Implementasi Metode Modifikasi Playfair Cipher Pada Data Pribadi Stakeholder di SMK Islam Al Futuhiyyah

Agam Sulaiman Ismaya[1], Gusti Eka Yuliastuti[2], Andy Rachman[3]
Institut Teknologi Adhi Tama Surabaya
e-mail: agamsulaiman711@gmail.com

ABSTRACT

The rapid development of information technology, especially in information systems, has brought about changes in various aspects, including in the data security sector. By utilizing information systems and technological advances, various methods can be used to secure data. This study employed the Playfair Cipher Cryptographic Method as a classic cryptographic method to secure stakeholder data at SMK Islam Al Futuhiyyah from rampant misuse of personal data. The Playfair Cipher algorithm that has been modified in this study can process letters, numbers, symbols, and capital letters, with an average execution time for the encryption algorithm of 0.013817753 seconds. However, there was a significant time difference at the decryption stage for the XLSX file format compared to the CSV file format. The decryption algorithm with the CSV file format took an average time of 0.017220058 seconds, and the decryption algorithm using the XLSX format took an average time of 1.08876535 seconds, so the time difference gained 1.071545292 seconds due to several factors such as algorithm optimization, hardware specifications, and system stability when the algorithm was run. The next test was carried out by measuring the percentage of the Avalanche Effect to measure the strength of the Playfair Cipher algorithm modified in this study. The results showed that this algorithm was strong in protecting data by 71.47%. Overall, the modifications made by researchers to the Playfair Cipher algorithm in this study have improved its ability to process various characters and improved data integrity.

Keywords: *avalanche effect, decryption, encryption, cryptography, Playfair cipher, execution time*

ABSTRAK

Perkembangan teknologi informasi yang pesat, terutama dalam bidang sistem informasi, telah membawa perubahan dalam berbagai aspek, terutama di sektor keamanan data. Dengan memanfaatkan sistem informasi dan kemajuan teknologi, berbagai metode dapat digunakan untuk mengamankan data. Metode Kriptografi Playfair Cipher, sebuah metode kriptografi klasik yang digunakan dalam penelitian ini untuk mengamankan data stakeholder di SMK ISLAM AL FUTUHIYYAH dari penyalahgunaan data pribadi yang marak terjadi. Algoritma Playfair Cipher yang telah dimodifikasi pada penelitian ini dapat memproses huruf, angka, simbol, dan huruf kapital, dengan waktu eksekusi untuk algoritma enkripsi dengan rata-rata 0,013817753 detik. Namun, terdapat perbedaan waktu yang mencolok pada tahap dekripsi untuk format file XLSX dibandingkan dengan format file CSV, dimana algoritma dekripsi dengan format file CSV membutuhkan waktu rata-rata 0,017220058 detik dan dekripsi dengan dormat XLSX membutuhkan waktu rata-rata 1,08876535 dengan selisih waktu 1,071545292 detik karena faktor seperti optimisasi algoritma, spesifikasi perangkat keras dan kestabilan sistem saat algoritma dijalankan. Untuk pengujian berikutnya dilakukan dengan mengukur persentase Avalanche Effect yang digunakan untuk mengukur kekuatan algoritma Playfair Cipher yang sudah dimodifikasi pada penelitian ini dan hasil menunjukkan bahwa algoritma ini kuat dalam melindungi data, dengan persentase sebesar 71,47%. Secara keseluruhan, modifikasi yang dilakukan oleh peneliti pada algoritma Playfair Cipher dalam penelitian ini telah meningkatkan kemampuannya untuk memproses berbagai karakter dan meningkatkan integritas data.

Kata kunci: Avalanche Effect, Dekripsi, Enkripsi, Kriptografi, Playfair Cipher, Waktu Eksekusi.

