Volume 5 Issue 1 (2025) Pages 93-104 P-ISSN:2798-2696 E-ISSIN:2798-0057
JOSTECH
Journal of Science and Technology
Website: https://ejournal.uinib.ac.id/jurnal/index.php/jostech Email: jostech@uinib.ac.id

Implementasi Kriptografi Menggunakan Kombinasi *Hill*, *Affine* dan *Stream Cipher* dalam Mengamankan Data Teks

Rahmad A. Otolomo[1], Isran K. Hasan[2], Asriadi[3], Hasan S. Panigoro[4], Djihad Wungguli[5], Nisky Imansyah Yahya[6]
[123456] Program Studi Matematika, Universitas Negeri Gorontalo, Indonesia
email: rahmadotolomo@gmail.com

Received 02 Februari 2025, Accepted 28 Maret 2025, Published 31 Maret 2025

Abstrak

Di masa perkembangan digital yang semakin pesat saat ini, rentan terhadap kebocoran informasi, perlindungan data menjadi salah satu aspek yang tak bisa diabaikan. Kerentanan terhadap serangan yang merugikan mendorong penerapan metode perlindungan data yang lebih aman. Salah satu solusi yang bisa digunakan dalam menjaga kerahasiaan data dengan menggunakan teknik kriptografi. Kriptografi adalah suatu teknik penyamaran pesan, data, atau informasi yang hanya dapat di akses oleh pihak tertentu. Pada penelitian ini berfokus pada penyandian data teks dengan mengkombinasikan tiga algoritma kriptografi yaitu algoritma Hill Cipher, Affine Cipher dan Stream Cipher Pada penelitian ini berfokus pada penyandian data teks dengan mengkombinasikan tiga algoritma kriptografi. Proses enkripsi dimulai dengan menggunakan Hill Cipher, kemudian hasil enkripsi tersebut dienkripsi kembali menggunakan Affine Cipher, dan terakhir dienkripsi kembali dengan Stream Cipher. Pada proses dekripsi, data yang telah dienkripsi diurai terlebih dahulu dengan Stream Cipher, kemudian dilanjutkan dengan Affine Cipher, dan diakhiri dengan Hill Cipher. Penelitian ini menghasilkan dua program GUI Python proses enkripsi dan dekripsi terhadap sebuah data teks.

Kata Kunci: *Dekripsi; Enkripsi; Keamanan Data; Penyandian*.

Abstract

In this time of rapid digital development, prone to information leakage, data protection is one aspect that cannot be ignored. Vulnerability to harmful attacks encourages the implementation of more secure data protection methods. One solution that can be used in maintaining data confidentiality is by using cryptographic techniques. Cryptography is a technique for masking messages, data, or information that can only be accessed by certain parties. In this research focuses on encrypting text data by combining three cryptographic algorithms, namely the Hill Cipher, Affine Cipher and Stream Cipher algorithms. The encryption process starts by using Hill Cipher, then the encryption results are re-encrypted using Affine Cipher, and finally re-encrypted with Stream Cipher. In the decryption process, the encrypted data is first decrypted with Stream Cipher, then continued with Affine Cipher, and ended with Hill Cipher. This research produces two Python GUI programs for encryption and decryption of text data.

Keywords: *Decryption; Encryption; Data Security; Encoding.*

✉ Corresponding author

PENDAHULUAN

Perkembangan teknologi pada jaman modern telah meyakinkan orang untuk melakukan interaksi dengan orang lain dengan bertukar data dan informasi tanpa batasan jarak dan waktu. Dengan meningkatnya tuntutan keamanan atas kerahasiaan informasi yang dipertukarkan, maka tantangan akan ketersediaan data dan sistem keamanan informasi yang lebih dipercaya untuk melindungi data dari ancaman pencurian data. Dalam melakukan pencurian data biasanya banyak cara yang bisa dilakukan, diantaranya dengan menggunakan algoritma Brute Force [1]. Penyerang memantau dan mungkin memanipulasi komunikasi antara dua orang yang berinteraksi,mengakibatkan pengungkapan informasi sensitif atau manipulasi data. Oleh karena itu, menghadapi tantangan ini, perlu adanya meningkatkan strategi keamanan data dan informasi yang terperinci, termasuk pelatihan kesadaran keamanan yang dapat melindungi data dari ancaman pencurian data, pengguna teknologi enkripsi yang tepat, dan implementasi kebijakan sistem keamanan yang ketat untuk melindungi data yang dikirimkan melalui jaringan komunikasi [2]. Ada beberapa cara melakukan pengamanan data ataupun pesan, diantaranya adalah dengan menggunakan teknik penyamaran data yang disebut dengan kriptografi dan teknik penyembunyian data yang disebut dengan steganografi. Salah satu cara yang umum digunakkan untuk melindungi data yaitu menggunakan teknik penyandian atau penyamaran data yang disebut kriptografi [3]. Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa [4].

