Kombinatorial Dalam Aplikasi Telepathwords

Reinaldo Michael Hasian/13512092
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*reinaldo_mh@students.itb.ac.id*

***Abstract*—Makalah ini membahas mengenai keamanan password dengan analisa kombinatorial. Dewasa ini hampir setiap orang memiliki akun di dunia maya,baik sosial media,email,game,dan lain-lain. Makalah ini membahas tentang telepathwords,yaitu aplikasi yang dapat memprediksi password user berdasarkan input karakter. Telepathwords dibuat dengan tujuan agar kita tidak membuat *password*/kata kunci yang lemah. Makalah ini akan membahas bagaimana cara kerja telepathwords,cara kerja,serta kelebihan dan kelemahannya.**

Kata Kunci-Kombinatorial,Kombinasi,password, keamanan,telepathwords,kriptografi,enkripsi

I. PENDAHULUAN

Saat ini,hampir setiap orang memiliki akun di dunia maya dan akun-akun tersebut biasanya akan membutuhkan *password/*kata kunci. Membuat kata kunci yang aman sudah menjadi penting sekarang ini apalagi di era kemajuan teknolgi yang begitu cepat. Seseorang tentunya akan membuat kode keamanan yang mudah di ingat,namun kode itu belum tentu sulit ditebak.

Kata kunci menjadi sesuatu yang penting untuk dirahasiakan karena tidak jarang orang-orang menyimpan informasi atau file penting dalam akunnya.

Orang akan cenderung membuat password yang di ingatnya. Menurut sebuah laporan Splash Data ada 25 jenis password yang sering digunakan di internet,yaitu :

1. password
2. 123456
3. 12345678
4. qwerty
5. abc123
6. monkey
7. 1234567
8. letmein
9. trustno1
10. dragon
11. baseball
12. 111111
13. iloveyou
14. master
15. sunshine
16. ashley
17. bailey
18. passw0rd
19. shadow
20. 123123
21. 654321
22. superman
23. qazwsx
24. michael
25. football

Kombinatorial adalah salah satu bahasan pokok Matematika Diskrit yang banyak dikembangkan dan diaplikasikan dalam berbagai bidang. Dalam sejarah Matematika kombinatorial menarik untuk dipelajari dan dikembangkan.

Dengan menggunakan teori kombinatorial kita dapat menghitung banyaknya kombinasi angka/dan huruf yang memungkinkan dalam sebuah password.

Telepathwords adalah salah 1 aplikasi yang menggunakan prinsip kombinatorial dalam menjalankan programnya,yaitu menebak kata sandi berdasarkan input user.

Telpathwords dibuat di Microsoft Research oleh penemu-penemu Microsoft dan kerjasama program PhD Carniege Mellon University(CMU).

Pembuat Telepathwords antara lain Saranga Comanduri(CMU Leader),Stuart Schechter (MSR Leader), Cormac Herley (MSR), Paul Hsu (MSR), Ricky Loynd (MSR), Jim St.George (MSR,logo designer).

II. DASAR TEORI

2.1 Password

"A **password** is a secret word or stringof character used for user authentication to prove identity or acces approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access"[1]

Password adalah kata atau kalimat yang digunakan sebagai pengenal untuk membuktikan atau mengijinkan perolehan akses ke suatu sumber,yang harus dijaga secara rahasia dari orang-orang yang tidak diijinkan mengakses.

Password sendiri terdiri dari 2 kata,yaitu pass dan word. Pass berarti lewat dan word berarti kata. Bila digabungkan password artinya kata yang dibutuhkan untuk melewati/mendapatkan sesuatu.

Ketentutuan pembuatan password disetiap akun berbeda-beda. Ada yang mengharuskan kombinasi huruf dan angka,ada yang mengharuskan menggunakan karakter khusus,ada yang memberikan syarat jumlah minimal kombinasi,ada pula yang membebaskan pengguna sama sekali.

Gambar 2. Contoh Password

2.2 Teori Kombinatorial

Teknik menghitung kemungkinan ada 2,yaitu pemjumlahan(sum rule) dan aturan perkalian (product rule).Kedua cara tersebut dibedakan berdasarkan cara dan waktu percobaan dilakukan.

