

KAJIAN KEAMANAN PADA PROTECT DOCUMENT MICROSOFT OFFICE DENGAN MENGIMPLEMENTASIKAN ALGORITMA BRUTE FORCE DALAM MERETAS FILE DOCUMENT TERPROTEKSI

Indra M Sarkis Simamora

Fakultas Ilmu Komputer Universitas Methodist Indonesia Medan
Jl Hangtuah No 8 Medan, Sumatera Utara
Email : poetramora@gmail.com

Abstrak

Banyak free software untuk meretas password pada protect document Microsoft office yang dapat diunduh dari internet. Dalam hal ini, bagaimana teknik atau metode yang digunakan oleh software tersebut dalam meretas password protect document Microsoft Office tersebut tidak dapat dikaji dengan pasti algoritma yang digunakannya. Pada penelitian sebelumnya penulis sudah pernah mengkaji dan mengimplemetasikan algoritma brute force untuk meretas password tidak disandikan, di mana dalam kajian ini algoritma brute force mampu meretas password yang digunakan walaupun kecepatan waktu proses retasi sangat berpengaruh terhadap panjang karakter, kombinasi karakter dan tipe karakter password yang digunakan. Pada pembahasan ini Algoritma brute force dicoba diterapkan dengan merancang sebuah aplikasi menggunakan bahasa pemrograman visual basic untuk meretas password yang digunakan pada protect document microsoft office word dan excel dan sekaligus mengkaji keamanan password yang digunakan, apakah disandikan atau tidak. Pada kajian ini, algoritma brute force berfungsi sebagai string matching antara file text yang tersembunyi yang dipanggil dengan fungsi "user32" dengan inialisasi character password yang dijadikan sebagai pattern, dengan mencoba kemungkinan kemungkinan yang ada sesuai dengan panjang password, type karakter password dan kombinasi character password yang digunakan. Luaran dari kajian ini adalah aplikasi brute force untuk meretas password protect document microsoft word dan excel.

Key word : Password, Brute Force, Protect Document, Microsoft Word, Microsoft Excel

1. Pendahuluan

Microsoft Office merupakan aplikasi yang umum digunakan, di mana penggunaannya dalam mengamankan berkasnya hanya memanfaatkan *protect document* yang disediakan oleh aplikasi tersebut untuk menjaga kerahasiaan isi dari dokumen yang di simpan tidak dapat diakses atau dibuka oleh pengguna lain. Penggunaan *protect document* mengharuskan pemilik dokumen harus mengingat sandi atau *password* yang digunakan dalam setiap membuka dokumen tersebut. Pada kenyataannya sering pengguna *protect document* pada *Microsoft office*, tidak mengingat atau lupa sandi / *password* yang digunakan, sehingga banyak para pengguna *Microsoft Office* mencari solusi dengan melakukan *browsing* dari internet bagaimana teknik mengatasinya. Berdasarkan penelusuran penulis melalui internet dalam mengatasi hal tersebut di atas, banyak *free software* yang dapat diunduh untuk meretas *protect document* tersebut yang antara lain *word Password Recovery Master*[5], *Excel Password Recovery Master*[6], *Acces Password Recovery Master*[7] dan masih banyak *free software* lainnya. Hasil pengujian penulis dengan menggunakan *free software* tersebut, diperoleh hasil yang ditunjukkan pada tabel 1

Tabel 1. Hasil Pengujian Free Software

No	Nama File	Type Document	Password
1	uji1.doc	Ms. Word 97-2003	a5c
2	uji2.docx	Ms. Word 2007-2010	a5c
3	uji1.xls	Ms. Exel 97-2003	c5a
4	uji2.xlsx	Ms. Exel 2007-2010	c5a

