Algoritma : Jurnal Matematika, Ilmu pengetahuan Alam, Kebumian dan Angkasa
Volume. 3, Nomor. 3 Mei 2025
e-ISSN: 3046-5427; p-ISSN: 3032-6230, Hal 01-06
DOI : https://doi.org/10.62383/algoritma.v3i3.468
Available Online at : https://journal.arimsi.or.id/index.php/Algoritma

Menghitung Peluang dalam Susunan Kata Sandi: Kombinatorika dalam Keamanan Digital

Arnah Ritonga[1*], Dina Harianja[2], Maisarah Putri Lalyta Siregar[3], Stepanus Simatupang[4], Vany Aisah Panggabean[5]
[1-5]Universitas Negeri Medan, Indonesia
Email: arnahritonga@unimed.ac.id [1], harianjadina0@gmail.com [2], maisarah.putrii2006@gmail.com [3], stepanussimatupang964@gmail.com [4], vani.panggabean17@gmail.com [5]

*Korespondensi penulis: arnahritonga@unimed.ac.id**

Abstract. *Today is a sophisticated era where everything is digital, be it smartphones, laptops, even safes. So digital password security is essential in protecting personal data. This study analyzes password strength using combinatorics and probability. Calculations are made to determine the number of possible password combinations based on the length and type of characters. In addition, the probability of success of a brute-force attack is calculated based on the number of guesses that can be made by the attacker. The results show that the longer and more complex the password, the less likely it is to be guessed. This study also discusses the concept of information entropy to measure the level of randomness of passwords and its impact on digital security. This study provides insight into the importance of choosing strong passwords.*

Keywords: *Brute-force, Combinatorics, Entropy, Password security, Probability*

Abstrak. Zaman sekarang adalah zaman canggih di mana semua serba digital, baik itu *smartphone*, laptop, bahkan brankas. Maka kemanan kata sandi digital sangat penting dalam menjaga data pribadi. Penelitian ini menganalisis kekuatan kata sandi menggunakan kombinatorika dan probabilitas. Perhitungan dilakukan untuk mengetahui jumlah kemungkinan kombinasi kata sandi berdasarkan panjang dan jenis karakter. Selain itu, peluang keberhasilan serangan brute-force dihitung berdasarkan jumlah tebakan yang bisa dilakukan oleh penyerang. Hasil penelitian menunjukkan bahwa semakin panjang dan kompleks kata sandi, semakin kecil kemungkinan untuk ditebak. Penelitian ini juga membahas konsep entropi informasi untuk mengukur tingkat keacakan kata sandi dan dampaknya terhadap keamanan digital. Studi ini memberikan wawasan tentang pentingnya memilih kata sandi yang kuat.

Kata kunci: *Brute-force*, Kombinatorik, Entropi, Keamanan kata sandi, Probabilitas

1. PENDAHULUAN

Kata Sandi merupakan alat keamanan yang digunakan oleh setiap elemen atau masyarakat didunia. Biasanya kata sandi digunakan sebagai alat kemanan sebuah media social, kata sandi juga digunakan oleh setiap instansi guna menjaga data setiap instansi. Setiap pengguna memiliki berbagai macam kata sandi yang bersifat unik, dikarenakan penggabungan beberapa character menjadi satu. Kata sandi yang aman memiliki kriteria masing masing, contohnya adalah tidak aman, cukup aman, aman, dan sangat aman. Cara kerja kata sandi adalah, pengguna akan diminta memasukan kata sandi yang telah ia buat dalam sebuah akun. Kemudian kata sandi yang telah dimasukan oleh pengguna akan dicocokan di system basis data yang dimiliki oleh aplikasi tersebut. Jika kata sandi yang dimasukan sama dengan yang berada di sistem basis data, maka pengguna akan diberikan akses masuk ke aplikasi tersebut. Setiap

Received: Februari 14,2025; Revised: Maret 18,2025; Accepted: April 07, 2025; Online Available: April 09, 2025

aplikasi biasanya memberikan fitur hidden ataupun mengenskripsi sebuah kata sandi. Mengenskripsi bertujuan untuk mengkodekan sebuah kata sandi.

