IMPLEMENTASI TEKNIK ENKRIPSI ONE-TIME PAD DENGAN MENGGUNAKAN GAMBAR SEBAGAI KUNCI

Abu Bakar Gadi – NIM : 13506040

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16040@students.if.itb.ac.id

Abstrak

Makalah ini membahas implementasi sebuah teknik kriptografi yang merupakan hasil pengembangan dari teknik kriptografi klasik *one-time pad*. Pada teknik kriptografi baru yang telah diimplementasikan oleh penulis ini, karakteristik utama dari teknik kriptografi klasik *one-time pad* masih tetap dipertahankan yaitu digunakannya sebuah kunci yang benar-benar random, yaitu dengan digunakannya gambar sebagai kunci. Pada makalah ini penulis juga akan menjabarkan lebih lanjut teknik pemanfaatan gambar sebagai kunci. Aplikasi teknik kriptografi ini dapat diunduh di http://s.itb.ac.id/~abu_gadi/one_time_pad.zip .

***Kata kunci**:* kriptografi klasik, tingkat keabuan pixel (RGB), kunci *random, one-time pad, unbreakable cipher*.

1. Pendahuluan

Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi dikenal sejak zaman romawi kuno. Pada zaman itu Caesar menggunakan kriptografi untuk menyamarkan pesan, sehingga pihak yang tidak berkepentingan (musuh) tidak dapat mengerti apa isi pesan yang sebenarnya. Namun pada zaman itu masih diterapkan teknik yang sederhana untuk melakukannya. Teknik pertama yang digunakan adalah substitusi satu karakter pada teks asli dengan karakter lain. Teknik berikutnya adalah transposisi (pengubahan posisi) karakter pada teks aslinya. Penggunaan kunci pada algoritma kriptografi klasik juga masih sederhana. Pada teknik Caesar Cipher sebagai contoh, kuncinya adalah pergeseran huruf.

Inti dari kriptografi adalah kerahasiaan kunci untuk dekripsi, algoritma yang digunakan pada proses enkripsi bukanlah sesuatu yang bersifat rahasia. Namun masalah kerahasiaan kunci ini masih dapat dipecahkan dengan teknik kriptanalisis yang memanfaatkan frekuensi kemunculan huruf pada cipherteks. Dengan menggunakan teknik kriptanalisis, seorang kriptanalis juga dapat menemukan kunci yang dipakai dengan teknik tertentu.

Jika masih ada kemungkinan kunci atau plainteks dapat ditebak, maka teknik kriptografi tersebut masih belum memiliki tingkat keamanan yang sempurna. Sehingga untuk tingkat kemanan yang sempurna, diperlukan suatu teknik kriptogafi yang tidak dapat dipecahkan (*unbreakable cipher*). Untuk dapat membuat suatu teknik kriptografi yang tidak dapat dipecahkan, maka ada syarat yang harus dipenuhi, yaitu kunci harus dipilih secara acak (bukan berupa suatu kata atau kalimat yang bermakna) dan panjang kunci harus sama dengan panjang plainteks yang akan dienkripsi.

2. Dasar Teori

2.1 One-Time Pad

Satu-satunya teknik kriptografi yang memenuhi syarat-syarat tersebut adalah teknik *one-time pad* yang ditemukan pada tahun 1917 oleh Vernam dan Major Joseph Mauborgne. Teknik enkripsi dan dekripsi algoritma *one-time pad* sangatlah sederhana, namun kekuatan sesungguhnya pada algoritma ini terletak pada kuncinya. Kunci yang digunakan pada algoritma ini adalah berupa karakter alfabet yang ditulis pada sebuah buku / lembaran. Jumlah karakter kunci yang digunakan dalam proses enkripsinya adalah sebanyak

karakter plainteksnya. Ilustrasi berikut ini akan menunjukkan cara kerja *one-time pad*.