Berdasarkan hasil pengujian dari beberapa type dokumen dengan berbagai *free software* yang diunduh, diperoleh hasil yang sama, di mana tpe dokumen *Microsoft Office* dengan versi (format type file) yang berbeda berhasil diretas. Dari sekian banyaknya *free software* yang dapat digunakan untuk meretas *password protect document* pada *Microsoft Office*, belum dapat dikaji penulis bagaimana teknik atau metode yang digunakan dalam meretas password tersebut. Pada penelitian sebelumnya, penulis sudah pernah mengkaji kinerja algoritma *brute force* dalam meretas *password* yang tidak disandikan, di mana pada kajian ini *password* yang digunakan dalam pengujian merupakan kombinasi

karakter A..Z, a..z, 0..9 dan karakter karakter khusus. Kesimpulan yang di dapat pada kajian ini, kecepatan waktu proses retasi pada *password* tergantung dari panjang dan kombinasi karakter yang digunakan pada *password*, semakin panjang *password* dan kombinasi karakter yang digunakan, maka waktu retasi semakin lama[2]. Dari uraian latar belakang di atas yang menjadi perumusan masalah adalah bagaimana meretas *password protect document Microsoft Office* dengan algoritma *brute force*, Serta bagaimana teknik pengamanan dokumen yang digunakan oleh Microsoft office tersebut. Pada penelitian ini penulis bertujuan untuk mengkaji keamanan pada *protect document* yang digunakan *Microsoft Office* dan merancang aplikasi untuk meretas *password* yang digunakan pada *protect document* dengan menerapkan algoritma *brute force*. Berhubung karena produk aplikasi Microsoft Office ada beberapa jenis, maka dalam penelitian ini penulis hanya fokus pada *protect document* pada microsoft word dan microsoft excel.

2. Algoritma Brute Force

Brute force dipopulerkan oleh Kenneth Thompson yang merupakan algoritma sederhana dan umum digunakan untuk memecahkan masalah *security system* yang menggunakan *password*, dengan tujuan untuk meretas *password* yang dilakukan dengan teknik pendekatan lempang (*straightforward*). Algoritma *Brute Force* dalam meretas *password* bekerja berdasarkan *problem statement* dengan mencoba semua kemungkinan kemungkinan *password*, yang umumnya menggunakan *password* kombinasi karakter a-z, A-Z, 0-9 dan kombinasi karakter karakter khusus pada keyboard. Untuk mendapatkan sebuah kunci yang digunakan dalam *password*, *Brute Force* melakukan percobaan sebanyak n kombinasi sesuai dengan panjang karakter dan kombinasi himpunan karakter yang digunakan dalam *password*. Dengan demikian panjang karakter dan kombinasi himpunan karakter pada *password* yang digunakan sangat mempengaruhi kecepatan proses retasi.

Algoritma *brute force* merupakan algoritma untuk mencocokkan semua teks dengan *pattern*, dimana teks merupakan kata yang dicari yang akan dicocokkan dengan *pattern*, sedangkan *pattern* merupakan kata yang diinput untuk dicocokkan secara rinci. Adapun langkah-langkah yang dilakukan algoritma *brute force* untuk mencocokkan string adalah sebagai berikut :[4]

1. Algoritma *brute force* mulai mencocokkan *pattern* dari awal teks. Di mana :
 Teks : yaitu (*long string*) yang panjangnya n karakter
Pattern : yaitu string dengan panjang m karakter $m < n$ yang akan di cari di dalam teks
2. Dari kiri ke kanan, algoritma ini akan mencocokkan karakter per karakter *pattern*

dengan karakter pada teks yang bersesuaian, sampai salah satu kondisi berikut terpenuhi