PENDAHULUAN

Penggunaan sistem informasi di negara-negara berkembang seperti Indonesia menghadapi tantangan dalam mengakses pengetahuan dan meningkatkan kualitas pendidikan [1]. Internet telah menjadi alat yang penting dalam komunikasi, kehidupan sehari-hari, dan pendidikan, dengan sekitar 3 miliar pengguna dalam dua dekade terakhir. [2]. Namun, internet juga menimbulkan tantangan keamanan baru, yang memerlukan penanganan kerentanannya terhadap serangan siber. [3]. Tergantung pada jenis data yang perlu dilindungi, ada banyak cara untuk menjaga keamanannya. Salah satu cara adalah dengan menggunakan metode penyandian, seperti Kriptografi. [4]. Salah satu contoh metode kriptografi, seperti Playfair Cipher, dimodifikasi untuk melindungi informasi digital yang disimpan dalam sistem. Algoritma Playfair Cipher menggunakan metode polygram cipher, memerlukan grid enkripsi 5x5 [5]. Kelebihan dari algoritma Playfair Cipher adalah penggunaan substitusi bigram , sehingga hasil enkripsi berupa pasangan huruf. Hal ini mempersulit analisis frekuensi terhadap metode tersebut [6].

SMK ISLAM AL FUTUHIYYAH, sebuah koleksi data pribadi dari siswa, orang tua, dan guru, membutuhkan digitalisasi dan keamanan untuk mencegah penyalahgunaan data. Peneliti memilih algoritma enkripsi simetris Playfair Cipher, namun kelemahannya adalah hasil dekripsi yang ambigu karena penggantian "J" dengan "I" dan penggunaan tabel 5x5 yang membatasi pilihan enkripsi. Untuk meningkatkan tingkat kerahasiaan data yang dienkripsi dengan metode Playfair Cipher, akan digunakan modifikasi metode Playfair Cipher seperti yang diajukan oleh Sumarsono et al. (2019). Modifikasi ini akan memperluas tabel Playfair Cipher dari 5x5 menjadi 5x19, dan mengubah tabel tersebut mengikuti urutan tabel ASCII serta menghilangkan penggantian "J" dengan "I."

TINJAUAN PUSTAKA

Enkripsi Playfair Cipher

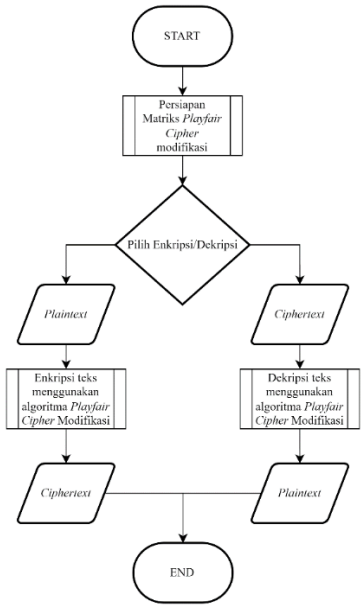
Charles Wheatstone, seorang fisikawan Inggris, menemukan sandi Playfair, yang dipopulerkan oleh Lyon Playfair pada tahun 1854. Awalnya, tentara Inggris menggunakan sandi ini untuk komunikasi taktis selama Perang Dunia I dan Perang Boer Kedua. Namun, setelah kemajuan teknologi, angkatan bersenjata berhenti menggunakan sandi ini karena munculnya teknologi enkripsi digital [8].

Algoritma Sandi Playfair adalah algoritma kunci simetris. Untuk menentukan matriks kunci 5x5, kunci hanya berisi huruf besar A hingga Z, dengan huruf J dihilangkan dari pernyataan. Susunan kunci di dalam tabel bujur sangkar tersebut diperluas Susunan kunci di dalam tabel persegi diperluas dengan menambahkan kolom keenam dan baris keenam, sehingga membuat analisis frekuensi kemunculan karakter menjadi sulit [9].

METODE

Gambaran Umum

Program yang dibuat menurut penelitian ini menggunakan algortima Playfair Cipher yang sudah dimodifikasi pada tahap enkripsi dan dekripsi sehingga dapat menghasilkan hasil ciphertext yang lebih teracak tanpa mengurangi tingkat integritas data yang telah terenkripsi. Penulis menyajikan garis besar yang komprehensif tentang sistem yang akan dibuat. Gambaran umumnya disajikan sebagai berikut :



