UJM 8 (2) (2019)
UNNES Journal of Mathematics
http://journal.unnes.ac.id/sju/index.php/ujm

PENGGUNAAN TEKNIK BRUTEFORCE UNTUK MENENTUKAN KEAMANAN SETIAP KATA SANDI MENGGUNAKAN METODE KOMBINATORIAL

Ilham Yusuf Alghani✉, M. Rizky Addin S

Universitas Amikom Yogyakarta, Indonesia
Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta, 55281

Info Artikel

Sejarah Artikel:
Diterima Desember 2018
Disetujui Juli 2020
Dipublikasikan Agustus 2020

Keywords:
Bruteforce, Password, Security.

Abstrak

Studi ini mengkaji keamanan kata sandi yang dimiliki oleh pengguna dangan menggunakan tehknik bruteforce. Tujuan studi ini adalah untuk membantu para pengguna dalam mengetahui keamanan kata sandi pengguna. Pengumpulan data dilakukan dengan cara menggunakan kata sandi yang telah disediakan yang kemudian dianalisis untuk mengetahui setiap keamanan kata sandi tersebut. Hasil dari setiap kata sandi dapat dibedakan menjadi 4 bagian yaitu, tidak aman, cukup aman, aman, dan sangat aman. Kajian tentang keamanan tersebut dapat sangat berguna untuk penggun dalam menentukan sebuah kata sandi yang akan sulit teretas.

Abstract

This study examines the security of passwords owned by users and uses bruteforce techniques. The purpose of this study is to help users know the security of user passwords. Data collection is done by using a password that has been provided which is then analyzed to find out each password security. The results of each password can be divided into 4 parts, namely, unsafe, safe, secure, and very safe. The study of security can be very useful for users in determining a password that will be difficult to hack.

How to cite:

Alghani, Ilham Yusuf., Addin, M.Rizky.2019. Penggunaan Teknik Bruteforce untuk Menentukan Keamanan Setiap Kata Sandi Menggunakan Metode Kombinatorial. *UNNES Journal of Mathematics*. 8(2): 52-59

✉Alamat korespondensi:
E-mail: ilhamyusuf276@gmail.com

p-ISSN 2252-6943
e-ISSN 2460-5859

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 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.

METODE

Kali ini kami akan melakukan penelitian menggunakan metode yaitu kombinatorial. Kombinatorial adalah metode yang digunakan untuk menghitung penyusunan dalam semua skema yang digunakan. Pada kasus ini metode kombinatorial bertindak untuk menentukan karakter yang digunakan dalam setiap kata sandi. Setiap karakter harus terpisah tidak boleh menjadi satu.

Kemudian kami menggunakan password yang telah disediakan sebagai data yang akan diteliti. Didalam data tersebut kita meneliti berapa cara yang dapat digunakan untuk memecahkan sebuah password menggunakan tehknik bruteforce. Bruteforce adalah tehnik untuk memecahkan sebuah password dengan sekumpulan kata acak yg di susun beratus-ratus hingga beribu-ribu, gunanya untuk memecahkan password yg dituju. Tehnik ini bersifat 50/50 karena dia menggunakan sekumpulan kata acak yg kita gunakan kata bisa berupa alfabet mulai dari a-z, A-Z, angka 1-100 atau lebih, dan bahkan hingga tanda baca, program akan mencoba membuat beberapa kata yg kemungkinan bisa untuk memecahkan password yg diinginkan. Proses pencarian password ini memerlukan waktu (kecepatan tergantung dengan spesifikasi computer user).

Kemudian yang harus dilakukan adalah melakukan observasi yang disertai dengan paparan. Paparan tersebut bertujuan untuk memudahkan para developer dalam menganalisis dengan seksama. Kemudian hasil dari analisis tersebut dimasukan dalam grafik dan tabel. Tujuan dari dimasukannya data kata sandi yang telah dianalisis ke tabel dan grafik karena dapat memudahkan dan memperjelas dalam memaparkan.

