Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
https://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/index
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893

Transformasi Digital Enkripsi Teks: Implementasi *Playfair Cipher* pada *Platform Google Colaboratory*

DOI: http://dx.doi.org/10.35889/jutisi.v14i2.2794

Muhlis Tahir[1], Hasan Basri[2], Ais Zulaikha Agustina[3*], Nofiyanti[4], Setyaning Puji Kinanti[5], Aditya Eka Putra[6]

Pendidikan Informatika, Universitas Trunojoyo Madura, Bangkalan, Indonesia
**e-mail Corresponding Author*: 220631100023@student.trunojoyo.ac.id

Abstract

Digital transformation requires a reliable information security system, especially in protecting text data on public networks. This study aims to implement and evaluate the classic Playfair Cipher algorithm using the Google Colaboratory platform. The method used is quantitative descriptive, with testing conducted on English-language text using the Python programming language. The results show that the algorithm is capable of encrypting and decrypting data accurately, with an average encryption processing time of 7.32 ms and decryption time of 10.86 ms. Security validation through frequency and bigram analysis proves the algorithm's effectiveness in obscuring the original text pattern. The conclusion of this study indicates that the Playfair Cipher algorithm remains relevant as an efficient, accurate, and practically integrable solution for simple text encryption on cloud platforms for educational and data security protection needs.

Keywords: *Text Encryption; Google Collaboratory; Data Security; Classical Cryptography; Playfair Cipher.*

Abstrak

Transformasi digital menuntut sistem keamanan informasi yang andal, khususnya dalam perlindungan data teks di jaringan publik. Penelitian ini bertujuan mengimplementasikan dan mengevaluasi algoritma klasik *Playfair Cipher* menggunakan platform *Google Colaboratory*. Metode yang digunakan adalah deskriptif kuantitatif, dengan pengujian dilakukan pada teks berbahasa Inggris menggunakan bahasa pemrograman Python. Hasil menunjukkan bahwa algoritma mampu mengenkripsi dan mendekripsi data secara akurat, dengan rata-rata waktu proses enkripsi 7,32 ms dan dekripsi 10,86 ms. Validasi keamanan melalui analisis frekuensi dan bigram membuktikan efektivitas algoritma dalam menyamarkan pola teks asli. Simpulan dari penelitian ini menunjukkan bahwa algoritma *Playfair Cipher* masih relevan sebagai solusi enkripsi teks sederhana yang efisien, akurat, dan dapat diintegrasikan secara praktis dalam *platform cloud* untuk kebutuhan edukasi dan perlindungan keamanan data.

Kata kunci: *Enkripsi Teks; Google Collaboratory; Keamanan Data; Kriptografi Klasik; Playfair Cipher.*

1. Pendahuluan

Kemajuan teknologi telah menghasilkan transformasi signifikan dalam berbagai aspek kehidupan manusia, mulai dari teknik berkomunikasi hingga cara menjalankan usaha. Di era digital saat ini, informasi bergerak dengan sangat cepat melalui jaringan internet, menciptakan arus data yang masif dan dinamis. Kondisi ini menuntut adanya sistem pengamanan data yang andal dan adaptif untuk melindungi informasi dari ancaman pencurian atau penyalahgunaan. *Kriptografi* sebagai ilmu dan seni mengamankan informasi melalui proses *enkripsi* menjadi pilar penting dalam menjaga kerahasiaan dan keutuhan data yang dikirim secara *online*[1]-[2]. Pentingnya tema ini diteliti karena perlindungan data yang lemah dapat berakibat pada kebocoran informasi, kerugian ekonomi, hingga pelanggaran privasi yang serius [3].

Namun, dalam praktiknya, pengiriman data teks melalui jaringan publik masih menyimpan berbagai kerentanan. Misalnya, dokumen yang tidak *terenkripsi* berisiko tinggi disadap dan

dibaca oleh pihak tidak berwenang selama proses transmisi berlangsung [4]. Selain itu, banyak metode *enkripsi modern* yang kompleks membutuhkan infrastruktur komputasi yang tinggi, sehingga kurang ramah bagi kalangan pelajar, peneliti pemula, atau institusi pendidikan dengan sumber daya terbatas. Oleh karena itu, diperlukan pendekatan yang efisien, mudah diimplementasikan, dan cukup aman untuk mengamankan data teks, terutama pada lingkungan akademik dan edukatif dengan keterbatasan perangkat keras.

