi rahasia dalam bentuk kata, kalimat dan lainnya yang dapat tersusun dari kumpulan huruf, angka dan juga simbol yang disimpan ke dalam sebuah file text sebelum mendistribusikan pesan rahasia tersebut. Proses pengamanan informasi dilakukan menggunakan algoritma vigenere dan algoritma F5. Algorima vigenere berfungsi dalam proses enkripsi pesan, yaitu mengubah pesan plaintext menjadi ciphertext sehingga tidak dapat dibaca oleh orang lain yang tidak berkepentingan. Sementara itu, algoritma F5 berfungsi untuk melakukan penyisipan ciphertext yang telah dihasilkan ke dalam sebuah media penampung berupa citra digital. Pemilihan citra digital dapat membuat keberadaan pesan rahasia tidak disadari oleh orang lain. Dari hasil pengujian sistem keamanan file text yang dihasilkan dapat disimpulkan bahwa proses enkripsi dan penyisipan pesan dapat dilakukan dengan baik dan tidak terdapat perubahan ukuran file citra yang dijadikan media penyisipan secara signifikan. Sementara dari hasil pengujian PSNR antara citra asli dengan citra stego menampilkan hasil di atas 30 dB dimana nilai tersebut dianggap baik dikarenakan tidak terdapat perubahan yang dapat dilihat secara langsung oleh mata perbedaan antara citra asli dengan citra stego yang dihasilkan.

Kata kunci: Keamanan, File Text, Algoritma Vigenere, Algoritma F5

PENDAHULUAN

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting pada sistem informasi saat ini. Hal ini di sebabkan pesatnya perkembangan ilmu pengetahuan dan teknologi yang memungkinkan

munculnya suatu teknik-teknik yang baru yang disalah gunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut (Gulo, 2019). Ironisnya, teknik yang digunakan untuk mengancam keamanan data selalu setingkat lebih maju dari pada teknik yang digunakan untuk mengamankan data, dengan berkembangnya teknologi informasi secara tidak langsung berpengaruh terhadap bidang keamanan, tidak terkecuali pada kurangnya keamanan data di PNM Ulamm yang terdampak bocornya data nasabah, sehingga dapat disalah gunakan olen pihak yang tidak bertanggung jawab (Aksenta et al., 2023). Semakin canggih teknologi yang berkembang saat ini, artinya semakin tinggi pula ancaman pencurian data. Untuk itu kesadaran akan pentingnya perlindungan data di berbagai teknologi yang dimiliki haruslah sama tingginya dengan kecanggihan teknologi yang dimiliki. Kehilangan data itu bisa sangat merugikan bahkan bisa menjadikan korban sebagai pelaku karena data bisa saja dijadikan alat untuk menipu. Karena itu timbul suatu gagasan yang mengacu kepada permasalahan tersebut, yakni untuk membuat suatu sistem keamanan yang dapat melindungi data yang dianggap penting dengan cara menyandikan data sehingga sulit untuk dideteksi oleh pihak yang tidak berhak (Oksidelfa Yanto, 2021). Segala sesuatu yang melanggar privasi dapat diartikan sebagai tindakan pengambilan, pengubahan atau pengaksesan terhadap data pribadi seseorang tanpa izin terlebih dahulu dari pemiliknya. Hal itu termasuk dalam kategori kejahatan cyber.

Dalam sebuah Perusahan PNM UlaMM memiliki data dan informasi yang sangat penting dan perlu dilakukan untuk menjaga kerahasiaan data tersebut. Dikarenakan data-data yang ada didalam Perusahaan PNM UlaMM itu sendiri bersifat pribadi dan rahasia sehingga jika data tersebut jatuh kepihak yang tidak semestinya akan berdampak buruk terhadap reputasi Perusahaan PNM UlaMM itu sendiri dan bahkan berdampak buruk juga bagi nasabah, misalnya bocornya data diri nasabah yang bersifat rahasia dan apabila data tersebut disalah gunakan orang yang tidak bertanggung jawab akibatnya sangat fatal, seperti penipuan yang mengatas namakan Perusahaan PNM UlaMM sehingga Perusahaan PNM UlaMM kehilangan reputasinya untuk dapat menghindari masalah ini, perusahaan PNM UlaMM harus melakukan pengamanan data nasabah agar data tersebut aman dan terjaga keakuratannya. Data rahasia pada penelitian ini berupa teks.txt., dengan memanfaatkan penggunaan teknik kriptografi dan teknik steganografi. Kriptografi adalah suatu teknik yang bertujuan untuk menyandikan sebuah informasi ke dalam bentuk lain sehingga tidak dapat diketahui informasi yang terkandung pada sebuah data rahasia. Sementara steganografi adalah suatu teknik penyisipan data ke dalam sebuah file (citra, audio, video dan lainnya). Sehingga orang lain tidak akan menyadari keberadaan sebuah teks pada file tersebut (Fathurrahman, 2020).