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

Jika sandi memiliki 8 kata maka

62^8=(62) (62) (62) (62) (62) (62) (62) (62)= 218.340.105.584.896 cara

Maka password dapat dipecahkan dengan

916.132.832 + 56.800.235.584 + 3.521.614.606.208 + 218.340.105.584.896 = 221.919.436.559.520 cara

Jika pengguna memiliki daftar password yang digunakan. Untuk password yang digunakan adalah becak, Becak, becak123, Becak, Becak123, b3cak, B3caK, B3caK123.

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.

1. Untuk kata sandi yang ke-1 adalah “becak”, becak terdiri dari 5 suku kata dan menggunakan huruf kecil.

   b = adalah huruf kecil, huruf “b” ada pada urutan ke-2.

   e = adalah huruf kecil, huruf “e” ada pada urutan ke-5.

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

   a = adalah huruf kecil, huruf “a” ada pada urutan ke-1.

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

   Karena disini pengguna menggunakan karakter yang sama yaitu adalah huruf kecil. Maka pilih urutan yang paling besar untuk memudahkan dalam menghitung.

   Total karakter yang digunakan adalah = 11 karakter

   Maka kata sandi tersebut dapat dipecahkan dengan :

   11^5 = (11) (11) (11) (11) (11) = 161.051 cara

   Maka kata sandi “becak” berstatus tidak aman.

2. Untuk kata sandi ke-2 adalah “Becak”, becak terdiri dari 5 suku kata dan menggunakan kombinasi dari huruf besar dan huruf kecil.

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

   e = adalah huruf kecil, huruf “e” ada pada urutan ke-5.

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

a = adalah huruf kecil, huruf "a" ada pada urutan ke-1. k = adalah huruf kecil, huruf "k" ada pada urutan ke-11.

Karena disini pengguna menggunakan kombinasi dari huruf besar dan huruf kecil. Maka untuk mencari total dengan cara menjumlahkan urutan huruf besar dan urutan huruf kecil yang berada pada data. Pada huruf kecil diambil dari urutan yang paling besar.

Total karakter yang digunakan adalah = 2 + 11 = 12 karakter

Maka kata sandi tersebut dapat dipecahkan dengan:

12^5 = (12) (12) (12) (12) (12) = 248.832 cara

Maka kata sandi diatas berstatus tidak aman.

3. Untuk kata sandi yang ke-3 adalah "becak123", kata sandi ini terdiri dari 8 suku kata dan menggunakan kombinasi dari huruf kecil dan angka.

   b = adalah huruf kecil, huruf "b" ada pada urutan ke-2.

   e = adalah huruf kecil, huruf "e" ada pada urutan ke-5.

   c = adalah huruf kecil, huruf "c" ada pada urutan ke-3.

   a = adalah huruf kecil, huruf "a" ada pada urutan ke-1.

   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 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 = 11 + 4 = 15 karakter

   Maka kata sandi dapat dipecahkan dengan :

   15^8 = (15) (15) (15) (15) (15) (15) (15) (15) = 2.562.890.625 cara

   Maka kata sandi berstatus sangat aman.

4. Untuk kata sandi yang ke-4 adalah "Becak123", 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.

   e = adalah huruf kecil, huruf "e" ada pada urutan ke-5.

   c = adalah huruf kecil, huruf "c" ada pada urutan ke-3.

   a = adalah huruf kecil, huruf "a" ada pada urutan ke-1.

   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 + 4 = 17 karakter

Maka kata sandi dapat dipecahkan dengan :

17^8 = (17) (17) (17) (17) (17) (17) (17) (17) = 6.975.757.441 cara

Maka kata sandi berstatus sangat aman.

5. Untuk kata sandi yang ke-5 adalah "b3cak", becak terdiri dari 5 suku kata dan menggunakan huruf kecil.

   b = adalah huruf kecil, 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.

   a = adalah huruf kecil, huruf "a" ada pada urutan ke-1.