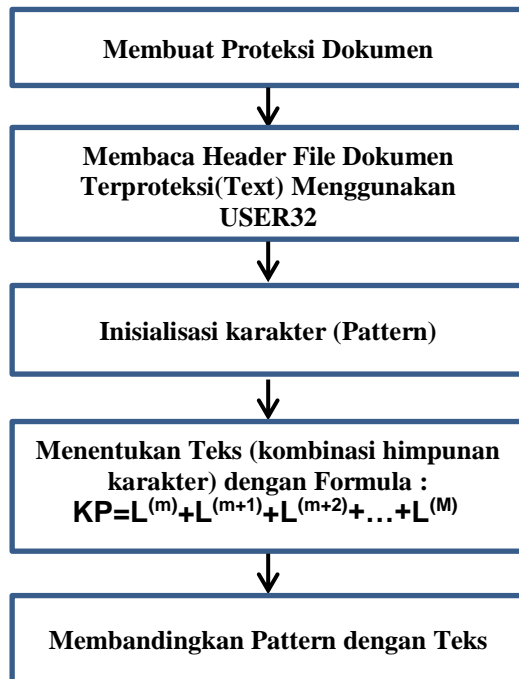
- a. Karakter di *pattern* dan di teks yang dibandingkan tidak cocok.
 - b. Semua karakter di *pattern* cocok, dan kemudian algoritma akan memberitahukan posisi penemuan.
3. Algoritma kemudian terus menggeser *pattern* sebesar satu ke kanan, dan mengulangi langkah-2 sampai *pattern* berada di ujung teks.

Langkah proses pencocokan string dengan algoritma *brute force* ditunjukkan sebagai berikut :[3]

Pattern : SEMNASTIKOM
Teks : PAPERKU SEMNASTIKOM 2016
 Langkah PAPERKU SEMNASTIKOM 2016
 1 SEMNASTIKOM
 2 SEMNASTIKOM
 3 SEMNASTIKOM
 4 SEMNASTIKOM
 5 SEMNASTIKOM
 6 SEMNASTIKOM
 7 SEMNASTIKOM
 8 SEMNASTIKOM
 9 SEMNASTIKOM

3. Metodologi

Metodologi penelitian yang dilakukan penulis dalam kajian keamanan pada *protect document Microsoft Office* dengan menerapkan algoritma *brute force* untuk meretas *password* dokumen terproteksi ditunjukkan pada *frame work* metodologi penelitian gambar 1 di bawah



Gambar 1. Frame Work Metodologi Penelitian

Frame work metodologi penelitian dijelaskan sebagai berikut :

a. Membuat proteksi document

Tahapan ini merupakan tahapan untuk mempersiapkan file document terproteksi dengan memanfaatkan protect document Microsoft office. File document terproteksi yang disiapkan hanya focus pada file document Microsoft word (*.doc , *.docx) dan Microsoft excel (*.xls, *.xlsx)

b. Membaca header file document terproteksi

Pada tahapan ini header file document terproteksi dipanggil dengan menggunakan fungsi "user32" untuk membaca isi file dan diinisialisasikan sebagai variabel text

c. Inisialisasi karakter(Pattern)

Pada tahapan ini karakter password yang digunakan user pada protect document Microsoft office, diasumsikan merupakan himpunan kombinasi karakter a-z, A-Z, 0-9 dan karakter-karakter khusus. Adapun deklarasi variable array untuk menampung set karakter yang digunakan sebagai berikut

```
pass={'a','b','c','d','e','f','g','h','i','j','k','l','m',
'n','o','p','q','r','s','t','u','v','w','x','y','z','A','B',
'C','D','E','F','G','H','I','J','K','L','M','N','O',
'P','Q','R','S','T','U','V','W','X','Y','Z','1','2',
'3','4','5','6','7','8','9','0',' ',' ','@','#','$','%','
'^','&','*','(',')','-',
'+','_','=','{','}','[',']',':',';','"',"'','<','>',',',',',
'?','/','\','|'}
```

d. Menentukan Teks (Kombinasi Himpunan Karakter)

Pada tahapan ini langkah yang dilakukan adalah memproses himpunan karakter yang diinput pada password, langkah berikutnya yang dilakukan adalah mendeklarasikan sebuah variable array yang dijadikan sebagai set karakter (teks). Untuk menampung semua anggota himpunan karakter dan kombinasinya digunakan formula: [1]

$$KP=L^{(m)}+L^{(m+1)}+L^{(m+2)}+\dots+L^{(M)}$$

Di mana :