Salah satu solusi yang ditawarkan adalah implementasi teknik *kriptografi* klasik, seperti *Playfair Cipher*, melalui platform berbasis *cloud* seperti *Google Colaboratory*. *Playfair Cipher* merupakan algoritma substitusi blok yang memproses pasangan huruf (*digraph*) dan dikenal memiliki keunggulan dalam mengacaukan pola bahasa yang umum sehingga lebih sulit dipecahkan dibandingkan teknik substitusi *monoalphabetic*[5],[6],[7]. Penggunaan *Google Colab* sebagai media penerapan algoritma ini memberikan efisiensi karena tidak membutuhkan instalasi lokal, mendukung kolaborasi *real-time*, serta memiliki dukungan *GPU/TPU* yang mempercepat proses komputasi[7][8],[9]. Penelitian sebelumnya juga menunjukkan bahwa *Playfair Cipher* lebih efektif dibanding *Shift Cipher* dalam menjaga keamanan data teks karena mampu mengurangi keefektifan analisis frekuensi[5]. Bahkan, teknik ini telah dimodifikasi untuk mengenkripsi huruf kapital, angka, dan simbol, menjadikannya lebih fleksibel dan relevan untuk kebutuhan saat ini[10]. Dengan pendekatan ini, diharapkan keamanan informasi dapat tetap terjaga tanpa mengorbankan keterjangkauan dan aksesibilitas teknologi.

Penelitian ini bertujuan untuk mengkaji dan mengimplementasikan algoritma *Playfair Cipher* melalui platform *Google Colaboratory* dalam konteks pengamanan data teks. Manfaat dari penelitian ini adalah untuk menyediakan alternatif solusi pengamanan data yang mudah, murah, dan efisien serta memberikan kontribusi terhadap pengembangan teknologi *kriptografi* edukatif yang dapat diakses oleh berbagai kalangan. Selain itu, penelitian ini diharapkan dapat mendorong pemanfaatan kembali *kriptografi* klasik dalam bentuk modern guna memenuhi kebutuhan keamanan informasi di era transformasi digital.

2. Tinjauan Pustaka

Penelitian mengenai teknik enkripsi teks telah banyak dilakukan oleh peneliti sebelumnya. Penelitian [1] mengembangkan teknik modifikasi untuk meningkatkan keamanan algoritma *Playfair Cipher* dengan menambahkan variasi pada proses substitusi huruf, serta melakukan pengujian efisiensi dan keamanannya melalui simulasi perangkat lunak berbasis Java. Hasilnya menunjukkan bahwa *Playfair Cipher* tetap dapat ditingkatkan untuk menghadapi ancaman *modern*. Sementara itu, [4] merancang aplikasi enkripsi-dekripsi berbasis *Playfair Cipher* untuk *file* teks menggunakan metode pengkodean langsung berbasis GUI, dengan fokus pada efisiensi proses dan kemudahan implementasi dalam sistem informasi sederhana.

Penelitian [5] melakukan analisis perbandingan antara teknik *Playfair* dan *Shift Cipher* dalam konteks keamanan data teks. Penelitian ini menggunakan pendekatan eksperimental dengan pengujian waktu eksekusi dan ketahanan terhadap analisis frekuensi. Hasilnya menunjukkan bahwa *Playfair Cipher* lebih unggul dalam menyamarkan pola teks asli. Penelitian [6] juga menyoroti efektivitas Playfair dalam menjaga kerahasiaan pesan melalui pengujian manual terhadap distribusi frekuensi karakter, meskipun tanpa dukungan platform komputasi modern. Adapun [7] mengkaji modifikasi pada metode *Playfair* untuk pengamanan data teks dengan pendekatan perancangan ulang matriks kunci dan penyisipan karakter khusus guna meningkatkan kerumitan proses kriptografi.