Plainteks :

a	k	u	g	a	n	t	e	n	g

Kunci random pada “pad” :

f	a	a	f	k	t	e	j	g	k

Cipherteks :

g	l	v	m	l	h	y	o	u	r

Dalam menghasilkan cipherteks tersebut, hanya dilakukan operasi penjumlahan sirkuler karakter biasa untuk proses enkripsi (dengan asumsi karakter yang diproses adalah alfabet), yaitu :

$c_i = E(p_i) = (p_i + k) \bmod 26$

untuk proses dekripsi, dilakukan hal kebalikannya, yaitu :

$p_i = D(c_i) = (c_i - k) \bmod 26$

keterangan :
k = kunci rahasia
c_i = karakter cipherteks
p_i = karakter plainteks

Hal yang membuat teknik OTP (*one-time pad*) ini tidak mungkin terpecahkan adalah acaknya kunci yang tertulis dalam buku tersebut. Tidak ada dasar pemilihan karakter yang dituliskan dalam buku kunci tersebut. Semuanya ditentukan benar-benar secara acak.

Namun teknik ini tidak umum digunakan karena alasan kepraktisan. Antara lain adalah keharusan pihak pengirim dan penerima untuk memiliki buku kunci yang sama, selain itu kunci yang diperlukan adalah sepanjang plainteks yang ada, sehingga tentu akan berukuran besar jika plainteks yang akan dienkripsi berukuran besar pula. Masalah keamanan juga muncul disini. Saat pihak pengirim pesan akan memberitahukan kunci (buku kunci) yang digunakan kepada pihak penerima, maka keamanan disaat pengiriman harus dijaga sedemikian rupa sehingga buku kunci tersebut dapat tersampaikan ke penerima pesan. Terlebih lagi apabila buku kunci tersebut dikirimkan ke pihak penerima melewati kurir (dengan asumsi penggunaan kurir adalah cara yang paling aman), pasti akan mengundang kecurigaan orang-orang yang melihatnya (tidak menutup kemungkinan, kurir bisa saja bertindak tidak jujur), sehingga proses dekripsi oleh penerima nantinya akan menjadi bermasalah.

2.2 Hasil Pengembangan One-Time Pad

Pada teknik kriptografi yang telah penulis implementasikan, kunci yang digunakan adalah berupa sebuah gambar dengan ukuran tertentu. Dengan mengakses tiap-tiap pixel dari gambar tersebut, dapat diperoleh bilangan-bilangan acak (dari intensitas RGB / tingkat keabuan masing-masing pixel) yang memenuhi syarat jika dijadikan kunci untuk sebuah teknik kriptografi yang unbreakable. Karena kunci yang digunakan adalah berupa gambar, maka masalah kepraktisan dapat diatasi. Masalah keamanan pada saat pendistribusian kunci ke pihak penerima juga dapat diatasi, karena gambar tentu saja bukanlah merupakan suatu hal yang mencurigakan. Penjelasan lebih lanjut mengenai penggunaan gambar sebagai kunci ada pada bagian berikutnya. Adapun fungsi enkripsi yang digunakan adalah sama seperti algoritma *one-time pad* yang sebenarnya, namun karakter yang ditangani adalah karakter ASCII-256.

2.3 Penggunaan Gambar Sebagai Kunci

Pada hasil implementasi teknik kriptografi yang penulis usulkan ini, digunakan kunci berupa gambar. Penulis menjadikan gambar sebagai kunci karena gambar mengandung informasi nilai dalam tiap pixelnya. Informasi tersebut adalah tingkat keabuan. Satu pixel dalam gambar mengandung informasi nilai sebesar 24 bit. Delapan bit pertama mewakili intensitas warna merah (*Red*), delapan bit kedua mewakili intensitas warna hijau (*Green*), dan 8 bit terakhir mewakili intensitas warna biru (*Blue*). Dengan memanfaatkan informasi dari intensitas keabuan tiap-tiap pixel yang terkandung dalam suatu gambar tersebut, kita dapat memperoleh suatu kunci yang benar-benar acak.