Gambar 1 *Flowchart* Gambaran Umum Sistem

HASIL DAN PEMBAHASAN

Peneliti melakukan pengujian terhadap algortima yang sudah diterapkan dalam melakukan enkripsi dan dekripsi terhadap data yang didapat, yaitu dengan melakukan pengujian terhadap performanya *(Execution Time*) dan keamanannya (*Avalanche Effect*). Semua pengujian dilakukan menggunakan 1 kunci yaitu :

agam$2a$12$nf1jDmbQ24j3XE0LXYMZWOecmwiZ/eW2.KkjJ.HgnPfrXSeON0/au

1. Execution Time

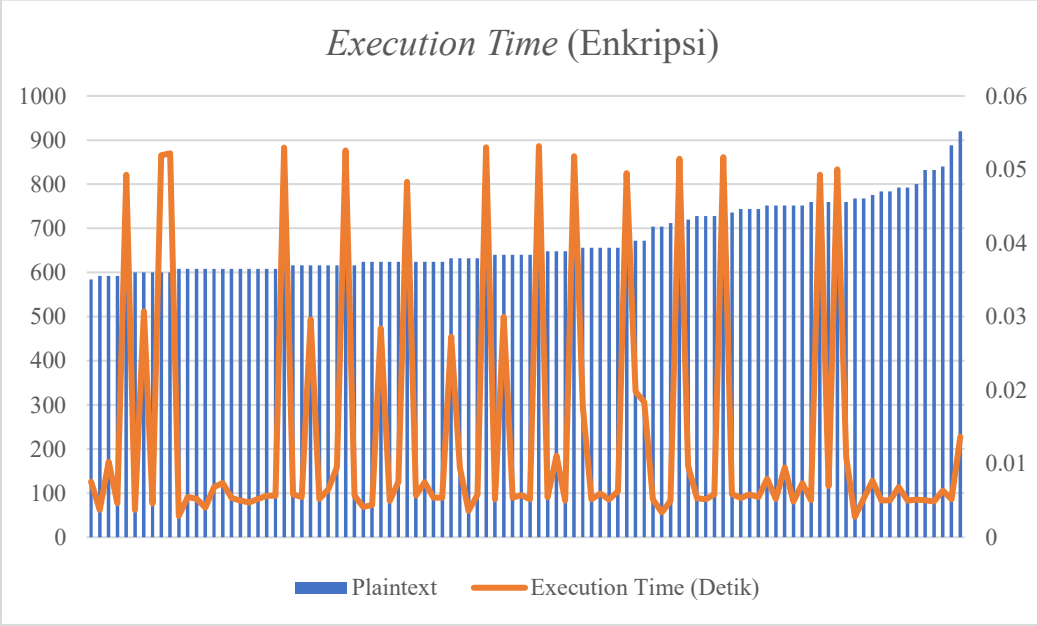
Perhitungan dari *Execution Time* akan dibagi menjadi 2 bagian yaitu *Execution Time* pada bagian enkripsi dan dekripsi.

1. Enkripsi
   Selama tahap enkripsi, data yang diproses diatur dalam satu baris data, yang mencakup berbagai informasi yang bersifat personal mengenai seorang siswa. Ini mencakup NISN, NIS, nama, jenis kelamin, tempat lahir, tanggal lahir, NIK, Nomor Kartu Keluarga, dan Nomor Seri Ijazah. Tabel berikut menampilkan data Execution Time yang tercatat dari proses enkripsi :

Tabel 1. *Execution Time* (Enkripsi)

No.	Panjang Bit *Plaintext*	Execution Time (Detik)
1	752	0,0079684
2	792	0,0068117
3	784	0,0049813

No.	Panjang Bit *Plaintext*	Execution Time (Detik)
4	888	0,0051473
5	840	0,0063587
6	920	0,0136684
7	832	0,0050255
8	832	0,0048399
9	656	0,0178681
10	656	0,0051698



Gambar 2. *Execution Time (Encryption)*

Dari Tabel 1 dan Gambar 2, Peneliti menemukan bahwa terdapat fluktuasi waktu dengan maksimal **0,0531834** pada data berukuran 640-bit, dengan rata-rata dari waktu Execution Time yaitu **0,013817753**, karena tidak ada keselarasan perbesaran dari Execution Time dengan panjang bit dari Plaintext maka dapat diperkirakan bahwa fluktuasi tersebut disebabkan oleh keadaan sistem yang kurang stabil pada saat menjalankan algoritma enkrpsi.