2.2.1 Kaidah Dasar Menghitung

1.Kaidah Penjumlahan

Jika N percobaan dilakukan dan setiap percobaan memilki (n) hasil yang berbeda-beda,maka akan terdapat $(n_0 + n_1 + n_2 + \ldots + n_N)$ buah hasil percobaan.

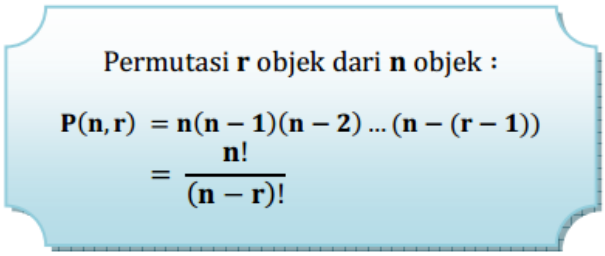
2.Kaidah Perkalian

Jika N percobaan dilakukan dan setiap percobaan memilki (n) hasil yang berbeda-beda,maka akan terdapat $(n_0 \times n_1 \times n_2 \times \ldots \times n_N)$ buah hasil percobaan.

3.Permutasi

Merupakan jumlah urutan yang berbeda dari pengaturan objek-objek. Permutasi merupakan bentuk khusus kaidah perkalian. Misalkan jumlah objek adalah n, maka
menurut kaidah perkalian, permutasi dari n objek adalah

$n(n-1)(n-2)\ldots(2)(1) = n!$



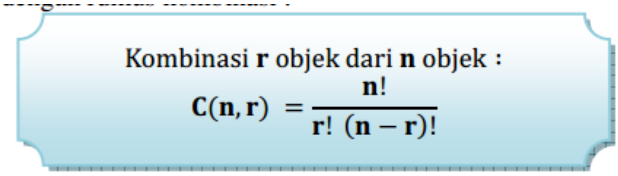
Gambar 2.1. Permutasi[5].

3.Kombinasi

Merupakan bentuk khusus dari permutasi yang mengabaikan urutan kemunculan[6].

Pada permutasi ABC ≠ BCA,namun pada kombinasi ABC,ACB,BCA,BAC,CBA,CAB adalah sama karena urutan tidak diperhatikan,itulah yang membedakan kombinasi dengan permutasi. Nilai kombinasi dari n objek selalu lebih sedikit dari permutasi n objek.

Hal tersebut dapat dibuktikan dengan rumus umum kombinasi :

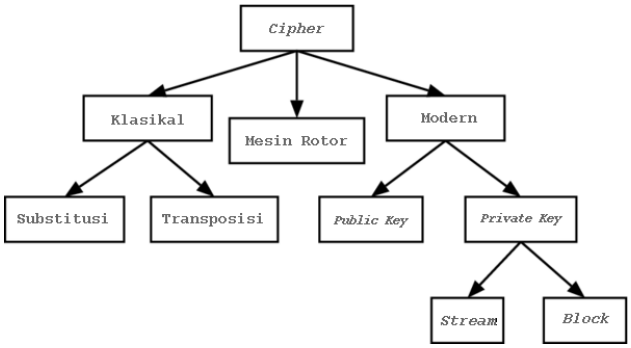


Gambar 2.2.Kombinasi[6].

2.3 Enkripsi

Enkripsi adalah proses mengamankan informasi agar tidak dapat diketahui tanpa bantuan khusus. Enkripsi sudah banyak digunakan untuk mengamankan komunikasi di berbagai Negara. Enkripsi kuat dimanfaatkan pada pertengahan tahun 1970-an untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain public.

Cipher adalah salah satu algoritma prosedural untuk menampilkan enkripsi dan deskripsi. Informasi asli disebut *plaintext* dan hasil enkripsi disebut *chipertext*. Chipertext berisi seluruh informasi plaintext namun bukan dalam bahasa yang bisa dimengerti manusia ataupun komputer tanpa menggunakan suatu proses deskripsi. Proses deskripsi tersebut membutuhkan suatu terjemahan yang disebut sebagai kunci.