Keacakan (*randomness*) kunci ini dapat kita peroleh karena pada suatu gambar, apabila kita mengambil sampel dua buah pixel yang berwarna mirip (bahkan mata manusia tidak dapat mendeteksi perbedaan warna keduanya) kemudian mencocokkan nilai intensitas keabuan (intensitas merah, hijau, dan birunya), maka kita akan mendapati perbedaan pada nilai intensitas keabuan masing-masing pixel. Setidaknya ada

perbedaan nilai pada salah satu intensitas warna merah, hijau, atau biru. Kecuali memang dua pixel tersebut benar-benar serupa. Namun hal ini sangat jarang terjadi pada suatu kunci gambar yang berkualitas baik.

Hal yang perlu diingat dalam algoritma *one-time pad* ini adalah bahwa panjang kunci adalah harus sama panjang dengan panjang plainteksnya. Sehingga apabila gambar yang digunakan sebagai kunci berukuran kecil dan tidak mencukupi apabila digunakan untuk memproses seluruh karakter plainteks, maka solusinya adalah dengan menggunakan kunci itu secara sirkuler. Apabila hingga pixel terakhir pada gambar telah digunakan namun masih tersisa plainteks/cipherteks yang belum diproses, maka kunci akan kembali menunjuk ke pixel awal yang ada di gambar dan begitu seterusnya.

Proses yang dilakukan dalam penetapan kunci adalah dengan melakukan penelusuran / iterasi pixel per pixel dari gambar. Posisi pixel direpresentasikan dengan sebuah matriks. Proses iterasi ini dilakukan dari posisi pixel paling kiri atas dan bergerak ke kanan pada tiap barisnya hingga sampai pada posisi pixel paling kanan bawah dan kembali ke awal lagi apabila kunci belum sama panjang dengan plainteks. Pada iterasi pertama kita mengambil nilai intensitas merah dari pixel tersebut sebagai bagian dari kunci, pada iterasi ke pixel berikutnya kita memilih intensitas warna hijau dari pixel tersebut, pada iterasi berikutnya kita memilih intensitas warna biru dari pixel, kemudian kembali lagi memilih intensitas warna merah dari pixel, dan begitu seterusnya (sirkuler) hingga didapatkan kunci yang terdiri dari deretan angka 8 bit sebanyak jumlah pixel dalam gambar (lebar x tinggi).

Penulis menetapkan untuk melakukan iterasi secara terurut dari kiri-atas hingga kanan-bawah karena dalam suatu gambar yang tergolong baik untuk dijadikan sebagai kunci, maka dua pixel yang bersebelahan akan memiliki intensitas warna merah, hijau, atau biru yang berbeda. Sehingga tidak diperlukan teknik khusus dalam penentuan urutan pixel yang akan diambil informasi warnanya. Karena menurut pendapat penulis, hal itu akan menghasilkan keacakan kunci yang tidak jauh berbeda. Disamping itu, juga tentu akan lebih sukar dalam implementasinya. Oleh karena itu diperlukan gambar yang memiliki tingkat keacakan pixel (*pixel randomness*) yang tinggi. Pada bagian berikut ini akan dijabarkan secara singkat cara menentukan kualitas dari kunci yang digunakan. Teknik ini juga penulis tambahkan sebagai fitur dalam aplikasi yang penulis buat.

2.4 Penentuan Kualitas Kunci

Semakin tinggi tingkat keacakan pixel pada suatu gambar, maka akan menghasilkan kualitas enkripsi yang lebih baik lagi. Dalam aplikasi yang telah diimplementasikan oleh penulis, untuk menentukan kualitas suatu gambar yang akan dijadikan kunci, penulis menggunakan sebuah teknik yang sederhana yaitu menggunakan perbandingan total intensitas keabuan (intensitas warna merah + hijau + biru) antara suatu pixel dengan pixel yang bersebelahan. Jumlah pixel yang memiliki warna yang sama ataupun tidak dengan pixel sebelahnya dicatat. Kemudian di akhir proses, kita akan mendapatkan total pixel yang berwarna sama dengan pixel sebelahnya dan total pixel yang berwarna berbeda dengan pixel sebelahnya. Dari kedua nilai itu dapat diperoleh suatu persentase keacakan pixel dari suatu gambar yang dapat dihitung sebagai berikut :

$$\text{Keacakan pixel} = \frac{\boldsymbol{B}}{\boldsymbol{S+B}} * \mathbf{100}\%$$

keterangan :
B = ∑ pixel berwarna beda dengan sebelahnya
S = ∑ pixel berwarna sama dengan sebelahnya