Algoritma Hill Cipher adalah suatu teknik kriptografi klasik yang memerlukan matriks untuk kunci dalam menjalankan proses enkripsi dan dekripsi pesan, baik dalam bentuk teks maupun data. Algoritma ini memproses blok data dengan ukuran yang sama dan dapat bekerja dengan baik pada data teks maupun angka [5]. Affine Cipher merupakan salah satu teknik kriptografi yang mungkin sederhana dengan menggunakan dua kunci berupa bilangan bulat a dan b untuk menjalankan proses enkripsi dan dekripsi pada data. Algoritma ini efisien untuk mengamankan pesan rahasia dalam bentuk teks dan dapat diterapkan dengan mudah [6]. Sementara Stream Cipher adalah salah satu teknik kriptografi yang menggunakan aliran bit atau stream dari kunci satu per satu untuk menjalankan proses enkripsi dan deskripsi pada data. Algoritma ini menyediakan cara untuk menjaga kerahasiaan data yang efektif dan komunikasi yang aman [7].

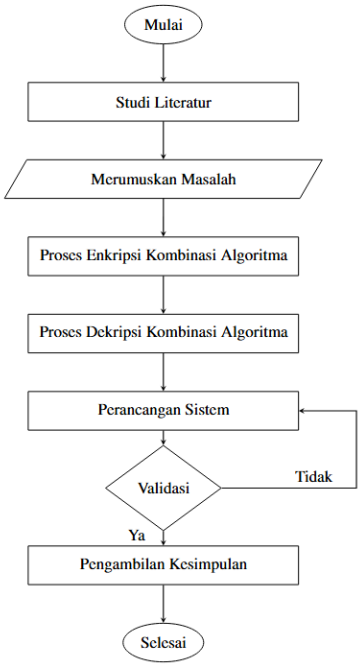
Penelitian ini menawarkan inovasi dalam penerapan kriptografi dengan mengombinasikan tiga algoritma yang memiliki karakteristik berbeda, yaitu Hill Cipher, Affine Cipher, dan Stream Cipher. Kombinasi ini meningkatkan keamanan karena setiap algoritma memiliki pendekatan enkripsi yang berbeda, sehingga apabila satu metode memiliki kelemahan, metode lainnya tetap memberikan perlindungan tambahan. Berbeda dari penelitian sebelumnya yang hanya menerapkan satu atau dua algoritma, penelitian ini menyajikan pendekatan berlapis untuk enkripsi data teks. Selain itu, penelitian ini mengimplementasikan algoritma tersebut dalam bentuk GUI berbasis Python, sehingga lebih mudah digunakan oleh pengguna tanpa keahlian

pemrograman. Ini memberikan kelebihan keamanan yang penting dan dipastikan bahwa data dilindungi sebaik mungkin.

METODOLOGI

Penelitian ini dilakukan dengan menggunakan metode studi literatur (library research). Dalam penelitian ini, dilakukan kajian teori terhadap buku, jurnal, artikel ilmiah, dan literatur lainnya, termasuk data yang bersumber dari internet, yang berkaitan dengan implementasi kombinasi algoritma Hill Cipher, Affine Cipher dan Stream Cipher pada proses enkripsi dan dekripsi data teks yang bertujuan untuk memperoleh informasi yang akan digunakan dalam pembahasan masalah ini. Selanjutnya, dilakukan pengimplementasian dalam program aplikasi menggunakan GUI Python.