KP = Kombinasi Password

L = Jumlah karakter dari setiap type password yang diset

m = Panjang minimum karakter set

M = Panjang maximal karakter set

Adapun algoritma yang digunakan untuk mengenerate kombinasi karakter yang digunakan sebagai teks berdasarkan panjang karakter password(*pattern*) sebagai berikut

```
For cCount = 1 To Len(charSet)
  ReDim Preserve cSet(cCount - 1) As Byte
  cSet(cCount - 1) = Asc(Mid(charSet, cCount, 1))
Next
cCount = cCount - 1
For i = 0 To UBound(cSet) - 1
  For j = i To UBound(cSet)
    If cSet(i) > cSet(j) Then
      i_ = cSet(i)
      cSet(i) = cSet(j)
      cSet(j) = i_
    End If
  Next
Next
```

e. Membandingkan Pattern dengan Teks

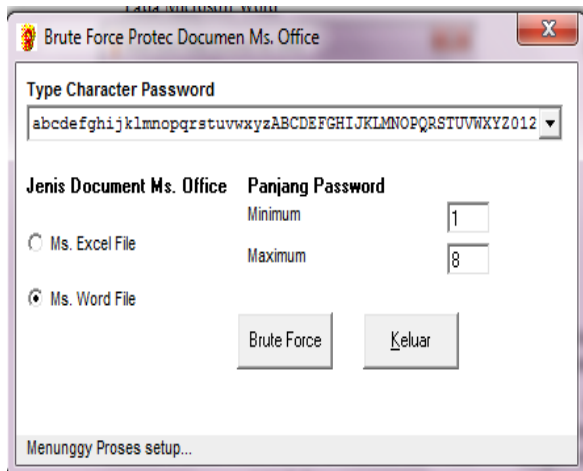
Pada tahapan ini akan dilakukan proses retasi password dengan cara membandingkan *pattern* dengan teks, yang dimulai dari karakter pertama. Di mana apabila pencocokan karakter pertama gagal, maka diteruskan dengan pencocokan karakter berikutnya dengan melakukan penambahan 1 karakter berikutnya pada password. Hal ini dilakukan secara looping hingga ditemukan *pattern* yang merupakan password yang sebenarnya. Adapun algoritma untuk meretas password sebagai berikut :

```
Do While True
  If IsStarting Then
    'Mengenerated String
    xStr = ""
    For i = 0 To pCount
      xStr = xStr cSet(pChar(i))
    Next
    pattern= xStr
    'Jika matching dan keluar
    If pattern= teks Then
      Exit Sub
    end If
  DoEvents
  ' Pencocokan karakter berikutnya
  IncPointers cCount, _
  Len(txtWordToCrack) - 1
End If
Loop
```

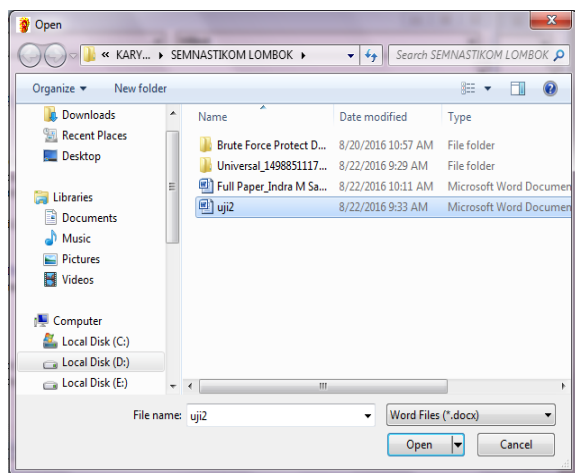
4. Pembahasan

Berdasarkan analisis masalah dan pengujian sistem yang dirancang untuk meretas protect document Microsoft Office dengan menerapkan algoritma brute force berhasil diretas. Hal ini terbukti dari pengujian beberapa file document Microsoft Office pada Microsoft Word dan Excel dengan menggunakan format type penyimpanan yang berbeda. Adapun hasil pengujian dalam meretas protect document sebagai berikut :