2. Dekripsi

Selama proses dekripsi, semua data dalam database diambil dan didekripsi. Hal ini membuat tahap dekripsi berbeda dari tahap enkripsi, karena proses dekripsi melibatkan pemrosesan seluruh data dan memerlukan waktu yang hampir sama dengan proses enkripsi, tetapi untuk seluruh database. Oleh karena itu, peneliti akan melakukan proses dekripsi sebanyak tiga kali dengan database yang memiliki 5, 10, 20, dan 100 entri data,

secara berurutan, untuk mengetahui berapa lama rata-rata yang dibutuhkan dalam tahap dekripsi :

Tabel 2. *Execution Time* (Dekripsi) 5 Baris

No	Execution time File .csv	Execution time File .xlsx
1.	0,0167187	1,2873954
2.	0,0052668	0,9126944
3.	0,0060639	0,875734

Tabel 3. *Execution Time* (Dekripsi) 10 Baris

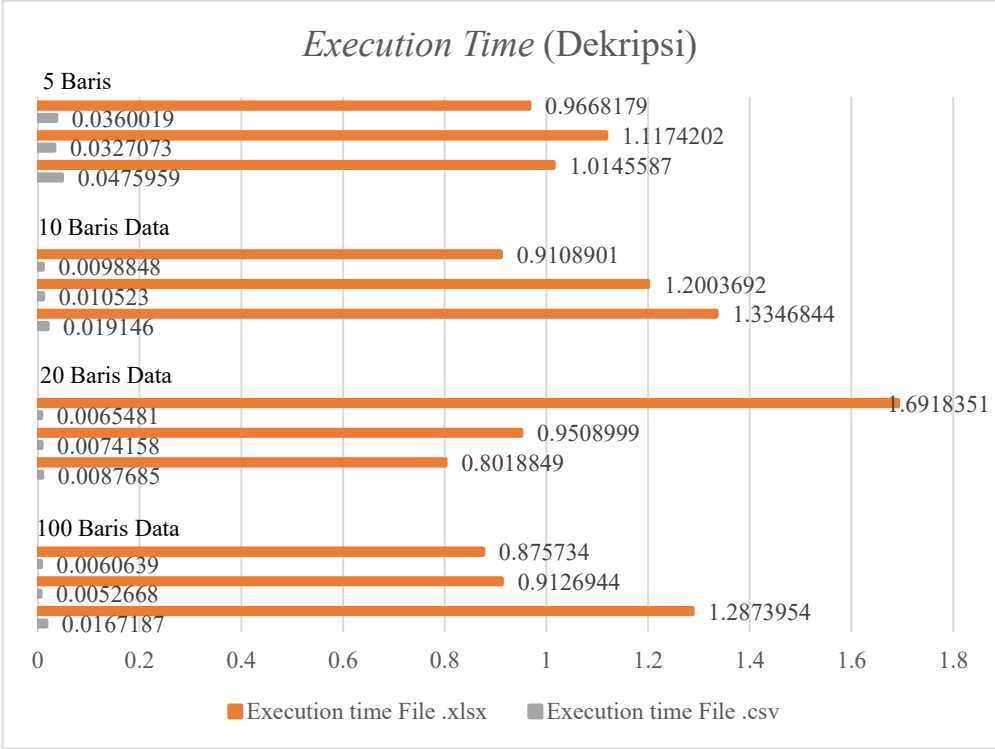
No	Execution time File .csv	Execution time File .xlsx
1.	0,0087685	0,8018849
2.	0,0074158	0,9508999
3.	0,0065481	1,6918351

Tabel 4. *Execution Time* (Dekripsi) 20 Baris

No	Execution time File .csv	Execution time File .xlsx
1.	0,019146	1,3346844
2.	0,010523	1,2003692
3.	0,0098848	0,9108901

Tabel 5. *Execution Time* (Dekripsi) 100 Baris

No	Execution time File .csv	Execution time File .xlsx
1.	0,0475959	1,0145587
2.	0,0327073	1,1174202
3.	0,0360019	0,9668179