Gambar 2.3. Taksonomi Chipher[8]

Beberapa jenis algoritma enkripsi yang ada saat ini diantaranya :
1.RSA
2.DES/3DES
3.BLOWFISH
4.IDEA
5.SEAL
6.RC4

III. CARA KERJA TELEPATHWORDS

A.Kegunaan dan Kelebihan

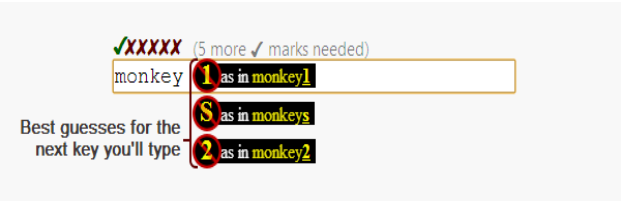
Telepathwords adalah salah satu hasil penelitian Microsoft yang bekerjasama dengan Carniege Mellon University yang dibuat untuk mengajarkan pengguna web dan mencegah mereka membuat password di dunia maya secara sembarangan/asal-asalan.

Telepathwords dapat memprediksi seberapa kuat password anda,artinya kita dapat mengetahui kemungkinan terkena hack oleh pihak yang tidak bertanggung jawab.

Gambar 2. Telepathwords

Telepathwords mencoba memprediksi karakter selanjutnya dari *input*-an pengguna. Cara Telepathwords memprediksi yaitu :

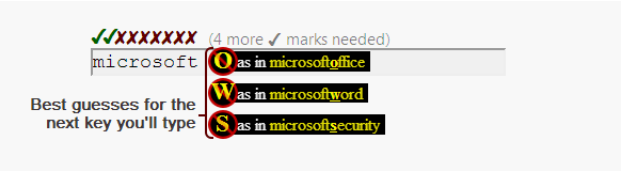
1. *Common Password*
   atau password yang banyak digunakan oleh publik dalam akun dunia maya mereka. Misalnya pada 25 jenis password yang ada di internet,terdapat kata kunci "monkey".



Gambar 3. Password Monkey

Telepathwords dapat menebak 5 karakter berikutnya dari huruf 'm' (akan ditandai dengan tanda silang di atas huruf yang bersangkutan). Selain itu Telepathwords juga memprediksi kemungkinan lain setelah "monkey" di-inputkan yaitu monkey1,monkeys,dan monkey2. Maka kombinasi password yang memungkinkan untuk ditebak akan berkurang jauh lebih banyak.

2. *Common Phrases*
   Cara lain adalah dengan frasa. Telepathwords mencoba mencari frasa yang sering terlihat di halaman web atau query yang umum. Misalnya kata kunci tersebut adalah "microsoft".

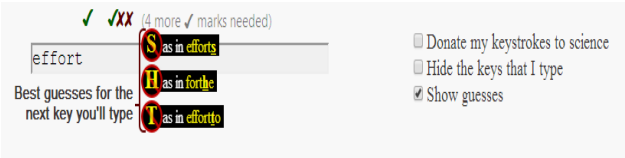


Gambar 4. Password Microsoft

Telepathwords sudah memprediksi kemungkinan kata kunci itu. Kombinasi kata kunci yang memungkinkan untuk ditebak jauh lebih sedikit. Hal ini akan mengurangi waktu program untuk menebak

password.

3. *Common password-selection behaviors*
   Telpathwords juga memprediksi karakter password selanjutnya dengan seleksi kelakuan umum password,misalnya dengan kemungkinan karakter berikutnya setelah input. Contoh input awal ‘e’,maka Telepathwords akan memprediksi karakter selanjutnya adalah ‘f’,jika benar akan lanjut ke ‘g’ atau kata yang mungkin,misalnya “effort” atau yang lainnya.



Gambar 3. Password effort

Seperti yang diketahui,Telepathwords memprediksi dengan 3 cara (Common Password,Common Phrases,dan Common password-selection behaviors).