Flowchart Rancangan Penelitian



Gambar 1. Flowchart Rancangan Penelitian

Adapun langkah-langkah yang akan dilakukan pada penelitian ini yaitu sebagai berikut :

1. Mempelajari Referensi

   Tahap awal pada penelitian ini yaitu dengan mempelajari berbagai referensi atau melakukan kajian teori terhadap buku, artikel ilmiah, jurnal, dan sejenisnya yang berkaitan dengan penelitian kriptografi menggunakan kombinasi algoritma Hill Cipher, Affine Cipher dan Stream Ciphe
2. Merumuskan Masalah

Setelah mempelajari referensi dan melakukan kajian teori, selanjutnya merumuskan masalah yang akan dibahas dalam penelitian ini

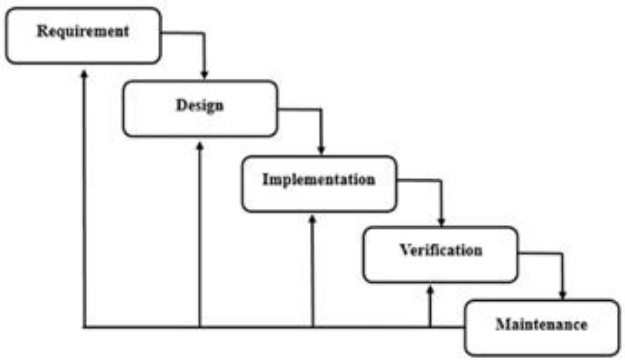
3. Proses Enkripsi Kombinasi Algoritma

Pada tahap ini sudah mencakup enkripsi dengan menggunakan kombinasi algoritma Hill Cipher, Affine Cipher dan Stream Cipher. Berikut ini penjelasan terkait proses enkripsi kombinasi algoritma tersebut :

a) Tahap awal yaitu menentukan sebuah plaintext (data asli).

b) Setelah menentukan plaintext, selanjutnya melakukan enkripsi terhadap plaintext menggunakan algoritma Hill Cipher terlebih dahulu, kemudian akan menghasilkan sebuah ciphertext (data acak). ciphertext ini belum menjadi hasil akhir dari prose enkripsi, karena masih akan di enkripsi lagi menggunakan algoritma Affine Cipher, sehingga ciphertext ini masih bisa di katakan sebuah plaintext kedua.
c) Selajutnya, hasil dari enkripsi (plaintext kedua), akan di enkripsi lagi menggunakan algoritma Stream Cipher, sehingga akan menghasilkan ciphertext baru. ciphertext ini merupakan hasil akhir dari proses enkripsi.

4. Proses Dekripsi Kombinasi Algoritma
   Pada tahap ini sudah mencakup dekripsi dengan menggunakan kombinasi algoritma Hill Cipher, Affine Cipher dan Stream Cipher. Berikut ini penjelasan terkait proses dekripsi kombinasi algoritma tersebut :
   a) Setelah melakukan tahapan enkripsi, selanjutnya masuk pada tahap dekripsi. Pada tahap ini, dimulai dengan melakukan dekripsi terhadap ciphertext baru menggunakan algoritma Stream Cipher terlebih dahulu.
   b) selanjutnya hasil dari deskripsi pertama akan dilanjutkan dengan menggunakan algoritma Affine Cipher kemudian akan menghasilkan sebuah ciphertext lama (plaintext kedua).
   c) Selanjutnya, hasil dari dekripsi (plaintext kedua) akan di dekripsi lagi menggunakan algoritma Hill Cipher, kemudian akan menghasilkan sebuah plaintext (data asli). plaintext ini adalah hasil akhir dari proses dekripsi, karena data kembali ke bentuk aslinya.
5. Perancangan Sistem



Gambar 2. Tahapan Pengembangan Sistem dengan Metode Waterfall

a) Persayaratan/Analisa Kebutuhan (Requirement)
   Pada fase ini, komunikasi antara pengembang sistem sangat penting untuk memahami kebutuhan perangkat lunak yang diharapkan oleh pengguna dan batasan-batasan yang terkait dengan perangkat lunak tersebut. Informasi ini dapat diperoleh melalui berbagai cara seperti wawancara, diskusi, atau survei langsung. Setelah itu, informasi yang diperoleh dianalisis untuk mendapatkan data yang dibutuhkan oleh pengguna.

