Penerapan Kriptografi Pada Aplikasi Penyimpanan Dokumen Pribadi Berupa Teks Pada PC

Pande Made Prajna Pradipa (13510082)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
van_de_made@yahoo.co.id

Abstract*—Makalah ini membahas tentang penerapan kriptografi, dalam menjaga kerahasiaan dokumen pribadi yang kita simpan pada personal computer (PC). Sering kita menyimpan dokumen yang bersifat rahasia pada PC dan ketika ada seseorang yang menggunakan PC kita, terdapat kemungkinan dokumen yang bersifat rahasia tersebut dibuka serta dibaca oleh orang lain. Agar kerahasiaan dokumen tersebut tetap terjaga walaupun telah dibuka oleh orang lain, maka kita menggunakan kriptografi. Dengan kriptografi, dokumen yang pada awalnya dalam bentuk plainteks dienkripsi menjadi cipherteks yang kemudian akan didekripsi kembali menjadi plainteks ketika dibuka kembali oleh si penyimpan data. Proses enkripsi dilakukan dengan melakukan penggeseran k karakter huruf dari karakter huruf semula, dan ketika proses dekripsi, karakter tersebut dikembalikan lagi seperti semula dengan menggeser k karakter huruf ke huruf semula dengan k adalah bilangan bulat positif. Ketika dienkripsi ke dalam bentuk cipherteks, dokumen tersebut akan mengandung karakter yang berbeda dari plainteks dan menyusun kata yang tidak memiliki arti sehingga tidak dapat dimengerti oleh orang awam walaupun dokumen tersebut telah terbuka. Proses enkripsi dan dekripsi ini menggunakan aplikasi yang menerapkan algoritma enkripsi dan dekripsi yang telah dipelajari saat kuliah sebelumnya. Pada algoritma ini tiap karakter huruf dikodekan dengan angka. Kemudian rumus yang digunakan pada algoritma tersebut untuk mengenkripsi adalah $c_i = E(p_i) = (p_i + k) \bmod 256$; dan untuk medekripsi menggunakan rumus $p_i = D(c_i) = (c_i - k) \bmod 256$. Pada rumus tersebut c_i adalah kode berupa angka dari huruf yang dienkripsi dan p_i adalah kode berupa angka dari huruf yang didekripsi. Dalam panerapan rumus ini, kita menggunakan alfabet ASCII yang berjumlah 256 karakter.

***Index Terms*—Kriptografi, Enkripsi, Dekripsi, Plainteks, Cipherteks, Alfabet ASCII.**

I. PENDAHULUAN

Dewasa ini, dalam kehidupan sehari-hari kegiatan manusia tidak terlepas dari penggunaan *personal computer* (PC). Penggunaan PC ini meliputi berbagai kegiatan, baik untuk bekerja, bermain, menonton video, mendengarkan musik, *browsing* internet, ataupun menyimpan dokumen. Dokumen yang disimpan ini ada berbagai macam, seperti musik, video, gambar, dokumen teks, dan sebagainya. Penyimpanan dokumen tersebut ada yang bersifat *public*, sehingga boleh dibuka oleh siapapun, namun ada juga yang bersifat *private* sehingga hanya orang yang menyimpan data yang boleh membukanya. PC yang kita miliki, biasanya tidak hanya kita yang menggunakannya, terkadang ada orang lain yang menggunakanya baik itu orang tua, saudara, ataupun teman. Jika ada orang lain yang menggunakan PC kita, ada kemungkinan dokumen yang bersifat *private* tersebut dapat terbuka dan terlihat oleh orang lain. Maka dari itu diperlukan metode yang membuat dokumen tersebut tidak dapat dimengerti oleh orang lain walaupun telah dibuka. Salah satu metode yang dapat digunakan adalah kriptografi. Pada makalah ini yang akan dibahas berfokus pada penyimpanan dokumen pribadi berupa teks. Dokumen pribadi tersebut yang awalnya berupa plainteks akan dienkripsi menjadi cipherteks. Plainteks adalah teks yang dapat dibaca dan dimengerti maknanya sedangkan cipherteks adalah teks yang telah dienkripsi sehingga tidak dapat dimengerti maknanya. Setelah dienkripsi menjadi cipherteks, dokumen tersebut dapat didekripsi kembali menjadi plainteks sehingga dapat dimengerti maknanya. Untuk melakukan enkripsi dan dekripsi tersebut, kita menggunakan algoritma enkripsi dan dekripsi dengan menggunakan alfabet ASCII yang berjumlah 256 karakter. Dengan menggunakan software yang menerapkan kriptografi ini, maka dokumen tersebut dapat terjaga kerahasiaannya.