Berdasarkan kajian tersebut, penelitian ini menghadirkan perbedaan signifikan (*state of the art*) dalam beberapa aspek. Pertama, algoritma *Playfair Cipher* yang bersifat klasik tidak hanya diimplementasikan kembali, tetapi juga diintegrasikan dengan *platform cloud Google Colaboratory* yang mendukung eksekusi langsung tanpa instalasi lokal, sehingga meningkatkan aksesibilitas dan efisiensi. Kedua, penelitian ini tidak hanya menampilkan hasil enkripsi, tetapi juga mengukur performa waktu proses enkripsi-dekripsi dan menguji keamanan melalui analisis frekuensi dan bigram, yang belum dilakukan secara menyeluruh dalam penelitian-penelitian sebelumnya. Hal ini menjadi kebaruan (*novelty*) utama dari penelitian, yakni kombinasi antara metode kriptografi klasik dan validasi performa dalam konteks teknologi *cloud modern* yang mendukung pembelajaran, eksperimen, dan pengembangan kriptografi secara lebih luas dan aplikatif.

3. Metodologi

Penelitian ini menggunakan pendekatan deskriptif kuantitatif yang bertujuan untuk mengimplementasikan dan mengevaluasi algoritma enkripsi teks *Playfair Cipher* pada *platform* pemrograman berbasis *cloud*, yaitu *Google Colaboratory*. Teknik ini dipilih karena mampu memberikan gambaran konkret mengenai proses, efisiensi, dan hasil enkripsi teks dalam konteks transformasi digital menggunakan pendekatan klasik namun berbasis teknologi *modern*.

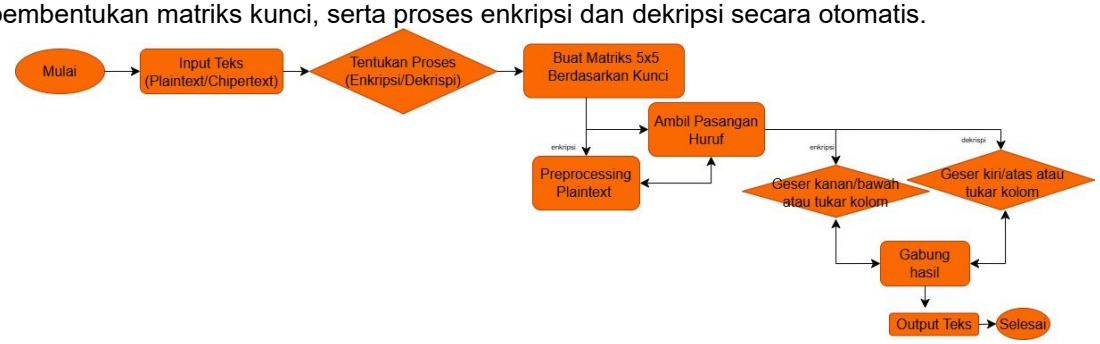
1) Objek Penelitian

Algoritma kriptografi klasik Playfair Cipher digunakan dalam lingkungan pemrograman Python dengan bantuan Google Colaboratory. Teks yang digunakan sebagai data uji adalah kalimat berbahasa Inggris yang terdiri dari berbagai panjang karakter untuk mengetahui pengaruh jumlah input terhadap kecepatan dan hasil enkripsi.

2) Tahapan Penelitian

Tahapan penelitian ini diawali dengan mengumpulkan referensi dari jurnal dan artikel yang membahas kriptografi klasik, khususnya teknik *Playfair Cipher*, serta *platform* pemrograman berbasis *cloud* seperti *Google Colab*. Setelah itu, dilakukan perancangan algoritma *Playfair Cipher* dengan menyusun algoritma enkripsi dan dekripsi berdasarkan aturan *Playfair Cipher*, termasuk pembentukan matriks 5x5, penggabungan pasangan huruf (digram), dan aturan substitusi berdasarkan posisi huruf dalam matriks.

Tahapan selanjutnya adalah implementasi dilakukan menggunakan bahasa *Python*. Proses ini meliputi input teks, pembersihan teks dari karakter tidak valid, pembentukan digram, pembentukan matriks kunci, serta proses enkripsi dan dekripsi secara otomatis.



Gambar 1. Alur proses enkripsi dan dekripsi

Salah satu teknik enkripsi dan dekripsi yang paling terkenal di dunia adalah *cipher Playfair*. Teknik playfair ini menggunakan matriks, di mana kunci yang telah ditetapkan[4]. Biasanya algoritma *Playfair Cipher* menggunakan tabel kunci 5x5 dengan jumlah karakter sebanyak 25 karakter[11]-[12], yaitu huruf A sampai huruf Z (pengecualian terhadap huruf J) seperti contoh dibawah ini:

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Gambar 2. Tabel Kunci 5x5

Dari tabel di atas, terlihat bahwa huruf J tidak ada, karena huruf J dianggap setara dengan huruf I, mengingat frekuensi kemunculannya yang paling rendah. Kunci yang diterapkan pada plainteks terdiri dari kata-kata tanpa adanya huruf yang diulang dalam kunci tersebut, contoh “MATAHARI” maka huruf yang *double* dihilangkan terlebih dahulu, menjadi “MATHRI”, kunci selanjutnya di masukkan satu persatu ke dalam table 5x5, selanjutnya sisa baris dan kolom yang kosong diisi oleh huruf secara urut dari baris pertama dahulu, huruf tidak ditulis kembali setelah muncul[13].

