Terbit *online* pada laman: http://jurnal.utu.ac.id/JTI

Jurnal Teknologi Informasi

ISSN (Online): 2829-8934

Pengaruh Lama Waktu Enkripsi Terhadap Kombinasi Gronsfeld Cipher dengan Playfair Cipher

Abdurrahman Ridho[1], Andriani Putri[2], Hayatun Maghfirah[3]
[1,2,3] Teknologi Informasi, Universitas Teuku Umar, Aceh Barat, Indonesia
Email: [1]abdurrahman.ridho@utu.ac.id

INFORMASI ARTIKEL

Riwayat Artikel:
Diterima: 09 Mei 2023
Revisi: 26 Mei 2023
Diterbitkan: 30 Mei 2023

Kata Kunci:
Kriptografi
Teks
Gronsfeld Cipher
Playfair Cipher
Python

ABSTRAK

Era digital saat ini, keamanan data semakin penting. Salah satu cara untuk mengamankan data adalah dengan menggunakan teknik enkripsi. Penelitian ini berfokus pada implementasi enkripsi teks dengan menggabungkan dua teknik enkripsi, yaitu Gronsfeld Cipher dan Playfair Cipher, menggunakan bahasa pemrograman Python. Gronsfeld Cipher digunakan sebagai teknik enkripsi pertama untuk mengacak urutan karakter pada plaintext. Sementara itu, Playfair Cipher digunakan sebagai teknik enkripsi kedua untuk mengenkripsi hasil dari enkripsi pertama. Dengan menggabungkan kedua teknik enkripsi ini, diharapkan dapat meningkatkan keamanan data dan membuat teks hasil lebih sulit dibaca oleh pihak yang tidak berwenang. Hasil menunjukkan bahwa enkripsi menggunakan kedua teknik enkripsi ini dapat dilakukan dengan baik dan menghasilkan ciphertext yang tidak dapat dibaca oleh pihak yang tidak berwenang. Selain itu, menggunakan kunci yang berbeda untuk setiap teknik enkripsi dapat meningkatkan keamanan data lebih lanjut.

1. Pendahuluan

Ada banyak jenis teknik enkripsi yang tersedia untuk mengamankan data, salah satunya adalah Gronsfeld Cipher. Gronsfeld Cipher adalah jenis cipher yang mengenkripsi pesan dengan menggeser setiap huruf pesan asli sesuai dengan nomor kunci. Teknik ini mirip dengan Caesar Cipher, namun menggunakan kunci yang terdiri dari beberapa digit angka.

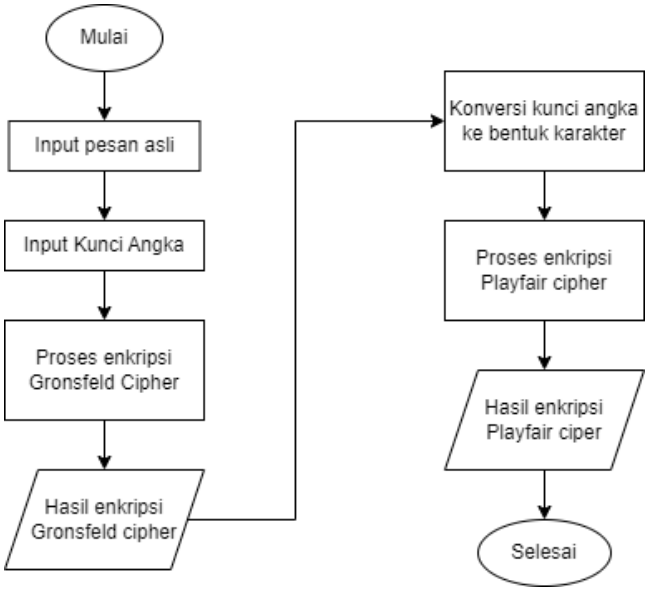
Namun, walaupun Gronsfeld Cipher dapat digunakan untuk mengenkripsi pesan, masih ada celah keamanan yang dapat dimanfaatkan oleh penyerang untuk membobolnya. Oleh karena itu, dibutuhkan teknik enkripsi lain yang dapat bekerja sama dengan Gronsfeld Cipher untuk meningkatkan keamanan data. Salah satu teknik enkripsi yang dapat digunakan bersama dengan Gronsfeld Cipher adalah Playfair Cipher. Playfair Cipher [1], adalah jenis cipher yang mengenkripsi pesan menggunakan tabel matrik [2], dengan membagi pesan asli menjadi pasangan dua huruf dan menggantikan setiap pasangan huruf dengan pasangan huruf lainnya yang telah diacak.