Mengenskripsi sebuah kata sandi bukan salah satu cara menyelesaikan masalah dari peretasan. Pada tahun-tahun modern seperti ini banyak software illegal yang digunakan para peretas untuk meretas sebuah akun. Para peretas biasanya akan memasukan kombinasi-kombinasi karakter untuk mencoba membuka sebuah akun, semakin rumit kombinasi dari kata sandi tersebut semakin lama dan susah untuk sebuah kata sandi teretas. Para peretas biasanya meretas sebuah akun untuk menjual data pemilik akun, ataupun sebagainya. Atas masalah tersebut kita diharapkan memilih kata sandi yang aman, ataupun memiliki kata sandi yang mepunyai kombinasi dari beberapa character, untuk meningkatkan keamanan pada akun pengguna. Tekhnik yang biasanya digunakann oleh hacker misalnya yaitu Bruteforce

Pemahaman terhadap bruteforce dapat menjadi tolak ukur seberapa aman kata sandi setiap pengguna di berbagai aplikasi. Pengetahuan ini juga dapat untuk membantu pengembangan aplikasi, dan membantu pengembang aplikasi untuk mengamankan data setiap user. Para pengembang aplikasi harus menentukan karakter setiap kata sandi yang dibutuhkan oleh pengguna. Kata sandi yang dipilih juga harus dari beberapa karakter yang berbeda, untuk keaman data bersama.

Penelitian ini menggunakan konsep kombinatorika, teori peluang, dan entropi informasi untuk menghitung jumlah kemungkinan kata sandi, menentukan peluang keberhasilan serangan brute-force, serta mengukur tingkat keacakan kata sandi menggunakan teori entropi Shannon.

2. METODE PENELITIAN

Penelitian ini dilakukan dengan langkah-langkah berikut: Menentukan ruang sampel kata sandi : berdasarkan jumlah karakter yang tersedia (huruf kecil, huruf besar, angka, simbol). Menghitung jumlah kombinasi kata sandi, dengan rumus: $C = k^n$ di mana k adalah jumlah karakter yang bisa digunakan dan n adalah panjang kata sandi. Menghitung peluang menebak kata sandi**,** dengan rumus: $P = \frac{m}{c}$ di mana m adalah jumlah tebakan yang dilakukan. Menghitung entropi kata sandi**,** dengan rumus Shannon: $H = n \times \log_2(k)$ yang menunjukkan tingkat keacakan kata sandi H . Semakin tinggi nilai, semakin sulit kata sandi ditebak.

3. HASIL DAN PEMBAHASAN

Dalam sebuah aplikasi mengharuskan pengguna menggunakan password minimal 5 dan maksimal 8. Setiap password boleh menggunakan angka, simbol, dan huruf. Antara huruf besar dan huruf kecil dibedakan.

- Pada huruf besar(A-Z) = 26
- Pada huruf kecil(a-z)= 26
- Pada Angka (0-9) = 10

Total karakter yang digunakan adalah 26+26+10 = 62.

Jika sandi memiliki 5 kata maka: 62^5 = (62) (62) (62) (62) (62) = 916.132.832 cara.

Jika sandi memiliki 6 kata maka 62^6 = (62) (62) (62) (62) (62) (62) = 56.800.235.584 cara.

Jika sandi memiliki 7 kata maka 62^7 = (62) (62) (62) (62) (62) (62) (62)= 3.521.614.606.208 cara.

- Sedangkan kriteria status password sebagai berikut :

✓ Tidak aman = kata sandi dapat dicari dengan cara dibawah 500.000 cara.

✓ Cukup aman = kata sandi dapat dicari dengan cara 500.001 – 1.000.000 cara.

✓ Aman = kata sandi dapat dicari dengan cara 1.000.001 – 5.000.000 cara.

✓ Sangat Aman = kata sandi dapat dicari dengan cara diatas 5.000.001 cara.