Berikut ini adalah beberapa aturan dari teknik *Playfair Cipher*[14]**:**

1. Huruf I digunakan untuk menggantikan huruf J dalam kalimat.
2. Apabila pasangan huruf memiliki huruf yang sama, letakkan huruf X atau Z di tengahnya.

3. Apabila jumlah huruf pada plaintext adalah ganjil, maka ditambah huruf X/Z untuk ditambahkan di akhir plaintext.

Apabila aturan di atas sudah dilakukan, maka diperluas rangkaian kunci dalam enkripsi *Playfair Cipher*[15]-[16].

1. Dalam kasus di mana dua huruf kunci yang identik ditemukan dalam satu baris, huruf di sebelah kanan huruf kunci tersebut akan menggantikan huruf sebelumnya.
2. Dalam kasus di mana dua huruf kunci yang sama berada dalam satu kolom, huruf di bawahnya akan menggantikan huruf sebelumnya.
3. Apabila 2 huruf tidak berada pada baris atau kolom yang sama, huruf pertama akan digantikan oleh huruf yang berada pada perpotongan antara baris pertama dan kolom kedua, dan huruf kedua akan digantikan oleh huruf yang berada pada titik keempat dari persegi panjang yang terbentuk oleh ketiga huruf tersebut.

Setelah implementasi selesai, dilakukan pengujian program dengan beberapa variasi panjang teks, serta pengamatan hasil keluaran (*output*) berupa *ciphertext* dan *plaintext*. Selain itu, dilakukan pengukuran waktu proses enkripsi dan dekripsi menggunakan modul *time* pada *Python*. Terakhir, dilakukan analisis hasil dengan menilai efisiensi algoritma berdasarkan waktu proses, tingkat keakuratan dekripsi, serta keterbacaan hasil enkripsi. Hasil juga dibandingkan dengan prinsip-prinsip dasar keamanan data seperti kerahasiaan dan keutuhan pesan.

4. Hasil dan Pembahasan

4.1 Hasil

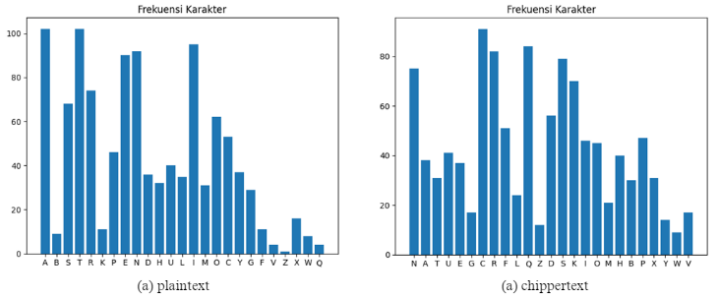
Untuk menguji performa algoritma *Playfair Cipher*, dilakukan proses enkripsi terhadap tiga sampel teks berbahasa Inggris dengan panjang karakter yang berbeda (100, 500, 1.000, 1.500, dan 2.000 karakter). Hasil enkripsi ditampilkan pada Tabel 1, dan waktu proses pengenkripsian dicatat menggunakan modul *time* dalam *Python*.