b) Desain (Design)
Pada fase ini, pengembang melakukan pembuatan desain sistem yang membantu dalam menentukan persyaratan perangkat keras (hardware) dan sistem, serta membantu dalam mendefinisikan arsitektur sistem secara keseluruhan.

c) Implemntasi (Implementation)
Pada fase ini, sistem dikembangkan pertama kali dalam bentuk program kecil yang disebut dengan unit, dimana nantinya akan terintegrasi dalam tahap berikutnya. Setiap unit dikembangkan dan diuji untuk memastikan fungsionalitasnya yang disebut sebagai unit testing

d) Tinjau (Verification)
Pada fase ini, sistem menjalani proses verifikasi dan pengujian untuk memastikan apakah sistem secara keseluruhan atau sebagian memenuhi persyaratan yang telah ditetapkan. Pengujian dapat dibagi menjadi tiga kategori, yaitu unit testing (pengujian pada modul kode tertentu), sistem pengujian (untuk menguji respons sistem saat semua modul terintegrasi), dan pengujian penerimaan (dilakukan bersama atau atas nama pelanggan untuk memastikan kepuasan terhadap semua kebutuhan pelanggan).

e) Pemeliharaan (Maintenance)
Ini merupakan tahap akhir dalam metode Waterfall. Pada fase ini, perangkat lunak yang telah selesai dikembangkan dan dijalankan akan dilakukan pemeliharaan. Pemeliharaan melibatkan perbaikan kesalahan yang mungkin tidak terdeteksi pada fase-fase sebelumnya.

6. Validasi
Tahap terakhir yait melakukan validasi data terhadap GUI dengan cara menghitung secara manual, sehingga dapat dibuktikan bahwa sistem benar-benar berjalan sesuai prosedur.
7. Pengambilan Kesimpulan
Pada tahap ini bertujuan untuk merangkum hasil dari seluruh proses yang telah dilakukan. Proses ini juga memberikan saran atau rekomndasi untuk perbaikan atau pengembangan lebih anjut.

Metode Pengembangan

Pada penelitian ini akan menghasilkan dua buah program GUI pyton yang dirancang menggunakan software Spyder. Setelah program tersebut dirancang, selanjutnya akan dikembangkan menjadi program GUI standalone (berdiri sendiri) tanpa bantuan software lain untuk menjalankannya termasuk Spyder itu sendiri.

HASIL DAN PEMBAHASAN

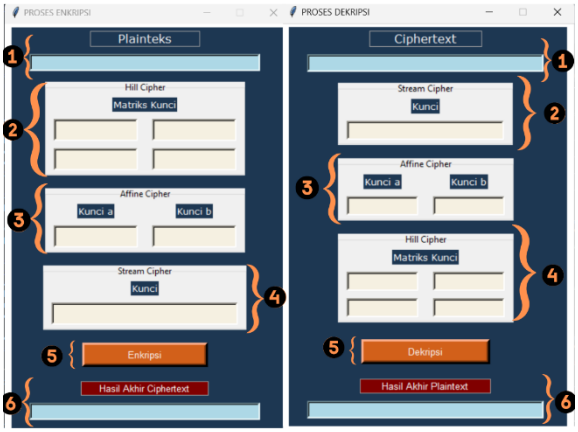
Analisa Kebutuhan

Analisis kebutuhan sistem bertujuan untuk mengidentifikasi terkait kebutuhan yang dibutuhkan dalam pembuatan sistem. Terdapat analisis kebutuhan fungsional yang mencakup tentang penjelasan proses yang dijalankan oleh sistem untuk mencapai tujuan. Ada beberapa persyaratan fungsional yang harus dipenuhi dalam pengembangan sistem ini yakni sebagai berikut :

a) Menampilkan hasil akhir proses enkripsi maupun dekripsi dari sebuah data teks sesuai dengan program yang dijalankan.
b) Kedua sistem ini menerima input dan mengeluarkan output bertipe data teks. Data teks tersebut berupa karakter abjad alphabet dan angka. Jumlah karakter adalah 62 karakter yang terdiri dari 26 huruf besar dan 26 huruf kecil serta angka 0 sampai 9.
c) Pada rogram yang pertama plaintext dienkripsi menjadi ciphertext 1, kemudian dienkripsi menjadi ciphertext 2, kemudian akan dienkripsi lagi menjadi ciphertext 3.
d) Pada program yang kedua ciphertext 3 didekripsi menjadi plaintext 2, kemudian didekripsi menjadi plaintext 1, kemudian didekripsi lagi menjadi plaintext atau data teks asli.
e) Masing-masing program memiliki bagian untuk memasukan plaintext, kunci dan ciphertext.