Berdasarkan penelitian oleh (Alasi et al., 2020) penelitian tersebut memanfaatkan penggunaan algoritma vigenere dalam melindungi keamanan suatu data yang terdapat di dalam database dengan proses enkripsi. Penelitian lainnya oleh (Tampubolon et al., 2020) pada penelitian tersebut diterapkan pengggunaan algoritma F5 untuk menyisipkan pesan ke dalam sebuah gambar yang tidak merubah tampilan pada gambar tersebut secara kasat mata. Berdasarkan beberapa penelitian terdahulu tersebut, untuk melindungi suatu data yang berisikan informasi rahasia akan diimplementasikan penggunaan algoritma vigenere dan algoritma F5.

Algoritma vigenere adalah suatu teknik penyandian teks alfabet menggunakan deretan sandi Caesar berdasarkan huruf pada kunci. Sandi vigenere merupakan bentuk sederhana dari substitusi. Sedangkan algoritma F5 suatu teknik yang menyisipkan bit pesan

kedalam bit koefisien DCT hasil kuantisasi yang telah dipermutasi, penilaian sebuah algoritma steganografi yang baik salah satunya dapat dipandang dari banyaknya pesan yang dapat disisipkan dalam file cover (Mardiah, 2022). Penggunaan kedua algoritma tersebut dalam proses pengamanan data bertujuan untuk menghasilkan sebuah sistem yang dapat menjaga kerahasiaan suatu informasi dengan lebih baik.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk melindungi kepentingan nasabah PNM ULaMM agar terlindungi kerahasiaan yang menyangkut keadaan keuangannya dan data pribadi nasabah, dan untuk membangun sebuah sistem yang dapat digunakan untuk mengamankan sebuah informasi atau data rahasia dalam bentuk kata, kalimat dan lainnya yang dapat tersusun dari kumpulan huruf, angka dan juga simbol yang disimpan ke dalam sebuah file text sebelum mendistribusikan pesan rahasia tersebut (Roberto, 2020). Penggunaan file text adalah untuk dijadikan media penampung teks rahasia yang akan diamankan agar lebih mudah dalam proses pengamanan teks (Putri et al., 2021). Dengan diamankannya informasi rahasia tersebut dapat mencegah tindak pencurian informasi bagi orang lain yang tidak berhak atas informasi rahasia tersebut. Untuk itu pada penelitian ini akan diimplementasikan penggunaan algoritma vigenere dan algoritma F5 ke dalam sebuah sistem untuk melindungi keamanan dari suatu data yang berisikan informasi rahasia.

METODE

Metode penelitian yang digunakan dalam penelitian ini adalah metode R&D (Research and Development). Metode penelitian dan pengembangan R&D (Research and Development) adalah metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektipan produk tersebut (Fransisca & Putri, 2019).

Untuk pengembangan system penelitian menggunakan model SDLC (Software Development Life Cycle). Software Development Life Cycle (SDLC) adalah tahapan-tahapan yang dilakukan peneliti atau proses pembuatan dan pengubahaan sistem serta model metodologi yang digunakan untuk mengembangkan sebuah sistem. SDLC juga merupakan pola yang diambil untuk mengembangkan sistem perangkat lunak, yang terdiri dari tahap-tahap: rencana (planning), analisis data (analysis), desain (design), implementasi (implementation), uji coba (testing), dan pengelolaan (maintenance). Model SDLC yang dipakai dalam penelitian ini adalah model Waterfall Model atau Classic Life Cicle model pengembangan perangkat lunak yang menekankan fase-fase yang berurutan dan sistematis (Jurnal, 2021).