Penelitian terdahulu terkait penggunaan Play Fair cipher diantaranya dengan melakukan modifikasi metode tabel play fair cipher[2]. Serta penelitian lainnya yang menggunakan sistem hybrid [3] Penelitian terdahulu lainnya telah melakukan percobaan dengan melakukan kombinasi-kombinasi pada cipher [3-6], Baik perubahan metode maupun penggabungan atau kombinasi cipher menjadi landasan dilakukannya penelitian ini dengan menggabungkan dua teknik enkripsi, yaitu Gronsfeld Cipher dan Playfair Cipher, menggunakan bahasa pemrograman Python. Dengan menggabungkan kedua teknik enkripsi ini, diharapkan dapat meningkatkan keamanan data dan membuat teks hasil lebih sulit dibaca oleh pihak yang tidak berwenang.

Dalam penelitian ini, akan digunakan bahasa pemrograman Python untuk mengimplementasikan kedua teknik enkripsi. Python dipilih karena merupakan bahasa pemrograman yang mudah dipahami dan memiliki banyak modul yang dapat digunakan untuk implementasi enkripsi. Selain itu, Python juga dapat dijalankan di berbagai platform, sehingga dapat digunakan oleh banyak pengguna dari berbagai sistem operasi.

2. Metodologi Penelitian

Metode yang digunakan dalam penelitian ini adalah dengan membuat fungsi enkripsi menggunakan kedua teknik enkripsi tersebut. Fungsi enkripsi akan menerima input plaintext, kunci, dan menghasilkan ciphertext sebagai output. Selain itu, akan dilakukan pengujian pada beberapa contoh plaintext dan kunci yang berbeda untuk memastikan bahwa enkripsi dapat dilakukan dengan baik dan menghasilkan ciphertext yang tidak dapat dibaca oleh pihak yang tidak berwenang sehingga tercipta proses berbagi data yang nyaman dan aman [6]. Hasil yang diharapkan pada penelitian yang menggunakan kombinasi kedua teknik enkripsi[7], yaitu Gronsfeld Cipher dan Playfair Cipher, dapat dilakukan dengan baik dan menghasilkan ciphertext yang tidak dapat dibaca oleh pihak yang tidak berwenang. Selain itu, penggunaan kunci yang berbeda untuk setiap teknik enkripsi dapat meningkatkan keamanan data



Gambar1. Diagram alur proses enkripsi menggunakan kombinasi cipher

3. Hasil dan Pembahasan

Kombinasi kedua cipher yaitu Gronsfeld Cipher dengan Playfair Cipher menghasilkan hasil enkripsi yang lebih sulit untuk dipecahkan bila dibandingkan dengan cipher yang berjalan sendiri untuk menghasilkan cipherteks dari plainteks yang dimasukkan oleh pengguna. Implementasi yang dilakukan menggunakan bahasa pemrograman python. Kunci yang digunakan pada penelitian ini hanya menggunakan satu buah kunci yang dimasukkan di awal enkripsi menggunakan Gronsfeld Cipher. Sementara pada playfair cipher menggunakan kunci berupa rangkaian teks. Namun pada penelitian ini dilakukan pengubahan angka menjadi karakter huruf ketika melakukan enkripsi menggunakan Playfair Cipher.

Percobaan pertama dilakukan dengan melakukan input string berupa rangkaian karakter ‘universitas teuku umar’, dengan kunci angka 123. Hasil enkripsi menunjukkan rangkaian karakter menjadi VPLWGUTKWBUWFWNVWPBT. Gronsfeld cipher memiliki keunikan berupa tidak mengenal adanya spasi antar karakter, sehingga karakter yang dimasukkan dengan spasi akan menghasilkan cipherteks tanpa spasi. Cipherteks tersebut kemudian di enkripsi menggunakan Playfair cipher sehingga menghasilkan rangkaian teks ZLMVKRUIBGRZGVLXZMDR. Pada percobaan pertama dengan

menghitung byte pada plainteks adalah 2272 bytes, dan lama proses berjalan untuk melakukan enkripsi dua kali baik itu menggunakan Gronsfeld dan kemudian Playfair cipher adalah 2999.305 mikrodetik.

```
Masukkan teks: universitas teuku umar
masukkan sejumlah angka sebagai kunci: 123
Plaintext:  universitas teuku umar
Ciphertext:  VPLWGUTKWBUWFWNVWPBT
-----------------------------------
Plaintext:  VPLWGUTKWBUWFWNVWPBT
Ciphertext Playfair:  ZLMVKRUIBGRZGVLXZMDR
Lama proses:  2999.3057250976562 mikrodetik
Jumlah nilai byte plainteks:  2272
```