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

   Karena disini pengguna menggunakan karakter yang sama yaitu adalah huruf kecil. Maka pilih urutan yang paling besar untuk memudahkan dalam menghitung.

   Total karakter yang digunakan adalah = 11 + 4 = 15karakter

   Maka kata sandi tersebut dapat dipecahkan dengan :

   15^5 = (15) (15) (15) (15) (15) = 759.375 cara

   Maka kata sandi "becak" berstatus cukup aman.

6. Untuk kata sandi yang ke-6 adalah "B3caK", kata sandi ini terdiri dari 5 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.

   a = adalah huruf kecil, huruf "a" ada pada urutan ke-1.

   K = adalah huruf kecil, huruf "k" ada pada urutan ke-11.

   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 + 4 = 17 karakter

   Maka kata sandi dapat dipecahkan dengan :

   17^5 = (17) (17) (17) (17) (17) = 1.419.857 cara

   Maka kata sandi berstatus aman.

7. Selanjutnya kata sandi ke-7 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

1.2Diagram dan Tabel

Jumlah Kata	Cara Pemecahan
5	916.132.832
6	56.800.235.584
7	3.521.614.606.208
8	218.340.105.584.896
Total	221.919.436.559.520

Tabel 1. Presentase total pemecahan suatu kata sandi

Kata sandi	Cara Pemecahan
becak	161.051
Becak	248.832
becak123	2.562.890.625
Becak123	6.975.757.441
b3cak	759.375
B3caK	1.419.857
B3c4K123	11.019.960.576

Tabel 2. Presentase cara setiap kata sandi

Dapat disimpulkan bahwa setiap kata sandi memiliki cara pemecahan sendiri-sendiri. Memiliki cara pemecahan yang banyak lebih menguntungkan dikarenakan akan sangat sulit jika akan diretas karena waktu yang di perlukan akan lebih banyak.

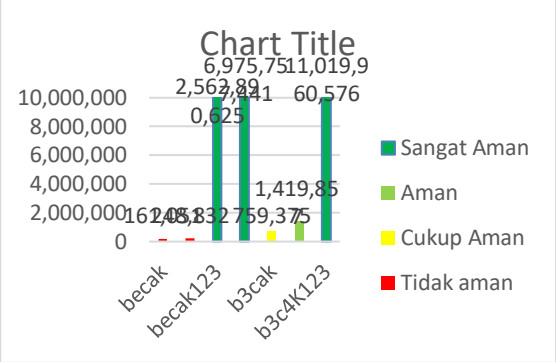


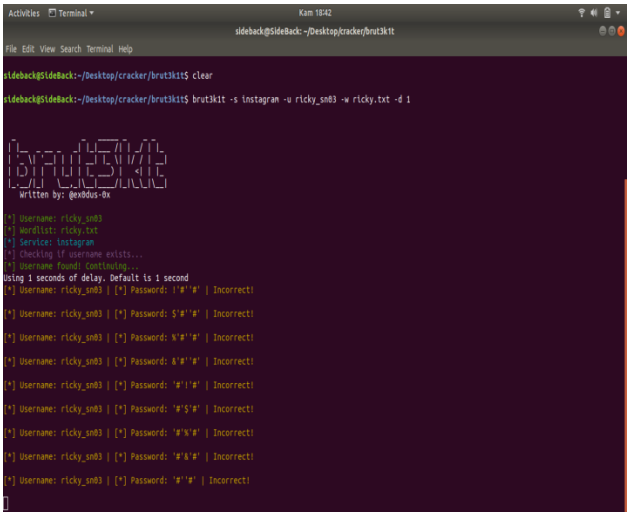
Diagram 1. Status keamanan

Dapat disimpulkan bahwa kata sandi yang berstatus tidak aman berjumlah 2, dan yang cukup aman tidak ada, kata sandi yang berstatus aman berjumlah 1, dan yang berstatus sangat aman berjumlah 2.