Tabel 1. Hasil uji performa enkripsi playfair cipher

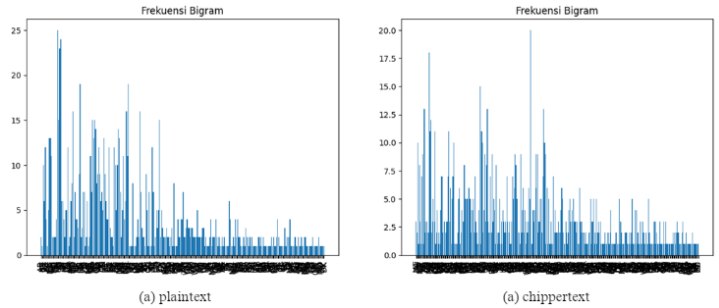
No	Panjang Karakter	Kunci	Waktu (ms)
1	100	unijoyo	1,1
2	500	unijoyo	3,3
3	1.000	unijoyo	7,2
4	1.500	unijoyo	10,4
5	2.000	unijoyo	14,6

Algoritma membentuk matriks 5x5 berdasarkan kunci yang diberikan oleh pengirim, yaitu "unijoyo", dan mengabaikan karakter 'j' dengan menggantinya menjadi 'i', sesuai aturan klasik Playfair.

Teks input disiapkan dengan membentuk pasangan karakter (*digraph*), menyisipkan huruf 'x' bila ditemukan karakter ganda dalam pasangan atau jika jumlah karakter ganjil. Setiap pasangan karakter kemudian diproses melalui matriks menggunakan prinsip dasar *Playfair Cipher*: pergeseran baris atau kolom untuk menghasilkan *ciphertext*. Algoritma hanya menghasilkan matriks kunci berdasarkan karakter unik dari kata kunci "unijoyo". Dengan metode ini, kunci dapat bervariasi tergantung entri pengguna, memberikan fleksibilitas sekaligus meningkatkan keamanan jika dikombinasikan dengan pengelolaan kunci yang baik. Keamanan terhadap *brute-force* meningkat seiring jumlah variasi kunci yang dapat dibentuk dari 25 huruf unik.



Gambar 3. Hasil tes analisis frekuensi karakter (a) *plaintext* dan (b) *ciphertext*



Gambar 4. Hasil pengujian bigram (a) plaintext dan (b) ciphertext

Untuk mengevaluasi keamanan dari sisi kriptanalisis, dilakukan dua jenis pengujian yaitu analisis frekuensi ditunjukkan pada gambar 2 dan analisis bigram ditunjukkan pada gambar 3. Tabel 2 menunjukkan bahwa setelah teks dienkripsi, distribusi karakter menjadi lebih merata, dengan pergeseran karakter dominan dari *plaintext* ke *ciphertext*.

Tabel 2. Hasil perbandingan analisis frekuensi tertinggi

Panjang karakter	Kunci	Frekuensi Tertinggi (Plaintext)		Frekuensi Tertinggi (Ciphertext)	
		Karakter	Frekuensi	Karakter	Frekuensi
100	unijoyo	E	80	I	57
500	unijoyo	E	356	U	242
1.000	unijoyo	E	717	B	459
1.500	unijoyo	E	1022	B	681
2.000	unijoyo	E	1346	B	892

Selanjutnya, Tabel 3 mengonfirmasi bahwa *Playfair Cipher* menyamarkan pola pasangan huruf yang umum muncul pada dataset teks.

Tabel 3. Hasil perbandingan analisis bigram tertinggi

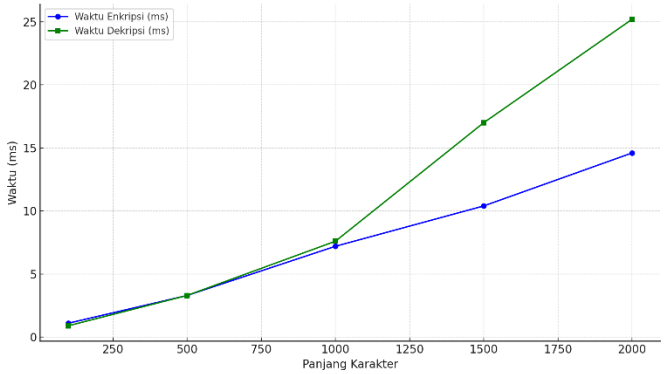
Panjang karakter	Kunci	Frekuensi Tertinggi (Plaintext)		Frekuensi Tertinggi (Ciphertext)	
		Karakter	Frekuensi	Karakter	Frekuensi
100	unijoyo	AN	15	AB	11
500	unijoyo	ST	59	BU	38
1.000	unijoyo	IN	136	YI	65
1.500	unijoyo	IN	208	OI	104
2.000	unijoyo	IN	269	OI	136

Pengujian waktu eksekusi dilakukan pada lima dataset dengan ukuran karakter berbeda. Hasil pengujian waktu enkripsi dan dekripsi disajikan pada Tabel 4 dan divisualisasikan pada Gambar 5.