Desain

Desain GUI python pengamanan data teks pada penelitian ini dibuat menjadi dua desain yaitu desain GUI proses enkripsi dan GUI proses dekrispi. Script desain GUI enkripsi dan dekripsi bisa dilihat pada lampiran B.1 dan lampiran B.2.



Gambar 3. Desain GUI Proses Enkripsi dan Dekripsi

Berdasarkan Gambar 4.1 di atas dapat dilihat bahwa:

a) Pada Gambar (a) desain GUI proses enkripsi terdiri atas (a.1) kotak input plaintext, (a.2) kotak input kunci matriks berordo [2 x 2] untuk algoritma Hill Cipher, (a.3) kotak input kunci a dan b untuk algoritma Affine Cipher, (a.4) kotak input kunci untuk algoritma Stream Cipher, (a.5) tombol enkripsi, dan (a.6) kotak hasil akhir enkripsi dengan algoritma Hill Cipher, Affine Cipher dan Stream Cipher
b) Pada Gambar (b) desain GUI proses dekripsi terdiri atas (b.1) kotak input hasil akhir ciphertext r, (b.2) kotak input kunci untuk algoritma Stream Cipher, (b.3) kotak input kunci a dan b untuk algoritma Affine Cipher, (b.4) kotak input kunci matriks berordo [2 x 2] untuk algoritma Hill Cipher, (b.5) tombol dekripsi,

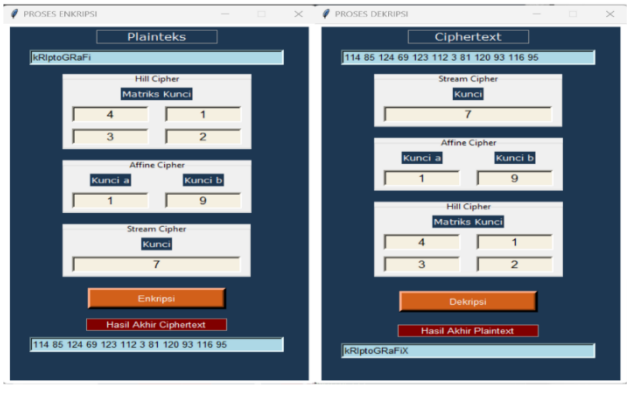
dan (b.6) kotak hasil dekripsi dengan algoritma Stream Cipher, Affine Cipher dan Stream Cipher

Implementasi

Implementasi yang akan dihasilkan dari penelitian ini adalah dua buah program GUI (Graphical User Interface) yaitu program GUI proses enkripsi dan dekripsi menggunakan kombinasi algoritma Hill Cipher, Affine Cipher dan Stream Cipher yang dibuat menggunakan software Spyder dengan bahasa pemrograman Python. Kedua program ini dapat digunakan oleh pengguna yang ingin mengririm pesan berupa data teks, terkhusus yang sifatnya rahasia. Dengan menggunakan Program GUI berbasis python memberikan kelebihan dibandingkan dengan metode lain. GUI memberikan tampilan yang mudah dipahami, memudahkan pengguna dalam memasukkan data, melihat hasil enkripsi, serta mendapatkan keluaran dengan cepat. Dengan menggunakan GUI, pengembang dapat dengan mudah memperluas fitur atau menggabungkan algoritma tambahan untuk meningkatkan keamanan sistem. Keamanan dari implementasi dengan mengkombinasikan tiga algortima dapat menahan serangan frekuensi karakter, karena plaintext mengalami beberapa lapisan enkripsi, Dengan enkripsi multi-lapisan, proses brute force menjadi lebih sulit dilakukan karena proses kombinasi kunci. Dengan adanya kombinasi algoritma ini serta implementasi berbasis GUI Python, penelitian ini memberikan solusi yang lebih aman dan mudah digunakan dalam perlindungan data teks.