Metodologi Pengumpulan Data

Teknik pengumpulan data yang dilakukan dalam penelitian ini sebagai berikut:

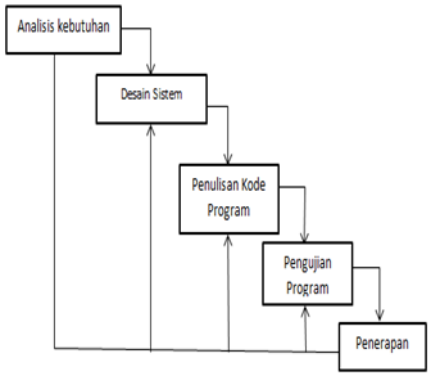
1. Penelitian Kepustakaan
   Dalam penelitian kepustakaan ini penulis melakukan dengan cara mencari Jurnal dan Ebook untuk mempelajari dan menambah wawasan serta mengumpulkan referensi dasar teori yang diambil dari berbagai artikel dan jurnal pada internet yang dibutuhkan dalam penelitian (Maulana et al., 2019).
2. Studi Literatur
   Studi Pustaka (Literatur) merupakan serangkaian yang berkenaan metode pengumpulan daftar pustaka, membaca dan mencatat, serta mengolah bahan penelitian atau menemukan referensi terkait kasus atau isu yang berkaitan dengan tugas akhir. Tujuannya untuk memberikan ide-ide untuk pengembangan kerangka konseptual pada metode penelitian berdasarkan tinjauan pustaka (Casro et al., 2020).
3. Observasi
   Pengamatan (observasi) merupakan salah satu teknik pengumpulan data yang efektif untuk mempelajari suatu

sistem (Sulaiman, 2020). Hal ini dilakukan dengan pengamatan secara langsung terhadap proses pengamanan yang dilakukan menggunakan algoritma vigenere. Serta proses penyisipan pesan menggunakan algoritma F5 ke dalam sebuah citra digital.

4. Wawancara
   Wawancara adalah teknik pengumpulan data yang dilakukan melalui tatap muka dan tanya jawab langsung antara peneliti dan narasumber (Irwanto, 2021). Sebelum melakukan wawancara, peneliti menulis terlebih dahulu membuat daftar petanyaan guna untuk memudahkan proses wawancara dan mendapatkan sebuah data yang lengkap sehingga lebih mudah untuk melakukan analisa data.

Metodologi Pengembangan Sistem

Adapun cara kerja aplikasi implementasi algoritma vigenere dan algoritma f5 untuk keamanan teks pada citra adalah sebagai berikut:



Gambar 1. Tahapan Metode Waterfall

Dimana dalam metode ini terdiri dari beberapa langkah sebagai berikut:

1. Analisis Kebutuhan
   Analisis kebutuhan adalah dimana beberapa kebutuhan bahan dalam sistem yang akan dipergunakan untuk menambah dan membantu jalan proses pembuatan suatu objek (Irianto et al., 2021).
2. Desain Sistem
   Desain sistem adalah tahapan awal desain perangkat lunak. Perancangan ini dilakukan untuk mengetahui kondisi umum sistem (Setiyani, 2021).
3. Penulisan Kode Program Bagian ini menginterpretasikan hasil dari desain yang telah dilakukan sebelumnya kedalam bentuk koding.
4. Pengujian Program
   Pengujian Aplikasi ini menggunakan pengujian Black Box. Pengujian Black Box berfokus pada persyaratan fungsional perangkat lunak (Software) yang dibuat (Andrian, 2021).
5. Penerapan
   Penerapan penelitian ini yaitu menerapkan algoritma vigenere dalam penyisipan data pada citra gambar dengan menggunakan algoritma F5.

Algoritma Vigenere

Vigenere adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci (Afandi & Nurhayati, 2021). 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. Sandi ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan. Pada saat kejayaannya, sandi ini dijuluki le chiffre indéchiffrable (bahasa Prancis: 'sandi yang tak terpecahkan') (Laila & Sinaga, 2019).

Vigenere Cipher adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi caesar berdasarkan huruf-huruf pada kata kunci. Vigenere Cipher merupakan bagian dari algoritma kriptografi klasik yang sangat dikenal karena menggunakan rumus matematika, selain itu Vigenere Cipher

Journal of Science and Social Research ISSN 2615 – 4307 (Print)
May 2024, VII (2): 441 – 448 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

juga dapat menggunakan tabel Vigenere untuk melakukan enkripsi plaintext ataupun dekripsi ciphertext (Hidayah et al., 2023).