Tabel 4. Hasil uji coba waktu enkripsi dan dekripsi

No	Panjang Karakter	Kunci	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)
1	100	unijoyo	1,1	0,9
2	500	unijoyo	3,3	3,3
3	1.000	unijoyo	7,2	7,6
4	1.500	unijoyo	10,4	17
5	2.000	unijoyo	14,6	25,2
Rata-rata			**7,32**	**10,86**

Gambar 5 menunjukkan bahwa waktu enkripsi dan dekripsi algoritma *Playfair Cipher* meningkat seiring dengan bertambahnya panjang karakter. Namun, kenaikan tersebut masih berada dalam rentang waktu yang sangat cepat dan efisien (rata-rata enkripsi 7,32 ms dan dekripsi 10,86 ms). Ini membuktikan bahwa algoritma *Playfair* tetap ringan dan layak digunakan untuk kebutuhan enkripsi teks sederhana meskipun ukuran data bertambah.



Gambar 5. Grafik hubungan antara panjang karakter dengan waktu enkripsi dan dekripsi

4.2 Pembahasan

Berdasarkan hasil pengujian yang telah dilakukan, algoritma *Playfair Cipher* terbukti mampu menyamarkan struktur karakter dan bigram dari teks asli secara efektif. Selain itu, algoritma ini juga menunjukkan tingkat keakuratan dekripsi yang mencapai 100%, sehingga dapat dipastikan bahwa data yang telah dienkripsi dapat dikembalikan ke bentuk aslinya tanpa kehilangan informasi. Dari segi performa waktu, *Playfair Cipher* mampu memproses data dengan cepat dan efisien, bahkan ketika digunakan untuk teks yang berjumlah lebih dari 2.000 karakter. Kecepatan ini menunjukkan bahwa algoritma ini sangat cocok diterapkan untuk kebutuhan enkripsi sederhana seperti pesan pribadi, catatan rahasia, atau aplikasi edukatif yang tidak menuntut sistem keamanan tingkat tinggi.

Temuan dalam penelitian ini juga menguatkan hasil dari beberapa penelitian terdahulu. Singh[1] menyatakan bahwa *Playfair Cipher* masih dapat ditingkatkan keamanannya dengan menggabungkannya bersama metode kriptografi lainnya. Penelitian ini membuktikan bahwa meskipun termasuk dalam kategori *cipher* klasik, *Playfair* tetap relevan digunakan sebagai dasar sistem keamanan data. Selain itu, penelitian oleh Sancaka dan Lusiana[4] juga menunjukkan efisiensi waktu yang sangat baik dari algoritma ini, dengan rata-rata waktu eksekusi di bawah 5 milidetik. Temuan ini selaras dengan hasil yang diperoleh dalam penelitian saat ini. Begitu pula dengan studi dari Siagian dan Indra[5] yang menilai bahwa *Playfair Cipher* merupakan salah satu algoritma kriptografi klasik paling efektif dalam hal penyamaran teks secara sederhana namun cepat. Tak hanya itu, hasil penelitian ini juga mendukung pandangan dari Wahyudi et al. [3] bahwa kombinasi *cipher* klasik mampu meningkatkan keamanan data, terutama dalam sistem dengan keterbatasan sumber daya.

5. Simpulan

Hasil pengujian menunjukkan bahwa algoritma *Playfair Cipher* memiliki kinerja yang cepat dan efisien, dengan rata-rata waktu enkripsi 7,32 ms dan dekripsi 10,86 ms. Validasi keamanan melalui analisis frekuensi dan bigram membuktikan bahwa algoritma mampu menyamarkan pola teks asli secara efektif, sehingga tahan terhadap analisis statistik dasar. Matriks kunci yang dibentuk dari karakter unik kata kunci juga meningkatkan variasi dan keamanan terhadap serangan brute-force. Dengan demikian, *Playfair Cipher* layak digunakan untuk kebutuhan enkripsi teks sederhana.

Daftar Referensi

[1] S. Singh, “A Novel Technique for Enhancement of the Security of Playfair Cipher,” *International Journal of Computer Engineering in Research Trends*, vol. 7, no. 1, pp. 8–12, 2020, doi: 10.22362/ijcert/2020/v7/i01/v7i102.