Gambar 2. Hasil enkripsi percobaan pertama dengan kombinasi cipher

Percobaan kedua dilakukan dengan melakukan input string rangkaian karakter ‘universitas teuku umar’ dengan kunci 1234, dari hasil percobaan kedua menghasilkan lama proses yang sama yaitu 2999.305 mikrodetik dengan jumlah byte plainteks 2272 bytes.

```
Masukkan teks: universitas teuku umar
masukkan sejumlah angka sebagai kunci: 1234
Plaintext:  universitas teuku umar
Ciphertext:  VPLZFTVMUCVXFWNYVODV
-----------------------------------
Plaintext:  VPLZFTVMUCVXFWNYVODV
Ciphertext Playfair:  ZLPVIQWLTEWYGVOXYLFD
Lama proses:  2999.544143676758 mikrodetik
Jumlah nilai byte plainteks:  2272
```

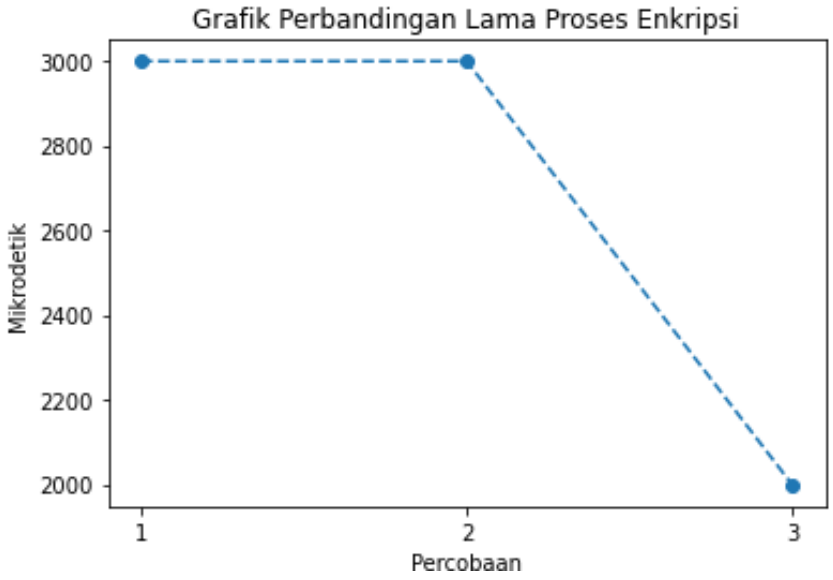
Gambar 3. Hasil enkripsi percobaan kedua dengan kombinasi cipher

Percobaan ketiga dilakukan dengan menambahkan kunci menjadi 5 karakter yaitu 12345 dengan rangkaian karakter pesan asli yang sama yaitu ‘universitas teuku umar’. Hasil percobaan ketiga menunjukkan lama proses yang lebih cepat yaitu 1998.186 mikrodetik dengan jumlah bytes pesan asli yang tetap 2272 bytes.

```
Masukkan teks: universitas teuku umar
masukkan sejumlah angka sebagai kunci: 12345
Plaintext:  universitas teuku umar
Ciphertext:  VPLZJSULXFTVHYPVWPEW
-----------------------------------
Plaintext:  VPLZJSULXFTVHYPVWPEW
Ciphertext Playfair:  ZLPVHTQPVHQYIXLZZMCZ
Lama proses:  1998.1861114501953 mikrodetik
Jumlah nilai byte plainteks:  2272
```

Gambar 4. Hasil enkripsi percobaan ketiga dengan kombinasi cipher

Ketiga percobaan yang dilakukan menghasilkan lama proses yang tidak terpengaruh oleh panjang kunci. Pada percobaan pertama dan kedua didapatkan hasil lama waktu yang sama, sementara pada percobaan ketiga dengan kunci sebanyak 5 karakter didapatkan hasil lama proses enkripsi yang lebih cepat.