Selanjutnya jika kata sandi adalah “B3caK123”, kata sandi ini terdiri dari 8 suku kata dan menggunakan kombinasi dari huruf kecil dan angka.

B = adalah huruf besar, huruf “B” ada pada urutan ke-2.

3 = adalah angka, angka “3” ada pada urutan ke-4.

c = adalah huruf kecil, huruf “c” ada pada urutan ke-3. 4 = adalah angka,

huruf “a” ada pada urutan ke-5.

k = adalah huruf kecil, huruf “k” ada pada urutan ke-11.

1 = adalah angka, angka “1” ada pada urutan ke-2.

2 = adalah angka, angka “2” ada pada urutan ke-3.

3 = adalah angka, angka “3” ada pada urutan ke-4.

Karena disini pengguna menggunakan kombinasi dari huruf besar, huruf kecil, dan angka. Maka untuk mencari total, dengan cara menjumlahkan urutan terbesar dari huruf kecil dan urutan terbesar dari angka yang berada pada data.

Total karakter yang digunakan adalah = 2 + 11 + 5 = 18 karakter.

Maka kata sandi dapat dipecahkan dengan : 18^8= (18) (18) (18) (18) (18) (18) (18) (18) = 11.019.960.576 cara. (Maka kata sandi berstatus sangat aman)

Pembahasan

1. Perhitungan Kombinasi Kata Sandi dan Entropi

Misalkan sebuah kata sandi hanya menggunakan huruf kecil (26 karakter). Jika panjang kata sandi adalah 8, maka jumlah kombinasi yang mungkin adalah: $C = 26^8 = 208.827.064.576$ cara.

Jika menggunakan huruf besar, angka, dan simbol (94 karakter), maka:

$$C = 94^8 = 6{,}095 \times 10^{15}$$

Perhitungan entropi untuk masing-masing skenario:

- Huruf kecil

  $H = 8 \times \log_2(26) \approx 37{,}6$ bit.
- Huruf besar, angka, dan simbol

  $H = 8 \times \log_2(94) \approx 52{,}6$ bit.

Semakin tinggi entropi, semakin kuat kata sandi terhadap serangan.

2. Peluang Serangan Brute-Force

Jika seorang penyerang mencoba 1 juta tebakan per detik, maka waktu yang dibutuhkan untuk mencoba semua kemungkinan kombinasi adalah:

- Huruf kecil: detik (sekitar 2,4 hari).
- Huruf besar, angka, simbol: detik (sekitar 61 tahun).

Dengan demikian, semakin panjang dan kompleks kata sandi, semakin lama waktu yang dibutuhkan untuk menebaknya.

4. KESIMPULAN DAN SARAN

Dari hasil penelitian yang sudah kami buat dapat kita simpulkan bahwa kombinatorial adalah metode yang digunakan untuk menghitung penyusunan dalam semua skema yang digunakan. Brute-force adalah tehnik untuk memecahkan sebuah password dengan sekumpulan kata acak yg di susun beratus-ratus hingga beribu-ribu, gunanya untuk memecahkan password yg dituju. Tehknik yang digunakan oleh bruteforce ialah mengkombinasikan setiap karakter, dan mencocokan satu persatu.

Dari setiap kata sandi yang telah di analisis kami menyimpulkan bahwa kata sandi yang ideal mempunyai tingkat keamanan sangat aman ialah kata sandi yang memiliki total karakter yang banyak dan dalam setiap kata sandi memiliki beberapa karakter yang berbeda. Jika

dibandingkan dengan kata sandi yang tidak aman, kata sandi ini memilik total karakter yang sedikit, dan hanya memiliki beberapa karakter yang sama, bahkan memiliki karakter yang sama semua. Dalam penggunaan bruteforce kata sandi yang sangat aman pasti memiliki jumlah cara dalam pemecahannya sangat banyak, dan jumlah cara yang banyak menyebabkan waktu yang diperlukan sangat banyak.