3. Hasil dan Analisis

3.1 Pengujian

Pada bagian ini penulis akan memberikan beberapa contoh hasil penggunaan aplikasi hasil implementasi pengembangan teknik *one-time pad*. Pada tiap pengujian digunakan kunci yang berbeda. Berikut ini adalah plainteks yang digunakan dalam pengujian enkripsi.

Plainteks :

AAAAAAAAAAlike many commuters i spent the first part of monday morning standing at the station despite the warnings, believing that a miracle might happen and my train might still arrive to take me AAAAAAAAAA on the daily trip to london. watching the weather output and talking to colleagues who made it into the office, it was clear that we were experiencing an unusual event. AAAAAAAAAA

3.1.1 Pengujian Pertama

Kunci :

Dimensi : 1600 x 1200 pixel
Keacakan Kunci : 95.17 %
Hasil Enkripsi :

Ã¼Ã-Ã ÃªÃ¶Ã¨ÃšÃ‹Ã©Ã¹$
Ã˜#Ã¡.7*Ã¾= Ã’Â½%!5Ã¦-Ã .
Â£Ã¾@OÃ›Ã´ÃˆÂ¨Ã¾Ã¯ Ã¨Ã¡ÃœÃ³
Â Ã©Ã³-*,Ã˜%'!$"+B#ÃŒ3Ã˜8 Â¸!#"1Ã·ÃŽ-
$ÃŠÃŒ
Ã¹Ã¿Ã¤Ã Â½Ã‡Ã½Ã°Ã‰Ã©ÃžÃ²Â¡ÃšÂ Ã
ÃªÃµÃ˜Ã’Ã Ã–Â Ã Ã Â§Â¼Ã–
Â«Ã¬ÃŸÃ-Ã¶Ã©Ã³Â–
Ã™Ã›Ã¢ÂšÃ©Ã²Â‘Ã¹Ã·Ã¨Ã¤Ã¯Â‘Ã§Ã¬Â¼
Ã¾ÃªÃ™Ã³

3.1.2 Pengujian Kedua

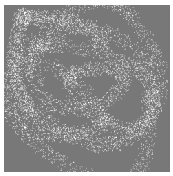
Kunci :

Dimensi : 241 x 241 pixel
Keacakan Kunci : 14.93 %
Hasil Enkripsi :

A AA A ÇikÀ È**any**{**com**ÈÐÏeÍÎ
i{**Îpen**Ï
ÏÃe{ÁÄÍÎÏ{Ë¼ÍÏ{ÊÁ{ÈÊÉ¿¼Ô{ÈÊÍÉÄÉÂ{ÎÏ¼
É¿ÄÉÂ{¼Ï{ÏÃÀ{ÎÏ¼ÏÄÊÉ{¿ÀÎËÄÏÀ{ÏÃÀ{Ò¼
ÍÉÄÉÂÎ {½ÀÇÄÀÑÄÉÂ{ÏÃ¼Ï{¼{ÈÄÍ¼¾Ç
À{ÈÄÂÃÏ{Ã¼ËÈÀÉ{¼É¿{ÈÔ{ÏÍ¼ÄÉ{ÈÄÂÃÏ
{ÎÏÄÇÇ{¼ÍÍÄÑÀ{ÏÊ{Ï¼ÆÀ{ÈÀ{
{ÊÉ{ÏÃÀ{¿¼ÄÇÔ{ÏÍÄË{ÏÊ{ÇÊÉ¿ÊÉ {
Ò¼Ï**ching** Ïhe{wÀ¼thÀr{oÐtËÐÏ{¼É¿
talÆinÂ{tÊ{colle¼ÂÐÀÎ{ÒÃÊ{È¼¿À{ÄÏ{ÄÉÏ
Ê{ÏÃÀ{ÊÁÁÄ¾À {ÄÏ{Ò¼Î{¾ÇÀ¼Í{ÏÃ¼Ï{Ò
À{ÒÀÍÀ{ÀÓËÀÍÄÀÉ¾ÄÉÂ{¼É{ÐÉÐÎÐ¼Ç{
ÀÑÀÉÏ {