Tinjau

Pada fase ini, akan di uji apakah sistem berjalan sesuai dengan prosedur persyaratan fungsional yang telah dijelaskan pada bagian analisa kebutuhan sebelumnya atau tidak. Berikut ini adalah hasil uji sistem kedua program GUI proses enkripsi dan deksripsi sesuai prosedur yang telah memenuhi persyaratan fungsional.



(a) (b)

Gambar 4. Hasil Uji Sistem Berdasarkan Persyaratan Fungsional

Pada gambar di atas terbukti bahwa sistem telah memenuhi persyaratan fungsional yang telah di jelaskan sebelumnya. Seluruh komponen yang dibutuhkan pada persyaratan fungsional tersebut telah terpenuhi.

Pemeliharaan

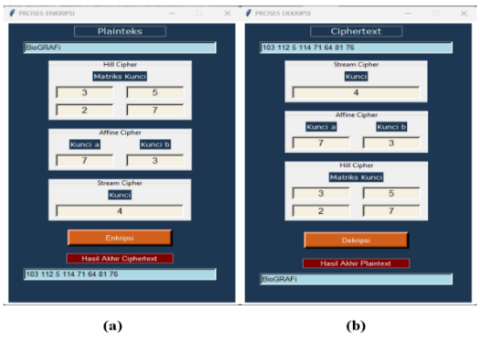
Pada fase ini, program bisa dijalankan sesuai perintah. Untuk pemeliharaan selanjutnya bisa dilakukan ketika ada kesalahan yang terjadi pada saat program dijalankan. Selain itu pada fase ini juga diperuntukan dalam sebuah pengembangan program nantinya. Jadi jika akan dilakukan sebuah pengembangan pada program ini, misalnya akan ada beberapa perubahan terhadap program, maka perlu dilakukan pemeliharaan.

Validasi Sistem

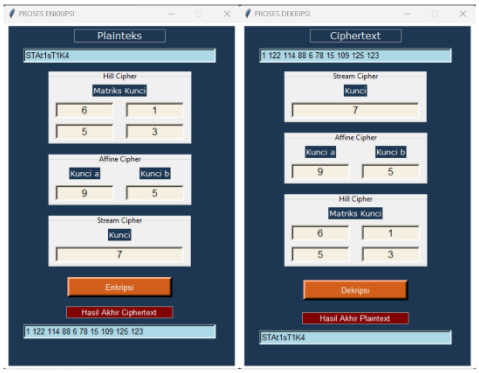
Setelah melakukan analisis dan perancangan sistem berdasarkan metode Waterfall selanjutnya akan dilakukan validasi sistem secara manual. Pada tahap ini akan dibuktikan bahwa hasil dari program sesuai dengan yang kita kerjakan secara manual atau tidak. Proses validasi dilakukan sebanyak tiga kali. Sebelum masuk pada proses validasi berikut adalah tabel daftar karakter yang akan di gunakan pada penelitian ini.

Tabel 1. Judul Tabel

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
0	1	2	3	4	5	6	7	8	9	10	11	12
n	**o**	**P**	**Q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
13	14	15	16	17	18	19	20	21	22	23	24	25
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
26	27	28	29	30	31	32	33	34	35	36	37	38
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
39	40	41	42	43	44	45	46	47	48	49	50	51
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**			
52	53	54	55	56	57	58	59	60	61			

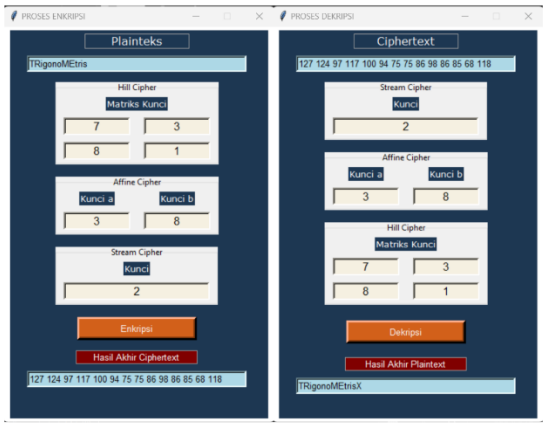


Gambar 5. Validasi Untuk Plaintext Huruf Semua



(a) (b)