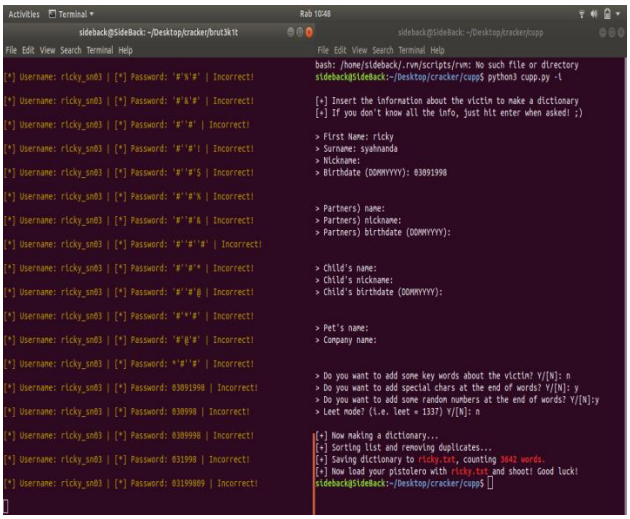
1.3 Gambar dan Pembahasan

Pada bab ini kita akan membahas bagaimana cara kerja dari program bruteforce itu sendiri sebelum kita memulai melakukan test dengan bruteforce kita harus menyediakan wordlist nya terlebih dahulu disini saya menggunakan program cupp.py dimana program ini untuk membuat wordlistnya kemudian untuk program bruteforcenya saya menggunakan program brut3kit pada program brut3kit kita disediakan beberapa pilihan seperti ingin melakukan bruteforce pada Instagram,facebook,gmail, atau untuk memecahkan md5,base64,dan sha256.

Dibawah adalah contoh program bruteforce yang mencoba memecahkan sebuah password Instagram menggunakan wordlist yang sudah disiapkan



Dibawah ini adalah proses membuat wordlist untuk memecahkan passwordnya isi wordlist ini berjumlah 3000 kalimat yang kemungkinan dipakai oleh si user



PENUTUP

Dari hasil penelitian yang sudah kami buat dapat kita simpulkan bahwa kombinatorial adalah metode yang digunakan untuk menghitung penyusunan dalam semua skema yang digunakan. Bruteforce 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.

Kami berharap data yang telah kami analisis sebaik mungkin dapat bermanfaat untuk setiap pengguna, agar tidak sekedar memilih kata sandi, tetapi juga membuat sebuah kata sandi yang dapat menjaga data dengan aman, dan menjadi solusi kepada developer agar dapat menjaga data dari peretasan.

Berdasarkan kesimpulan yang ada, di atas kami merekomendasikan kepada instansi atau orang yang dapat meningkatkan keamanan yang berguna untuk menjaga data-datanya diantaranya yaitu :

1. Kepada para pengembang aplikasi
   Memberikan sebuah aturan ataupun syarat kepada pengguna agar menggunakan kata sandi yang memiliki banyak suku kata, dan terdiri dari banyak karakter, misalnya menggunakan huruf besar, huruf kecil, angka, dan symbol dalam satu kata sandi.
2. Kepada para pengguna aplikasi
   Membuat kata sandi yang mudah diingat, memiliki banyak suku kata yang terdiri dari kombinasi karakter yang berbeda. Setiap media social diharapkan memiliki kata sandi yang berbeda untuk mencegah peretasan.

UCAPAN TERIMAKASIH

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

Pada kesempatan kali ini kami menyampaikan rasa terima kasih yang sebesar-besarnya kepada Bapak Ferry Wahyu Wibowo, S.Si, M.Cs selaku dosen pembibing, yang telah membantu dalam membimbing dalam bab kombinatorial ini.

Ucapan terima kasih juga kami haturkan kepada :

1. Orang Tua yang selalu mendukung agar terselesainya paper ini..
2. Teman teman IF02 yang membantu dalam penyusunan paper ini.

DAFTAR PUSTAKA

Tools Wordlist : https://github.com/Mebus/cupp

Tools BruteForce : https://github.com/ex0dus-0x/brut3k1t