II. DASAR TEORI

2.1 Kriptografi

Kriptografi, secara umum, adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

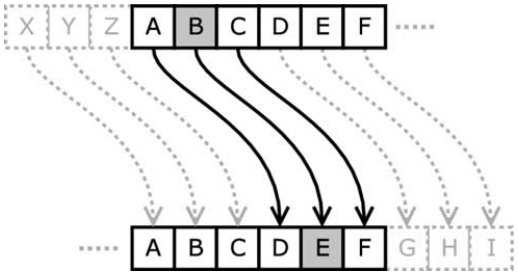
Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

- Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali

yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.

- Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
- Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
- Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Kriptogafi sederhana pernah digunakan pada masa Kaisar Romawi Julius Caesar. Metode yang digunakan disebut *Caesar Cipher*. Pada metode ini enkripsi dilakukan dengan cara menggeser karakter alfabet pada plainteks menuju 3 karakter sesudahnya.



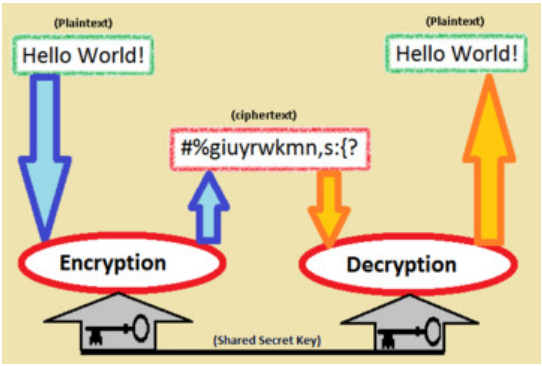
Gambar 1. *Caesar Cipher*

Contohnya:
Plainteks:AWASIASTERIXDANTEMANNYAOBELIX
Cipherteks:DZDVLDVWHULAGDQWHPDQQBREHOLA

2.2 Enkripsi & Dekripsi

Dalam kriptografi, enkripsi adalah proses transformasi informasi, disebut sebagai plainteks, menggunakan algoritma agar tidak dapat dibaca oleh sembarang orang. Hasil dari proses ini adalah informasi terenkripsi yang disebut cipherteks. Cipherteks adalah adalah informasi yang telah disandikan dan tidak memiliki makna lagi.

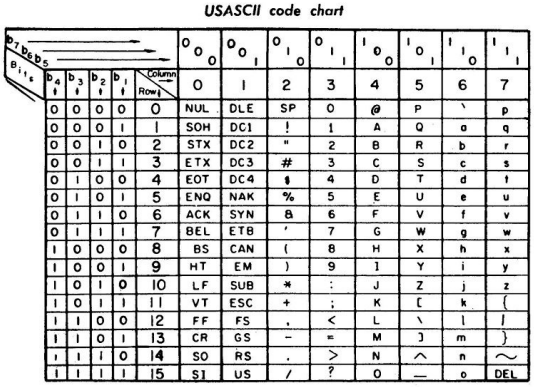
Kebalikan dari enkripsi adalah dekripsi. Dekripsi mentransformasi cipherteks menjadi plainteks kembali sehingga informasi dapat dibaca dan dapat dimengerti maknanya.



Gambar 2. Proses Enkripsi dan Dekripsi

2.3 ASCII

ASCII (American Standard Code for Information Interchange) merupakan suatu standard internasional dalam kode huruf dan simbol, seperti *Hex* dan *Unicode,* tetapi lebih bersifat universal. Kode ASCII memiliki komposisi bilangan biner sebanyak 8 bit dimulai dari 0000 0000 hingga 1111 1111. Total kombinasi yang dihasilkan sebanyak 256, dimulai dari kode 0 hingga 255 dalam sistem bilangan desimal.