Gambar 6. Validasi Untuk Plaintext Huruf dan Angka



(a) (b)

Gambar 7. Validasi Untuk Plaintext Berjumlah Ganjil

Setelah melakukan Validasi secara manual, terbukti bahwa program berjalan sesuai prosedur persyaratan fungsional. Dengan menggabungkan algortima *Hill Cipher*, *Affine Cipher* dan *Stream Cipher* dalam mengamankan data teks dapat meningkatkan keamanan data yang tinggi untuk menjaga privasi agar lebih aman. Penerapan algoritma ini dalam aplikasi dapat di implementasikan pada berbagai aspek di dunia nyata, misalnya pesan enkripsi atau menyimpan data sensitif. Dengan mengenkripsi data pada beberapa tingkat menggunakan beberapa algoritma, aplikasi ini tidak hanya meningkatkan kerahasiaan tetapi juga mencegah serangan yang memanfaatkan satu algoritma tunggal. Misalnya jika seseorang penyerang berhasil memecahkan enkripsi *Hill Cipher*, algoritma ini masih harus melindungi lapisan enkripsi tambahan yang disediakan oleh *Affine Cipher* dan *Stream Cipher*, yang masing-masing memperkenalkan tingkat kerumitan tersendiri. Oleh karena itu, penggunaan gabungan algoritma ini menawarkan solusi kemanan yang lebih baik. Dalam hal ini sudah di uji Validasi sebanyak tiga kali dengan mengkombinasikan beberapa karakter yang membuktikan bahwa program berjalan sesuai prosedur persyaratan fungsional.

Definisi

1. **Kriptografi** [8] *kriptografi dapat didefinisikan sebagai seni dan ilmu untuk membuat pesan atau informasi menjadi tersembunyi atau tidak dapat dimengerti oleh pihak yang tidak berwenang.[9] kriptografi dapat diartikan sebagai disiplin ilmu yang mempelajari metode-metode matematika yang berkaitan dengan aspek keamanan informasi, termasuk integritas data, kerahasiaan, dan keaslian data.[10] Kriptografi adalah seni menyembunyikan fakta-fakta dalam komunikasi melalui penyandian sehingga hanya penerima yang ditujukan yang dapat menafsirkannya.[11] Kriptografi adalah studi tentang komunikasi aman di hadapan penyerang*
2. **Terminologi Kriptografi** [12] *Terminilogi pada kriptografi yaitu :*

a) Pesan, Plaintext, Ciphertext
b) Pengirim dan Penerima Pesan
c) Enkripsi dan Dekripsi
d) Cipher dan Kunci
e) Penyadap

3. **Algoritma Hill Cipher** [13] *Merupakan algoritma kriptografi kunci simetris yang menggunakan matriks untuk mengenkripsi dan mendekripsi pesan.*
4. **Algoritma Affine Cipher** [14] *Digunakan untuk penyandian pesan atau informasi dan termasuk dalam kategori algoritma klasik yang telah digunakan sejak sebelum adanya perkembangan teknologi digital. [15] Algoritma Affine Cipher adalah metode penyamaran yang merupakan pengembangan dari caesar cipher.*
5. **Algoritma Stream Cipher** [16] *Memiliki teknik enkripsi populer yang digunakan dalam berbagai standar komunikasi dan protokol.*