Ketika user mengetikan sebuah karakter,Telepathwords akan mengirimkan karakter tersebut ke mesin prediksinya. Mesin prediksi tersebut memiliki database password umum dan frasa yang sangat besar.Kemudian karakter yang kita masukkan tadi akan di *generate* oleh mesin prediksi untuk mengeluarkan karakter selanjutnya sampai pada karakter terakhir. Untuk mengukur seberapa baik password kita,Telepathwords juga mempertahakan/menyikan log gerakan mouse dan *timing* kita mengetikan karakter atau menghapus karakter. Namun,log ini tidak mempengaruhi prediksi Telepathwords,ini hanya dimaksudkan untuk meningkatkan pemahaman peneliti tentang bagaimana *user* memilih password dan bagaimana cara mereka membantu kita untuk memilih password yang lebih baik dimasa depan.

Untuk melindungi isi log,Telepathwords mengenkripsi entri log pada browser kita sebelum dikirim ke server untuk dianalisa.

IV. ANALISIS DAN PEMBAHASAN

Dari pembahasan diatas diketahui bahwa Telepathwords menggunakan database sebagai acuan untuk memprediksi password pengguna. Tentunya hal ini akan membuat hasil prediksinya kurang akurat karena tidak semua frasa di masukkan dalam database tersebut. Selain itu kemungkinan penggunaan bahasa di dunia yang berbeda-beda,misalnya huruf Kanji (Jepang) dan Pinyin (Cina) tentunya berbeda dengan aksara Thailand. Hal ini membuat kombinasi password yang mungkin akan berkurang. Cara untuk mengurangi kekurangan ini adalah memperbanyak database frasa agar kemungkinan password lebih akurat untuk diprediksi. Selain itu pengguna dapat berasal dari berbagai Negara,suku,etnis,ataupun golongan. Ini memungkinkan adanya penggunaan kata-kata yang belum tentu ada di kamus.

Kita tahu bahwa nama pasangan,makanan favorit,nama peliharaan,orang yang disukai/dibenci, tanggal lahir,tanggal pernikahan,dan tanggal-tanggal yang penting juga kerap kali dijadikan pengguna sebagai password akunnya. Jadi,walaupun Telepathwords belum tentu bisa memprediksi kata sandi tersebut,tidak berarti kata sandi itu aman untuk digunakan. Sedangkan orang yang mungkin mengincar akun kita mengetahui data-data tersebut.

V. KESIMPULAN

Dari pembahasan aplikasi dapat diambil kesimpulan sebagai berikut :

1. Aplikasi dapat menebak character password selanjutnya dari input user. Jika tebakan benar,maka akan muncul tanda “X” jika salah akan muncul tanda centang.
2. Jika password yang di input memiliki sedikit tanda silang artinya password tersebut bisa dibilang aman untuk digunakan
3. Dengan menggunakan Telepathwords kita dapat mengetahui seberapa aman kata sandi kita.
4. Telepathwords menggunakan kombinatorial untuk memprediksi password yang mungkin dimaksudkan pengguna dengan database yang ada membuat kemungkinan mengerucut.
5. Telepathwords tidak bisa memprediksi semua password yang mungkin lemah

REFERENCES

[1] http://en.wikipedia.org/wiki/Password
Tanggal akses Minggu 15 Desember 2013

[2] http://www.digitaltrends.com
Tanggal akses Senin 16 Desember 2013

[3] http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2007-2008/Makalah/MakalahIF2153-0708-068.pdf
Tanggal akses Senin 16 Desember 2013 pukul 22:00

[4] Munir, Rinaldi, Diktat Kuliah IF 2091 Struktur Diskrit, Institut Teknologi Bandung, 2008.

[5] http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2007-2008/Makalah/MakalahIF2153-0708-035.pdf

[6] Munir, Rinaldi. “Bahan Kuliah IF2153 Matematika Diskrit”. Departemen Teknik Informatika, Institut Teknologi Bandung, 2004

[7] https://telepathwords.research.microsoft.com/

[8] http://id.wikipedia.org/wiki/Enkripsi

[9] http://www.mycrypto.net/encryption/crypto_algorithms.html

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 15 Desember 2013

Reinaldo Michael Hasian 13512092