Gambar 3. *Execution Time (Decryption)*

Dari Tabel 2 – 5 dan Gambar 3, Peneliti menemukan bahwa tidak ada fluktuasi lama waktu yang signifikan pada Execution Time dari file berformat CSV, namun terdapat fluktuasi waktu sekitar 1,6 pada format file XLSX pada file yang memiliki 20 baris data. Ditemukan bahwa rata-rata waktu algoritma dekripsi untuk file berformat CSV adalah **0,017220058** detik dan rata-rata waktu algortma dekripsi untuk file berformat XLSX adalah **1,08876535** detik, dengan selisih waktu yang dibutuhkan untuk melakukan dekripsi pada kedua format yaitu **1,071545292** detik. Peneliti menemukan bahwa tidak ada keselarasan dari penambahan ukuran data dengan waktu Execution Time yang dapat diartikan bahwa fluktuasi waktu dapat disebabkan oleh sistem yang kurang stabil saat menjalankan algoritma dekripsi.

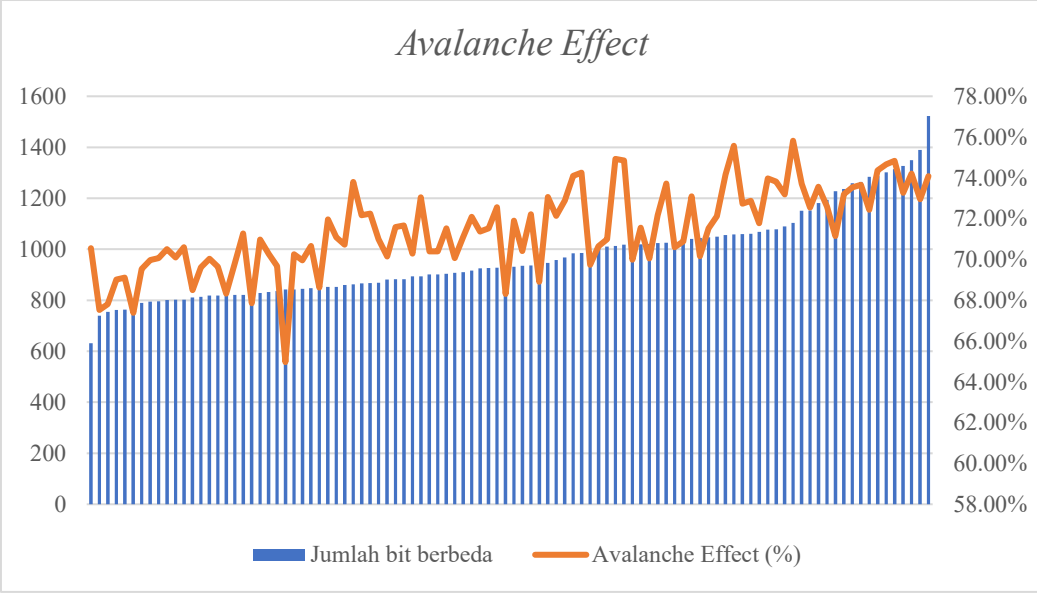
2. Avalanche Effect

Pengujian Avalanche Effect dilakukan pada saat data sudah terenkripsi lalu dilakukan dekripsi, dengan demikian data dapat dibandingkan dari bentuk plaintext dengan bentuk ciphertext-nya. Berikut merupakan tabel yang berisikan data siswa beserta nilai Avalanche Effect :

Tabel 6. *Avalanche Effect*

No	Jumlah Bit Berbeda	Avalanche Effect (%)
1	1181	73,57%
2	1259	73,54%
3	1314	74,83%

No	Jumlah Bit Berbeda	Avalanche Effect (%)
4	1389	72,95%
5	1522	74,08%
6	1287	74,36%
7	1350	74,21%
8	1025	73,73%
9	1151	73,71%
10	1056	74,16%



Gambar 4. *Avalanche Effect*

Dari Tabel 6 dan Gambar 4, didapati bahwa rata-rata hasil pengujian *Avalanche Effect* yang dilakukan oleh peneliti adalah **71,47%**. Dapat dilihat bahwa ada keselarasan dari kenaikan jumlah bit yang berbeda dengan persentase *Avalanche Effect* yang menunjukkan bahwa pada setiap panjang bit baris data maka ada batas persentase *Avalanche Effect* yang akan didapatkan. Dengan persentase *Avalanche Effect* paling tinggi yaitu **75,82%** dan persentase paling rendah yaitu **64,97%**.