SIMPULAN

Berdasarkan hasil dan pembahasan dapat disimpulkan bahwa proses enkripsi dan dekripsi data teks dengan menggunakan kombinasi algoritma Hill Cipher, Affine Cipher dan Stream Cipher dilakukan dengan mengenkripsi plaintext menggunakan algoritma Hill Cipher terlebih dahulu, selanjutnya dienkripsi lagi menggunakan algoritma Affine Cipher, setelah itu hasilnya dienkripsi lagi menggunakan algoritma Stream Cipher. Kemudian hasil enkripsi tersebut akan didekripsi menggunakan algoritma Stream Cipher Selanjutnya di dekripsi lagi menggunakan Affine Cipher, setelah itu hasilnya akan didekripsi lagi menggunakan algoritma Hill Cipher sehingga hasilnya akan kembali menjadi bentuk asli plaintext. Implementasi Kriptografi dengan mengkombinasikan tiga buah algoritma yaitu Hill Cipher, Affine Cipher dan Stream Cipher dalam mengamankan data teks pada penelitian ini menunjukkan bahwa hasil penelitian yang dibuat adalah dua program GUI Python proses enkripsi dan dekripsi. Kedua program tersebut dapat melakukan proses enkripsi maupun dekripsi pesan berupa data teks. Hasil validasi dari kedua program tersebut diperoleh dari pembuktian antara perhitungan manual dan perhitungan di program menghasilkan hasil yang sama. Terkhusus untuk pesan yang berjumlah ganjil, secara otomatis akan digenapkan yaitu dengan menambahkan sebuah karakter ”X” pada pesan tersebut sehingga proses enkripsi dan dekripsi dapat berjalan.

DAFTAR PUSTAKA

[1] I. Gunawan, "Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force," TECHSI - Jurnal Teknik Informatika, vol. 13, no. 1, p. 14, Apr. 2021, doi: 10.29103/techsi.v13i1.2395.

[2] M. Azhari, J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," Jurnal Pendidikan Sains dan Komputer, vol. 2, no. 1, pp. 2809–476, 2022, doi: 10.47709/jpsk.v2i1.1390.

[3] W. Stallings, Cryptography and network security : principles and practice. 2017.

[4] E. C. Prabowo and I. Afrianto, "PENERAPAN DIGITAL SIGNATURE DAN KRIPTOGRAFI PADA OTENTIKASI SERTIFIKAT TANAH DIGITAL," Ilmiah Komputer dan, vol. 6, no. 2, 2017.

[5] P. Hasan, S. Yunita, D. Ariyus, S. Sepuluh Nopember Jayapura, and U. Amikom Yogyakarta, "Implementasi Hill Cipher Pada Kode Telepon dan Five Modulus Method dalam Mengamankan Pesan Implementation of Hill Cipher in Telephone Code and Five Modulus Method for Securing Messages," 2020.

[6] S. Yana Wulandari, "Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message," vol. 3, pp. 741–744, 2020.

[7] I. Marzuki et al., "Pengembangan Sistem Login Hotspot dengan Perantara Sosial Media Strategi Pemasaran Menggunakan Metode Kombinasi SWOT Dan AHP (Studi Kasus : STMIK Pradnya Paramita)," 2015

[8] L. Peccati, M. D'Amico, and M. Cigola, "Linear algebra," in UNITEXT - La Matematica per il 3 piu 2, 2018. doi: 10.1007/978-3-030-02336-2_1.

[9] R. Munir, "KRIPTOGRAFI Kuliah Pengantar," 2019.

[10] D. P. Whitfield, "Redshank Tringa totanus flocking behaviour, distance from cover and vulnerability to sparrowhawk Accipiter nisus predation," J Avian Biol, vol. 34, no. 2, pp. 163–169, Jun. 2003, doi: 10.1034/j.1600-048X.2003.03065.x.

[11] Menezes, A J, and Van Oorsschot, "Handbook of Applied Cryptography," 1996. [Online]. Available: http://kickme.to/tiger/

[12] F. J. Och, "Minimum error rate training in statistical machine translation," 2003. doi: 10.3115/1075096.1075117.

[13] B. Schneier, Applied cryptography : protocols, algorithms, and source code in C. Wiley, 1996.

[14] R. K. Hasoun, S. Faris Khlebus, and H. Kadhim Tayyeh, "A New Approach of Classical Hill Cipher in Public Key Cryptography," 2021. [Online]. Available: http://www.ijnaa.semnan.ac.ir

[15] R. Gusmana, H. Haryansyah, and F. Fitria, "IMPLEMENTASI ALGORITMA AFFINE CIPHER DAN CAESAR CIPHER DALAM MENGAMANKAN DATA TEKS," Sebatik, vol. 26, no. 2, pp. 517–524, Dec. 2022, doi: 10.46984/sebatik.v26i2.2084.

[16] Stinson D R, "Cryptography Theory and Practice Fourth Edition," 2018.