Gambar 3. USASCII code chart

III. ANALISIS

Untuk menerapkan kriptografi ini, kita menggunakan algoritma yang didasari oleh metode *Caesar Cipher.* Pada metode *Caesar Cipher,* enkripsi dilakukan dengan menggeser 3 karakter alfabet sehingga:

1. **A** menjadi **D**
2. **B** menjadi **E**
3. **C** menjadi **F**
4. **D** menjadi **G**
5. **E** menjadi **H**
6. **F** menjadi **I**
7. **G** menjadi **J**
8. **H** menjadi **K**
9. **I** menjadi **L**
10. **J** menjadi **M**
11. **K** menjadi **N**

12. **L** menjadi **O**
13. **M** menjadi **P**
14. **N** menjadi **Q**
15. **O** menjadi **R**
16. **P** menjadi **S**
17. **Q** menjadi **T**
18. **R** menjadi **U**
19. **S** menjadi **V**
20. **T** menjadi **W**
21. **U** menjadi **X**
22. **V** menjadi **Y**
23. **W** menjadi **Z**
24. **X** menjadi **A**
25. **Y** menjadi **B**
26. **Z** menjadi **C**

Misalkan setiap huruf dikodekan dengan angka (A=0, B=1,..., Z=25), dari hasil di atas maka untuk melakukan enkripsi dapat dirumuskan sebagai berikut:

Enkripsi: $c_i = E(p_i) = (p_i + 3) \bmod 26$

Sebaliknya untuk melakukan dekripsi kita dapat rumuskan sebagai berikut:

Dekripsi: $p_i = D(c_i) = (c_i - 3) \bmod 26$

Dengan c_i merupakan kode angka dari huruf yang akan dienkripsi dan p_i merupakan kode angka dari huruf yang akan didekripsi.

Rumus di atas berlaku untuk penggeseran 3 karakter dan karakter berjumlah 26. Untuk penggeseran sebanyak k, dimana k adalah bilangan bulat positif, dan karakter berjumlah 256 (jumlah karakter ASCII), maka untuk rumus enkripsinya didapatkan sebagai berikut:

Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 256$

Sebaliknya untuk melakukan dekripsi kita dapat rumuskan sebagai berikut:

Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 256$

Dari rumusan di atas dapat kita buat algoritma untuk melakukan enkripsi yaitu:

```
program enkripsi;
{ Mengenkripsi berkas 'plain.txt'
  menjadi 'cipher.txt' dengan
  metode caesar cipher }
uses
  crt;
var
   F1, F2 : text;
   p : char;
   c : integer;
   k : integer;

begin
   assign(F1, 'plain.txt');
   reset(F1);

   assign(F2, 'cipher.txt');
   rewrite(F2);

   write('k = ?'); readln(k);
   while not EOF(F1) do
    begin
      while not EOLN(F1) do
       begin
         read(F1, p);
         c := (ord(p) + k) mod 256;
         write(F2, chr(c));
       end;
      readln(F1);
      writeln(F2);
   end;
   close(F1);
   close(F2);
end.
```

Gambar 4. Algoritma Enkripsi

Sedangkan algoritma untuk dekripsinya adalah sebagai berikut:

```
program dekripsi;
{ Mendekripsi berkas 'cipher.txt'
  menjadi 'plain2.txt' dengan
  metode caesar cipher }
uses
  crt;
var
   F1, F2 : text;
   p : char;
   c : integer;
   k : integer;

begin
   assign(F1, 'cipher.txt');
   reset(F1);

   assign(F2, 'plain2.txt');
   rewrite(F2);

   write('k = ?'); readln(k);
   while not EOF(F1) do
    begin
      while not EOLN(F1) do
       begin
         read(F1, p);
         c := (ord(p) - k) mod 256;
         write(F2, chr(c));
       end;
      readln(F1);
      writeln(F2);
   end;
   close(F1);
   close(F2)
end.
```

Gambar 5. Algoritma Dekripsi

Kedua algoritma tersebut akan diterapkan pada aplikasi yang digunakan untuk mengenkripsi dan mendekripsi dokumen berupa teks. Pada saat sebelum mengenkripsi dan mendekripsi dokumen, penyimpan dokumen akan diminta memasukkan nilai k yang diinginkan.

Contoh penggunaan aplikasi ini adalah sebagai berikut.

Nama	Tinggi	Berat
Elin Jamilah	160	50
Fariz RM	157	49
Taufik Hidayat	176	65
Siti Nurhaliza	172	67
Oma Irama	171	60
Aziz Burhan	181	54
Santi Nursanti	167	59
Cut Yanti	169	61
Ina Sabarina	171	62

Tabel 1. Contoh Dokumen Dalam Bentuk Plainteks

Dokumen pada Tabel 1 ada dalam bentuk plainteks, jika kita enkripsi maka hasilnya akan terlihat seperti berikut.