KESIMPULAN

Berdasarkan penelitian dan pengujian yang telah dilakukan, dapat diambil beberapa kesimpulan sebagai berikut ini :

1. Penelitian ini telah memodifikasi algoritma *Playfair Cipher* untuk mengenkripsi huruf, angka, simbol, dan huruf kapital. Integritas data meningkat setelah proses enkripsi. Algoritma *Playfair Cipher* asli hanya mampu mengenkripsi huruf dan memiliki integritas data yang kurang baik. Versi yang telah ditingkatkan dalam penelitian ini lebih serbaguna dan aman untuk mengenkripsi karakter lebih banyak sambil tetap menjaga integritas data.
2. Fase enkripsi memerlukan waktu **0.013817753** detik, sedangkan fase dekripsi memerlukan waktu **0.017220058** detik untuk setiap jenis file CSV. Namun, saat mendekripsi file XLSX, algoritma memerlukan waktu **1.08876535** detik, yang merupakan peningkatan yang

signifikan. Dekripsi XLSX memerlukan waktu **1.071545292** detik lebih lama dibandingkan dengan CSV. Perbedaan ini disebabkan oleh optimisasi algoritma, spesifikasi perangkat keras, dan optimisasi lainnya.

3. Algoritma *Playfair Cipher* yang dimodifikasi dalam penelitian ini memiliki persentase *Avalanche Effect* sebesar **50%**, menunjukkan perlindungan data yang kuat. Menurut hasil penelitian, metode ini memiliki Avalanche Effect sebesar **71,47%.**

DAFTAR PUSTAKA

[1] M. Aziz Choiri, A. Rachman, A. Purwadi, and A. K. Salim, "Rancang Bangun Sistem Informasi Perpustakaan Sekolah Berbasis Web di SMK Islam Al-Futuhiyyah Menggunakan Model Waterfall," *Prosiding Seminar Nasional Teknik Elektro, Sistem Informasi, Dan Teknik Informatika (SNESTIK)*, vol. 1, no. 1, pp. 197–206, Jun. 2021, doi: 10.31284/p.snestik.2021.1798.

[2] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[3] M. Ocka Dharma Putra, A. Rahman, A. Azhari, and D. Redaksi, "PENGGUNAAN VIRTUAL PRIVATE NETWORK(VPN) PADA PT SEMEN BATURAJA (PERSERO)TBK," *JURNAL INTECH*, vol. 3, no. 1, pp. 17–21, May 2022.

[4] C. Nurina Prabiantissa, G. E. Yuliastuti, S. Agustini, and D. H. Sulaksono, "Proteksi Data X-Ray Paru-Paru Pasien COVID-19 menggunakan Algoritma Rivest Shamir Adleman dan Algoritma Enkripsi Rubic Cube Principle," *Prosiding Seminar Nasional Sains dan Teknologi Terapan*, vol. 1, no. 1, pp. 93–100, 2020.

[5] S. Dewi Br Surbakti, "Implementasi Algoritma Playfair Cipher pada Penyandian Data," *Jurnal Teknik Informatika Unika Santo Thomas*, vol. 4, no. 2, pp. 116–123, 2019, doi: https://doi.org/10.17605/jti.v4i2.42.

[6] Galih Agustian Perdana, Carudin, and R. Mayasari, "Implementasi Algoritma Kriptografi Playfair Cipher untuk Mengamankan Data Aset," *Jurnal Informatika Polinema*, vol. 7, no. 2, pp. 109–114, Feb. 2021, doi: 10.33795/jip.v7i2.394.

[7] Sumarsono, M. Anshari, and A. Mujahidah, "Expending Technique Cryptography for Plaintext Messages by Modifying Playfair Cipher Algorithm with Matrix 5 x 19," in *2019 International Conference on Electrical Engineering and Computer Science (ICECOS)*, IEEE, Oct. 2019, pp. 10–13. doi: 10.1109/ICECOS47637.2019.8984560.

[8] 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, doi: 10.33096/ijodas.v1i1.4.

[9] I. Kurniawan, "PERANCANGAN APLIKASI UNTUK KEAMANAN FOLDER DENGAN ALGORITMA PALY FAIR," *Jurnal Informatika Kaputama (JIK)*, vol. 3, no. 1, pp. 1–5, 2019, doi: https://doi.org/10.1234/jik.v3i1.131.