Proses enkripsi menggunakan Vigenere Cipher membutuhkan 1 buah kunci untuk dapat menghasilkan ciphertext. Kunci yang digunakan merupakan sebuah kata atau susunan dari beberapa huruf. Kemudian dari kunci yang sudah ditentukan akan dikonversikan menggunakan tabel konversi sehingga menjadi bentuk desimal. Selain mengkonversi kunci yang digunakan, Vigenere Cipher juga harus mengkonversi plaintext (Pi) menggunakan tabel konversi agar menjadi bentuk desimal, kemudian ciphertext (Ci) akan diperoleh dengan mengenkripsi plaintext dengan persamaan (Muhammad & Bahtiar, 2020):

Ci = (Pi + Ki) mod 94

Ci merupakan ciphertext dari pergeseran karakter yang terdapat pada plaintext. Pi merupakan plaintext. Ki merupakan kunci yang digunakan (Utomo et al., 2019).

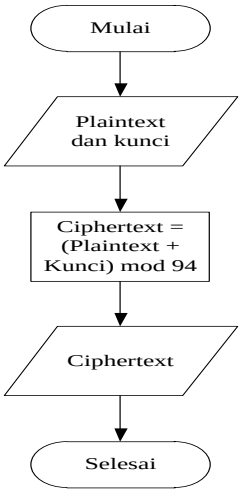
Proses dekripsi menggunakan Vigenere Cipher membutuhkan 1 buah kunci untuk dapat menghasilkan plaintext. Kunci yang digunakan merupakan kunci yang sama dengan kunci yang digunakan pada proses enkripsi. Selain mengkonversi kunci yang digunakan, Vigenere Cipher juga harus mengkonversi ciphertext (Ci) menggunakan tabel konversi yang juga menghasilkan bilangan desimal, kemudian plaintext (Pi) akan diperoleh dengan mendekripsi plaintext dengan persamaan:

Pi = (Ci – Ki + 94) mod 94

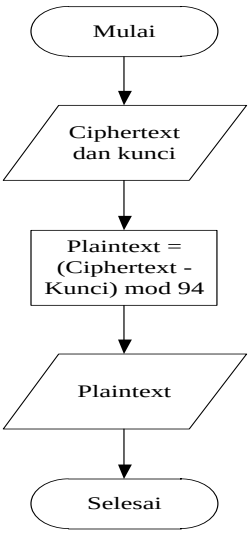
Pi merupakan plaintext dari pergeseran karakter yang terdapat pada ciphertext. Ci merupakan pergeseran karakter pada ciphertext. Ki merupakan kunci berupa hasil konversi tabel berupa bilangan desimal dari pergeseran karakter yang terdapat pada kunci yang digunakan (Afandi & Nurhayati, 2021).

Flowchart Algoritma Vigenere

Flowchart algoritma vigenere menggambarkan proses penggunaan algoritma vigenere dalam melakukan enkripsi dan dekripsi terhadap data yang akan diamankan pada penelitian ini:



Gambar 2. Flowchart Enkripsi Algoritma Vigenere



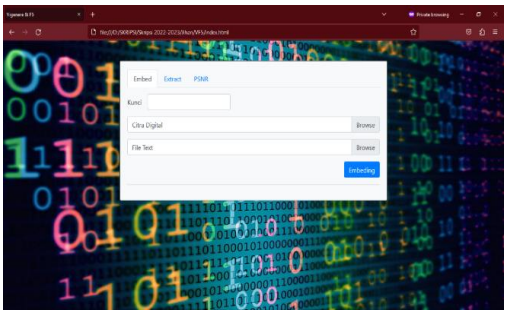
Gambar 3. Flowchart Dekripsi Algoritma Vigenere

HASIL DAN PEMBAHASAN

Tampilan Halaman Embed

Halaman embed yang terdapat pada sistem digunakan untuk melakukan proses pengamanan dan penyisipan data pada file text ke dalam citra digital. Tampilan halaman embed dapat dilihat pada Gambarl 4.