Nama	Tinggi	Berat
tüp}vzpz/|t}äyä/{ää	|äzp}	épêp
□□|t}tâpé/spüx/sp	péxü=	ztwxsä□
□□ât|□pâ/ztwxsä□p}/|	}/|tü	spüx/
épêp/|t}t|äzp}/qpêpz	qp}êpz	wxsä
étzp{x/zt□xâx}v□□êp}	päâ/psp	étzp{
spüx/sp{p|/□péxü=/]	xâx}v	ttüzp/|
Ztâxzp/épêp/qtüypp}<	äzp}	}äyä/{
qpwåp/{päâ/psp{pw□	Ztwxs	xâx}v□□
}t|äzp}/qp}êpz/ép{	qp}êp	äzp}/qp

Tabel 2. Contoh Dokumen Dalam Bentuk Cipherteks

Tabel 2 menunukkan hasil enkripsi dari Tabel 1. Hasil enkripsi tersebut dalam bentuk chiperteks dan tidak dapat dimengerti maknanya oleh orang awam. Dengan menggunakan aplikasi ini dokumen tersebut menjadi tidak bisa dibaca oleh orang lain walaupun telah terbuka.

IV. APLIKASI

Ketika di-*instal*, secara otomatis aplikasi ini akan ter-*instal* pada program untuk mengolah kata, seperti *Microsoft Word*, *Word Processor*, *Notepad*, dan lain-lain. Pada saat dokumen berupa teks ini akan disimpan, secara otomatis aplikasi tersebut akan menanyakan apakah dokumen tersebut akan dienkripsikan atau tidak. Jika iya, aplikasi tersebut akan menanyakan nilai k yang diinginkan dan mengenkripsi dokumen tersebut ke dalam bentuk cipherteks sesuai nilai k yang dimasukkan. Dokumen dalam bentuk cipherteks ini yang kemudian akan disimpan.

Jika dokumen ini ingin kita dekripsi, kita tinggal memilih pilihan dekripsi pada menu dan memasukkan nilai k yang pernah kita masukkan pada saat mengenkripsi data. Dekripsi ini akan mentransformasi bentul cipherteks yang karakternya tidak dapat dimengerti maknanya menjadi bentuk plainteks yang dapat kita mengerti maknanya.

Aplikasi ini akan sangat bermanfaat bagi orang-orang yang menyimpan dokumen bersifat *private* pada PC, seperti guru yang menyimpan soal-soal ujian, intelejen yang menyimpan dokumen rahasia, atau remaja yang suka menulis *diary* di PC. Penggunaan aplikasi ini memperkecil kemungkinan terbacanya dokumen tersebut oleh orang lain.

V. KESIMPULAN

Berdasarkan pemaparan yang diungkapkan di atas, aplikasi yang menerapkan kriptografi ini dapat digunakan untuk menjaga kerahasiaan suatu dokumen. Pemanfaatan algoritma enkripsi dan dekripsi menggunakan karakter ASCII dapat sangat bermanfaat untuk menjaga kerahasiaan suatu dokumen pribadi yang bersifat *private*. Aplikasi ini sangat berguna bagi orang-orang yang menyimpan dokumen pribadi pada PC.

VII. ACKNOWLEDGMENT

Ucapan terima kasih pertama-tama Saya haturkan kepada Tuhan YME atas terselesaikannya makalah ini. Kemudian Saya juga mengucapkan terima kasih kepada Pak Rinaldi Munir atas bimbingan beliau selama kuliah serta berbagai referensi yang dapat digunakan untuk

penyelesaian makalah ini. Terima kasih juga Saya ucapkan kepada teman-teman yang telah membantu dan mendukung Saya selama pembuatan makalah ini.

REFERENSI

[1] Munir, Rinaldi, "Matematika Diskrit", Informatika, 2003.

[2] http://www.informatika.org/~rinaldi/Matdis/2011-2012/strukdis11-12.htm
Tanggal akses 11 Desember 2011 07.00 WIB

[3] http://id.wikipedia.org/wiki/Berkas:ASCII_Code_Chart-Quick_ref_card.jpg
Tanggal akses 11 Desember 2011 17.30 WIB

[4] http://id.wikipedia.org/wiki/ASCII
Tanggal akses 11 Desember 2011 17.00 WIB

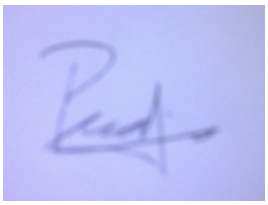
[5] http://id.wikipedia.org/wiki/Kriptografi
Tanggal akses 11 Desember 2011 16.00 WIB

[6] http://en.wikipedia.org/wiki/Encryption
Tanggal akses 11 Desember 2011 16.00 WIB

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, 12 Desember 2011



Pande Made Prajna Pradipa