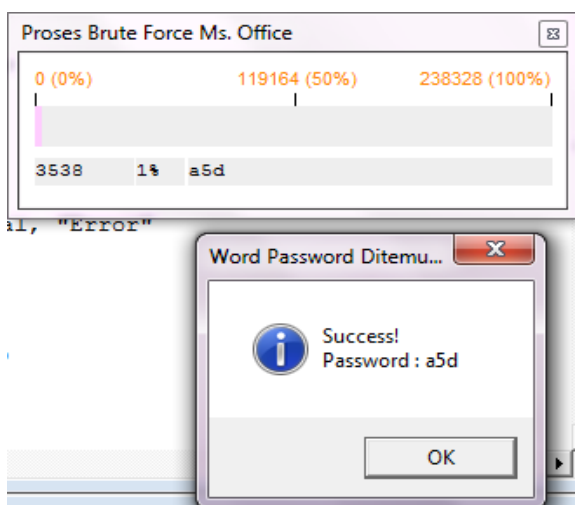
a. Brute Force dalam meretas Protec Document Pada Microsoft Word



Gambar 2. Brute Force Protect Document Ms. Word

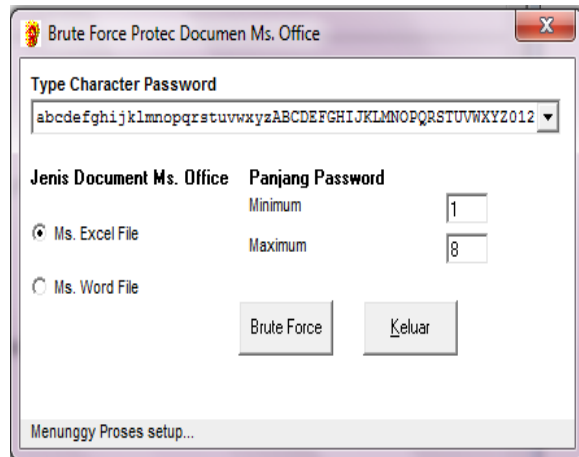


Gambar 3. Proses Buka File Document Ms. Word

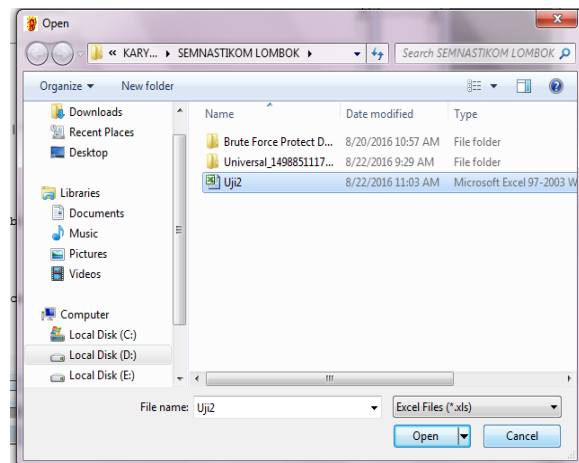


Gambar 4. Proses Retasi Password Protec Document Ms. Word

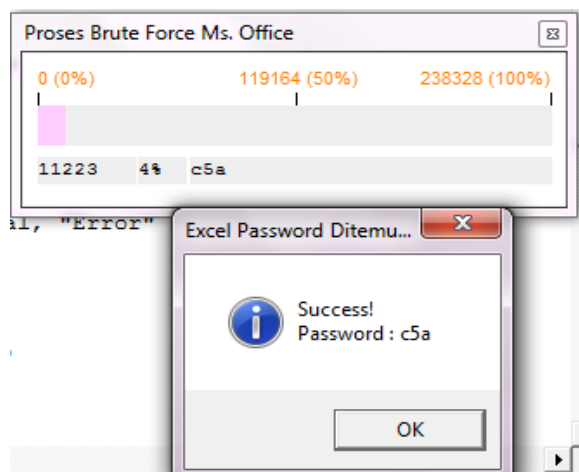
b. Brute Force dalam meretas protect document pada Microsoft Excel