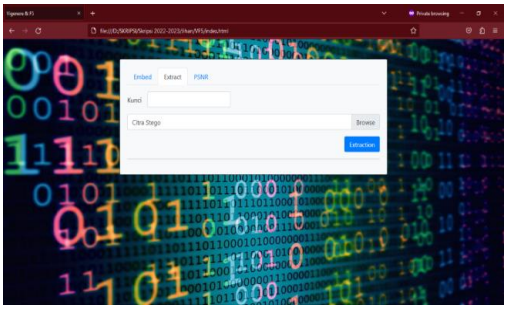
Journal of Science and Social Research ISSN 2615 – 4307 (Print)
May 2024, VII (2): 441 – 448 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR



Gambar 4. Tampilan Halaman Embed

Tampilan Halaman Extract

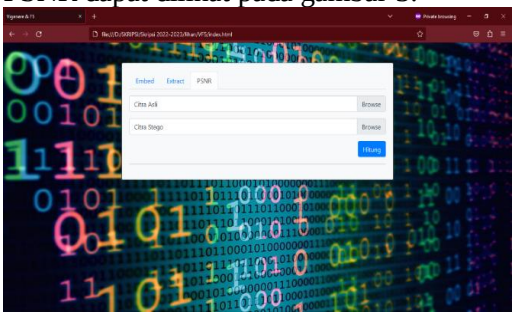
Halaman extrac digunakan untuk menampilkan data teks yang terdapat pada citra stego. Tampilan halaman extract dapat dilihat pada gambar 2.



Gambar 2. Tampilan Halaman Extract

Tampilan Halaman PSNR

Halaman PSNR digunakan untuk melihat nilai PSNR antara citra asli dengan citra stego. Tampilan halaman PSNR dapat dilihat pada gambar 3.



Gambar 3. Tampilan Halaman PSNR

SIMPULAN

Berdasarkan hasil penelitian steganografi citra digital di Dinas Pariwisata Kota Medan, penulis mengambil kesimpulan sebagai berikut:

1. Setelah dianalisis dengan steganografi menggunakan algoritma F5 dengan tiga kualitas yang berbeda diketahui kualitas citra tinggi dengan ukuran 1063 x 598 memiliki nilai MSE 3.58 dan PSNR 35,72, kualitas sedang memiliki nilai MSE 0.30 dan PSNR 85.59 dan kualitas rendah memiliki nilai MSE 0.17 dan PSNR 83.76, kualitas citra setelah dilakukan steganografi dipengaruhi oleh ukuran/kualitas citra tersebut, jika kualitas citra tinggi maka proses penyisipan semakin bagus dan jika kualitas citra rendah nilai PSNR nya kecil atau kurang bagus.
2. Data teks pada penelitian ini berupa text/karakter yang terdapat pada file dengan extensi txt.
3. Citra text yang digunakan sebagai media penyisipan pesan adalah file citra dengan extensi png.
4. Setelah pesan disisipkan kedalam sebuah citra maka data yang disisipkan tidak ada perubahan namun perubahan terjadi pada ukuran pixel pada citra.
5. Aplikasi yang dihasilkan pada penelitian ini juga dapat digunakan untuk membandingkan nilai PSNR dari citra asli dengan citra yang telah disisipkan pesan didalamnya.

DAFTAR PUSTAKA

Afandi, M. I., & Nurhayati, N. (2021). Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android. It (Informatic Technique) Journal, 8(1), 30. https://doi.org/10.22303/it.8.1.2020.30-41

Aksenta, A., Irmawati, I., Ridwan, A., Hayati, N., Sepriano, S., Herlinah, H., Silalah, A. T., Pipin, S. J., Abdurrohim, I., & Boari, Y. (2023). Literasi Digital: Pengetahuan & Transformasi Terkini Teknologi Digital Era Industri 4.0 dan Sociaty 5.0. PT. Sonpedia Publishing

Indonesia.

Alasi, T. S., Taufik, A., & Afkari, A. (2020). Jurnal Informasi Komputer Logika Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database. 1.

Andrian, D. (2021). Penerapan Metode Waterfall Dalam Perancangan Sistem Informasi Pengawasan Proyek Berbasis Web. Jurnal Informatika Dan Rekayasa Perangkat Lunak (JATIKA), 2(1), 85–93.