Gambar 5. Diagram garis perbandingan hasil enkripsi ketiga percobaan pada sesi 1

Rata-rata waktu pada tiga percobaan pertama adalah 2665.599 mikrodetik, dengan panjang kunci yang ditambah 1 karakter di tiap percobaan.

Tabel 1. Tabel Rata-Rata Waktu Lama Proses Percobaan Sesi 1

Percobaan	**Panjang Kunci**	**Lama Proses (Mikrodetik)**
1	3 angka	2999.305
2	4 angka	2999.305
3	5 angka	1998.186
Rata-rata		2665.599

Sesi 2 percobaan berikutnya menggunakan pesan asli yang lebih singkat. Pesan asli yang dimasukkan pada percobaan ini menggunakan kombinasi rangkaian karakter ‘utu’, dengan tetap menggunakan kombinasi rangkaian kunci berupa angka 123 dan tetap menggunakan enkripsi Gronsfeld cipher dengan Playfair Cipher.

```
Masukkan teks: utu
masukkan sejumlah angka sebagai kunci: 123
Plaintext:  utu
Ciphertext:  VVX
-------------------------------------
Plaintext:  VVX
Ciphertext Playfair:  WWYY
Lama proses:  7726.192474365234 mikrodetik
Jumlah nilai byte plainteks:  350
```

Gambar 6. Hasil enkripsi percobaan 1 sesi 2

Hasil percobaan menunjukkan lama proses adalah 7726.192 mikrodetik dengan jumlah nilai bytes pada pesan asli sebesar 350 bytes. Percobaan dilanjutkan dengan menambahkan karakter pada kunci menjadi 1234.

```
Masukkan teks: utu
masukkan sejumlah angka sebagai kunci: 1234
Plaintext:  utu
Ciphertext:  VVX
-------------------------------------
Plaintext:  VVX
Ciphertext Playfair:  WWYY
Lama proses:  4196.643829345703 mikrodetik
Jumlah nilai byte plainteks:  350
```

Gambar 7.Hasil enkripsi percobaan 2 sesi 2

Pada percobaan 2 sesi 2 menunjukkan hasil berupa penurunan lama proses menjadi 4196.643 mikrodetik bila dibandingkan dengan percobaan sebelumnya pada sesi yang sama yaitu 7726.192 mikrodetik. Dengan penambahan karakter pada kunci dan dengan pesan asli yang sama. Percobaan 3 dalam sesi 2 dilakukan dengan menambahkan kembali 1 karakter pada kunci, sehingga kunci menjadi 12345

```
Masukkan teks: utu
masukkan sejumlah angka sebagai kunci: 12345
Plaintext:  utu
Ciphertext:  VVX
-------------------------------------
Plaintext:  VVX
Ciphertext Playfair:  WWYY
Lama proses:  5816.936492919922 mikrodetik
Jumlah nilai byte plainteks:  350
```

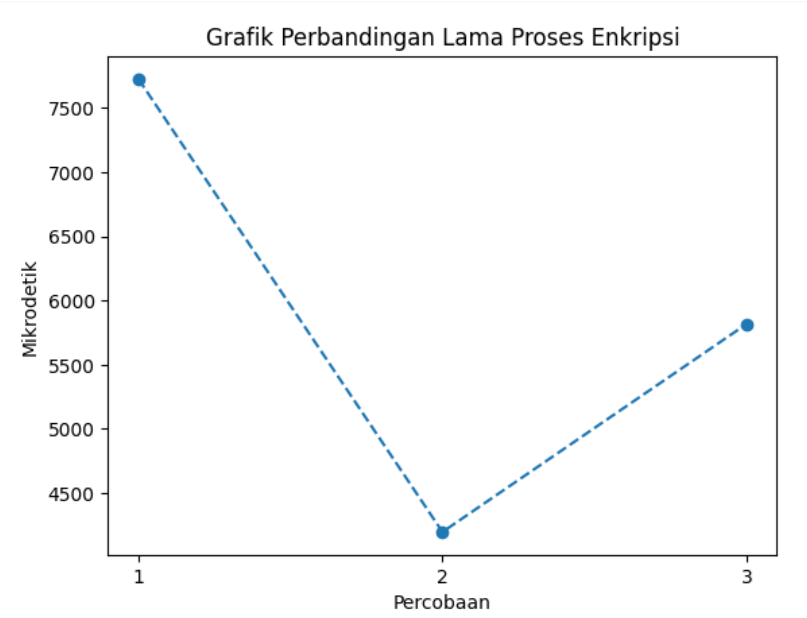
Gambar 8. Hasil enkripsi percobaan 3 sesi 2

Percobaan 3 sesi 2 menunjukkan adanya peningkatan lama proses dibandingkan dengan percobaan 2 sesi 2 yang naik menjadi 5816.936 mikrodetik. Menunjukkan adanya peningkatan lama waktu bila dibandingkan dengan percobaan 2 sesi 2, namun tetap dibawah lama proses yang terjadi pada percobaan 1 sesi 2.