[2] M. Tahir, D. D. Andayani, D. Y. Cholili, D. I. Maulidia, N. W. Hidayatulloh, and A. Hasanah, *Keamanan Jaringan Komputer*, Cetakan I. Malang: PT. Literasi Nusantara Abadi Grup, 2023.

[3] E. N. Wahyudi *et al.*, “Peningkatan Keamanan Data Melalui Teknik Super Enkripsi Menggunakan Algoritma Vigenere dan Caesar,” *Jurnal Informatika Polinema*, vol. 10, no. 3, pp. 315–322, 2024.

[4] T. M. P. Sancaka and V. Lusiana, “Penerapan Metode Playfair Cipher Dalam Aplikasi Enkripsi-Dekripsi File Teks,” *Jurnal Ilmiah Elektronika dan Komputer*, vol. 15, no. 2, pp.

260–270, Dec. 2022, [Online]. Available: http://journal.stekom.ac.id/index.php/elkom□page260

[5] A. A. Siagian and Z. Indra, “Analisis Teknik Playfair dan Shift Cipher Sebagai Metode Kriptografi Klasik Untuk Keamanan Data,” *Jurnal Komputer dan Teknologi*, vol. 4, no. 1, pp. 13–19, 2025, doi: 10.58290/jukomte.

[6] L. N. Azizah, “How Can Playfair Cipher Secure Data?,” *Proceeding International Conference on Science and Engineering*, vol. 3, pp. 273–277, 2020.

[7] D. Susanti, “Analisis Modifikasi Metode Playfair Cipher Dalam Pengamanan Data Teks,” *Indonesian Journal of Data and Science*, vol. 1, no. 1, pp. 11–18, Mar. 2020.

[8] A. N. Nasution, A. Syahfitri, and Z. Indra, “Implementasi Algoritma Kriptografi Modern Melalui Google Colab: Studi Kasus AES dan RSA,” *MOTEKAR: Jurnal Multidisiplin Teknologi dan Arsitektur*, vol. 2, no. 2, pp. 841–845, Nov. 2024.

[9] R. Nazar, “Implementasi Pemrograman Python Menggunakan Google Colab,” *Jurnal Informatika dan Komputer*, vol. 15, no. 1, pp. 50–56, Jun. 2024.

[10] A. S. Ismaya, G. E. Yuliastuti, and A. Rachman, “Implementasi Metode Modifikasi Playfair Cipher Pada Data Pribadi Stakeholder di SMK Islam Al Futuhiyyah,” *Seminar Nasional Sains dan Teknologi Terapan XI*, pp. 1–8, 2023.

[11] B. Deepa, V. Maheswari, and V. Balaji, “An Efficient Cryptosystem Using Playfair Cipher Together with Graph Labeling Techniques,” *J Phys Conf Ser*, vol. 1964, no. 2, pp. 1–15, Jul. 2021, doi: 10.1088/1742-6596/1964/2/022016.

[12] N. Sugirtham *et al.*, “Modified Playfair for Text File Encryption and Meticulous Decryption with Arbitrary Fillers by Septenary Quadrate Pattern,” *International Journal of Networked and Distributed Computing*, vol. 12, no. 1, pp. 108–118, Jun. 2024, doi: 10.1007/s44227-023-00019-4.

[13] R. C. N. Santi, “Implementasi Algoritma Enkripsi Playfair pada File Teks,” *Jurnal Teknologi Informasi DINAMIK*, vol. 15, no. 1, pp. 27–33, Jan. 2020.

[14] A. M. Faadhil, D. I. Mulyana, G. Nawangsah, and L. S. Saptan, “Pengamanan Transkrip Mahasiswa Menggunakan Kriptografi Playfair Cipher,” *Jurnal Teknik Elektro dan Komputasi (ELKOM)*, vol. 4, no. 1, pp. 91–98, Mar. 2022, doi: 10.32528/elkom.v4i1.7117.

[15] L. Qurban, “Arabic and English Texts Encryption Using Modified Playfair Algorithm,” *Wasit Journal for Pure sciences*, vol. 3, no. 1, pp. 74–82, Mar. 2024, doi: 10.31185/wjps.285.

[16] M. M. Maha, M. Masuduzzaman, and A. Bhowmik, “An Effective Modification of Playfair Cipher With Performance Analysis Using 6X6 Matrix,” *ACM International Conference Proceeding Series*, pp. 1–6, Jan. 2020, doi: 10.1145/3377049.3377085.