Casro, C., Purwati, Y., Setyaningsih, G., & Kuncoro, A. P. (2020). Rancang Bangun Aplikasi Pengaduan Pelanggan Berbasis Web Menggunakan Framework Codeigniter Di Indotechno Purwokerto. Jurnal Sains Dan Informatika, 6(2), 166–174. https://doi.org/10.34128/jsi.v6i2.244

Fathurrahman, R. F. (2020). Implementasi Steganografi Pada Citra Digital Dengan Metode Spread Spectrum Dan Affine Cipher. Universitas Komputer Indonesia.

Fransisca, S., & Putri, R. N. (2019). Pemanfaatan Teknologi RFID Untuk Pengelolaan Inventaris Sekolah Dengan Metode (R&D). Jurnal Mahasiswa Aplikasi Teknologi Komputer Dan Informasi, 1(1), 72–75.

GULO, M. (2019). RANCANG BANGUN APLIKASI PESAN QR CODE MENGGUNAKAN ALGORITMA BEAUFORT BERBASIS ANDROID.

Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks. Journal on Education, 5(3), 8563–8573.

Irianto, Sudarmin, & Afrisawati. (2021). Penerapan Metode Customer Relationship Management Pada Penjualan Toko Baju Azzahra. Journal of Science and Social Research, 4(2), 191. https://doi.org/10.54314/jssr.v4i2.584

Irwanto, I. (2021). Perancangan Sistem Informasi Sekolah Kejuruan dengan Menggunakan Metode Waterfall (Studi Kasus SMK PGRI 1 Kota Serang-Banten). Lectura : Jurnal Pendidikan, 12(1), 86–107. https://doi.org/10.31849/lectura.v12i1.6093

Jurnal, J. (2021). Rancang Bangun Marketplace Berbasis Website menggunakan Metodologi Systems Development Life Cycle (SDLC) dengan Model Waterfall. Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi), 5, 2.

Laila, N., & Sinaga, A. S. R. M. (2019). Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra. ScientiCO: Computer Science and Informatics Journal, 1(2), 47–58.

Mardiah, M. (2022). Implementasi algoritma Cipher Block Chaining dan transposisi grup simetri S4 pada pengamanan pesan teks. Universitas Islam Negeri Maulana Malik Ibrahim.

Maulana, F., Arwan, A., & Pramono, D. (2019). Pengembangan Sistem Aplikasi Manajemen Distribusi Pupuk Berbasis Web (Studi Kasus : PT. Petrokopindo Cipta Selaras) Fahrir). Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 3(10), 10279–10286.

Muhammad, R. R., & Bahtiar, N. (2020). Pengembangan Aplikasi Parental Control Berbasis Android Menggunakan Kriptografi Vigenere Cipher pada Pattern Lock. Jurnal Masyarakat Informatika, 11(2), 15–26.

Oksidelfa Yanto, S. H. (2021). Pemidanaan atas Kejahatan yang Berhubungan dengan Teknologi Informasi. Samudra Biru.

Putri, A. E., Kartikadewi, A., & Rosyid, L. A. A. (2021). Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada

Dinas Pendidikan Kabupaten Tangerang. Appl. Inf. Syst. Manag, 3(2), 69–78.

Roberto, A. (2020). LEBIH MENGENAL DIGITAL BANKING MANFAAT, PELUANG, DAN TANTANGAN. http://pasca. ugm. ac. id/.

Setiyani, L. (2021). Desain Sistem: Use Case Diagram. Prosiding Seminar Nasional Inovasi Dan Adopsi Teknologi (INOTEK), 1(1), 246–260.

Sulaiman, M. M. (2020). Perancangan Prototipe Sistem Pakar Diagnosa Kerusakan Mobil Toyota Tipe Mpv Menggunakan Metode Forward Dan Backward Chaining Berbasis Android. Journal Of Artificial Intelligence And Innovative Applications, 1(1), 6–11.

Tampubolon, D. T. P., Chahyadi, F., & Muhammad Radzi Rathomi. (2020). Penyisipan Pesan Pada Gambar Menggunakan Algoritma Blowfish Dan Algoritma F5. Student Online Journal (SOJ), 1, 74–87.

Utomo, I. W., Latifah, R., & Risanty, R. D. (2019). Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher Dan Vigenere Cipher. JUST IT: Jurnal Sistem Informasi, Teknologi Informasi Dan Komputer, 9(2), 142–149.