Tabel 2. Tabel Rata-Rata Waktu Lama Proses Percobaan Sesi 2

Percobaan	**Panjang Kunci**	**Lama Proses**
1	3 angka	7726.192
2	4 angka	4196.643
3	5 angka	5816.936
Rata-rata		5913.257

Sesi 2 percobaan pada penelitian ini mendapatkan hasil rata-rata lama proses enkripsi dengan menggunakan kombinasi 2 buah cipher adalah 5193.257 mikrodetik. Dengan adanya perubahan lama proses yang terjadi pada setiap percobaan.



Gambar 9. Diagram garis perbandingan hasil enkripsi ketiga percobaan pada sesi 2

Diagram garis menunjukkan adanya penurunan lama waktu proses enkripsi menggunakan kombinasi 2 buah cipher dengan pesan asli yang sama pada ketiga percobaan namun menggunakan kunci yang ditambahkan 1 karakter pada setiap percobaan. Hasil ini menunjukkan bahwa adanya kemungkinan faktor lain yang mempengaruhi cepat dan lambatnya proses enkripsi selain dari pada jumlah bytes, kunci dan pesan asli.

4. Kesimpulan

Penelitian ini dilakukan untuk menghitung lama proses enkripsi yang terjadi pada kombinasi Gronsfeld cipher dengan Playfair Cipher. Percobaan dilakukan dengan menggunakan 2 sesi percobaan yang didalamnya terdapat 3 percobaan dengan sedikit modifikasi pada sampel di tiap percobaanya. Hasil yang didapatkan adalah bahwa lama proses enkripsi menggunakan gabungan cipher ini memiliki faktor lain yang mempengaruhi, hal tersebut dibuktikan dengan beberapa percobaan menunjukkan penurunan lama waktu proses disaat karakter pada kunci dinaikkan bila dibandingkan dengan kunci yang lebih pendek pada percobaan sebelumnya. Faktor yang mempengaruhi cepat dan lambatnya proses enkripsi tidak terbatas pada jumlah karakter dan ukuran bytes karakter yang diinput baik pada pesan asli maupun kunci yang digunakan.

Daftar Pustaka

[1] A. Hariati, K. Hardiyanti, and W. E. Putri, “Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks,” *Sinkron*, vol. 2, no. 2, pp. 13–17, 2018, [Online]. Available: https://jurnal.polgan.ac.id/index.php/sinkron/index

[2] D. Susanti, “Analisis Modifikasi Metode Playfair Cipher Dalam Pengamanan Data Teks,” *Indones. J. Data Sci.*, vol. 1, no. 1, pp. 11–18, 2020, doi: 10.33096/ijodas.v1i1.4.

[3] R. K. Salih and M. S. Yousif, “Hybrid encryption using playfair and RSA cryptosystems,” *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 2, pp. 2345–2350, 2021, doi: 10.22075/IJNAA.2021.5379.

[4] A. L. Noviani and I. Yuliani, “Perancangan Perangkat Lunak Kriptografi Menggunakan Gronsfeld Cipher, Vernam Cipher dan Ron Code 4 Stream Cipher,” *Enter*, vol. 2, pp. 549–559, 2019.

[5] B. J. Dwi, M. Joko Priono, P. Pengiriman Pesan, A. Suhendri, B. Dwi Juniansyah, and D. Darwis, “Implementasi Kombinasi Affine Cipher Dan One-Time Pad Dalam,” *J. Inform.*, vol. 18, no. 2, pp. 124–129, 2018.

[6] M. N. Ghuge and P. N. Chatur, "Collaborative Key Management in Ciphertext Policy Attribute Based Encryption for Cloud," *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2018*, no. Icicct, pp. 156–158, 2018, doi: 10.1109/ICICCT.2018.8473169.

[7] R. Rahim *et al.*, "Combination Vigenere Cipher and One Time Pad for data security," *Int. J. Eng. Technol.*, vol. 7, pp. 92–94, 2018, doi: 10.14419/ijet.v7i2.3.12624.