Gambar 5. Brute Force Protect Document Ms. Excel



Gambar 6. Proses Buka File Document Ms.Excel



Gambar 7. Proses Retasi Password Protect Document Ms. Excel

Dari pengujian system yang dilakukan dengan menggunakan type format document Microsoft Word dan Excel yang berbeda diperoleh hasil yang ditunjukkan pada tabel 2 berikut :

Tabel 2. Hasil Pengujian Retasi Password Protect Document Microsoft Word dan Excel

No	Nama File	Type Document	Password
1	uji1.doc	Ms. Word 97-2003	a5c
2	uji2.docx	Ms. Word 2007-2010	a5c
3	uji1.xls	Ms. Exel 97-2003	c5a
4	uji2.xlsx	Ms. Exel 2007-2010	c5a

- [6] http://www.rixler.com/excel_password_recovery.htm, didownload tanggal Akses 05 Agustus 2016 10:42 Wib
- [7] http://www.rixler.com/access_password_recovery.htm, didownload tanggal Akses 05 Agustus 2016 11:05 Wib

5. Kesimpulan

Dari pengujian sistem aplikasi yang dirancang untuk meretas password *protect document* pada Microsoft word dan Excel dengan menerapkan algoritma *Brute Force*, ditarik kesimpulan sebagai berikut :

1. Hasil pengujian dengan system aplikasi yang dirancang dengan menggunakan algoritma brute force, dinyatakan sukses dalam meretas password *protect document*.
2. Kecepatan proses retasi password dengan menggunakan *free software* pada *protect document* Micosoft Word dan Excel lebih cepat jika dibandingkan dengan system aplikasi yang dirancang dengan menggunakan algoritma *brute force*.
3. *Protec document* yang ada pada Micrososft Word dan Excel belum menggunakan algoritma kriptografi untuk menyandikan password yang digunakan.
4. Sebaiknya penggunaan *protect document* pada Microsoft Office diharapkan menggunakan kombinasi karakter a..z, A..Z, 0..9 dan karakter khusus, serta mempertimbangkan panjang password, karena dengan demikian waktu proses retasi akan semakin lama.

Daftar Pustaka

- [1] Krisnaldi Eka Pramudita(2010), "Bruto Force Attack dalam Penerapannya pada Password Cracking" http://www.academia.edu/8679011/Brute_Force_Attack_dan_Penerapannya_pada_Password_Cracking, tanggal akses 05 Agustus 2016 09:20 Wib
- [2] M.Sarkis Indra,"Kajian Algoritma Brute Force dalam Meretas Passwrod tidak Disandakan", Seminar Nasional Ilmu Komputer 2015, USU Press, ISBN :979 458 831 8, PP. 161-164, Agustus 2015.
- [3] Munir, Rinaldi, "*Algoritma Brute Force Bagian 2-Algoritma Brute Force (lanjutan).ppt*" <https://informatikauad.files.wordpress.com/2011/04/6-algoritma-brute-force-bagian-2.ppt>, Tanggal Akses 05 Agustus 2016 15:40 Wib
- [4] Munir, Rinaldi,"*Algoritma Bruto Force Bahan Kuliah Strategi Algoritma*", <http://www.slideshare.net/NURYADI/algoritma-brute-force>, tanggal akses 06 Agustus 2016 11:30 Wib.
- [5] http://www.rixler.com/word_password_recovery.htm, didownload tanggal Akses 05 Agustus 2016 10:14 Wib