Penelitian ini menunjukkan bahwa semakin panjang dan beragam karakter dalam kata sandi, semakin kecil kemungkinan untuk ditebak dengan serangan brute-force. Selain itu, penggunaan entropi menunjukkan bahwa tingkat keacakan kata sandi juga berperan penting dalam meningkatkan keamanan digital. Oleh karena itu, pengguna disarankan untuk menggunakan kata sandi yang panjang dan kompleks untuk meningkatkan keamanan digital.

UCAPAN TERIMA KASIH

Syukur Alhamdulillah kita panjatkan kepada Allah S.W.T yang telah melimpahkan rahmatnya yang memudahkan kami dalah menyelesaikan jurnal Teori Peluang yang bertema Kombinatorial ini. Tanpa doa dan semangat yang keras jurnal ini tidak akan berakhir dengan baik.

Ucapan terimakasih kepada semua pihak yang telah berkontribusi dalam penelitian ini, terutama untuk Ibu Arnah Ritonga S.Si., M.Si yang telah membimbing kami sehingga jurnal kami dapat selesai.

DAFTAR REFERENSI

Ahmad, E., Fahroza, M., Ramadhani, F., Syahfitri, A., & Fadhlurohhman, D. (2021). Implementasi kombinatorial dalam penentuan kata sandi teknologi. *Jurnal Ilmu Komputer, Teknologi Informasi dan Teknik Telekomunikasi.* https://doi.org/10.30596/JCOSITTE.V2I1.6526

Alghani, I. Y. (2019). Penggunaan teknik bruteforce untuk menentukan keamanan setiap kata sandi menggunakan metode kombinatorial. *Unnes Journal of Mathematics, 8*(2), 52–59.

Alkurdi, Y., Al-Fayoumi, M., Al-Badarneh, A., & Al-Haija, Q. (2023). Meningkatkan keamanan kata sandi melalui pembelajaran terbimbing. *Konferensi Internasional tentang Teknologi Informasi (ICIT) 2023*, 256–259. https://doi.org/10.1109/ICIT58056.2023.10226141

Bethapudi, P., Harika, T., Nirisha, G., & Prasanna, K. (2024). Sistem autentikasi kata sandi tiga tingkat. *Jurnal Riset Internasional tentang Advanced Engineering Hub (IRJAEH).* https://doi.org/10.47392/irjaeh.2024.0332

Esser, A., Girme, R., Mukherjee, A., & Sarkar, S. (2024). Memory-efficient attacks on small LWE keys. *Journal of Cryptology, 37*, 36. https://doi.org/10.1007/978-981-99-8730-6_3

George, G., & Thampi, S. (2022). Combinatorial analysis for securing IoT-assisted Industry 4.0 applications from vulnerability-based attacks. *IEEE Transactions on Industrial Informatics, 18*, 3–15. https://doi.org/10.1109/TII.2020.3045393

Gu, Y., Akao, S., Esfahani, N., Miao, Y., & Sakurai, K. (2022). Mengenai keamanan teori informasi dari transformasi kombinatorial all-or-nothing. *IEEE Transactions on Information Theory, 68*, 6904–6914. https://doi.org/10.1109/TIT.2022.3174008

Reaz, K., & Wunder, G. (2022). Entropi ekspektasi sebagai metrik kekuatan kata sandi. *Konferensi IEEE 2022 tentang Komunikasi dan Keamanan Jaringan (CNS)*, 1–2. https://doi.org/10.1109/CNS56114.2022.9947259

Riznyk, V. (2022). Combinatorial optimization of systems of neural network cryptographic data protection. *Ukrainian Journal of Information Technology*. https://doi.org/10.23939/ujit2022.02.056

Wiese, M., & Boche, H. (2021). Mosaics of combinatorial designs for information-theoretic security. *arXiv*. https://arxiv.org/abs/2104.15009

Zaland, Z., Bazai, S., Marjan, S., & Ashraf, M. (2021). Algoritma keamanan kata sandi tiga tingkat untuk basis data daring. *Konferensi Informatika dan Rekayasa Perangkat Lunak Internasional ke-2 (IISEC) 2021*, 1–6. https://doi.org/10.1109/IISEC54230.2021.9672434