3.1.3 Pengujian Ketiga

Kunci :



Dimensi : 241 x 241 pixel
Keacakan Kunci : 16.12%
Hasil Enkripsi :

¹¹¹¹¹¹¹¹¹äáãÝ åÙæñ ÛçååíìÝêë á ëèÝæì ìà
Ý Þáêëì èÙêì çÞ åçæÜÙñ åçêæáæß ëìÙæ
Üáæß Ùì ìàÝ ëìÙìáçæ-
ÜÝëèáìÝ ìàÝ ïÙêæáæßë¤ aÝäáÝîáæß ìà`ì
`-
åhêÙbäÝ åhßàs àÙèèÝæ ÙæÜ lñ ìq`ám
åhfàs ëìáää ÙêêáîÝ ìç ìÙãÝ åÝ ¹¹¹¹¹¹¹¹¹
çæ ìàÝ ÜÙáäñ ìêáè ìç äçæÜçæ¦ ïÙìÛàáæ
ß ìàÝ ïÝÙìàÝê çíìèíì ÙæÜ ìÙäãáæß ìç
ÛçääÝÙßíÝë ïàç åÙÜÝ áì áæìç ìàÝ çÞÞ
áÛÝ¤ áì ïÙë ÛäÝ`ê sàÙì ïÝ ïÝêÝ Ýðè
dêáÝæÛáæf Ùæ íæíëíÙä dîÝæì¦ ¹¹¹¹¹¹@¹¹¹

*Catatan :
Hasil yang tercetak dalam kotak bisa jadi tidak sama dengan hasil dari aplikasi, karena ada karakter-karakter khusus yang *non-printable*.

3.2 Analisis Pengujian

Pada pengujian pertama digunakan kunci dengan dimensi 1600 x 1200 pixel dengan tingkat keacakan kunci 95.17%. Hasil enkripsinya menunjukkan sesuatu yang sudah sangat jelas bahwa cipherteks tersebut tidak dapat dipecahkan dengan analisis frekuensi karena sudah tidak memiliki hubungan statistik apapun dengan plainteks.

Pada pengujian kedua digunakan kunci dengan dimensi 241 x 241 pixel dengan tingkat keacakan kunci 14.93 %. Walaupun tingkat keacakannya rendah, hasil enkripsinya sudah tidak menunjukkan hubungan statistik apapun dengan plainteksnya. Namun yang perlu dijadikan perhatian adalah kemunculan potongan-potongan cipherteks yang masih sama dengan plainteksnya. Pada kotak hasil enkripsi pengujian kedua, diperlihatkan dengan adanya beberapa potongan cipherteks yang dicetak tebal. Sebagai contoh potongan “com” yang pada

plainteksnya berada dalam kata commuters dan “ching” yang berada dalam kata watching. Hal ini disebabkan karena pada posisi karakter-karakter tersebut, secara berurutan, pixel-pixel yang diambil informasi intensitas keabuannya berwarna hitam 100%, dengan demikian intensitas warna merah, hijau, dan birunya adalah 0. Sehingga sederetan karakter yang bersesuaian dengan pixel-pixel hitam tersebut akan ditambahkan dengan 0 dan akan menghasilkan karakter cipher yang sama dengan karakter aslinya.

Pada pengujian ketiga digunakan kunci dengan dimensi 241 x 241 pixel dengan tingkat keacakan kunci 16.12 %. Walaupun tingkat keacakannya rendah, hasil enkripsinya menunjukkan cipherteks yang cukup baik. Namun masih ditemui beberapa potong cipher yang berulang. Hal ini dipengaruhi oleh tingkat keacakan yang kurang tinggi. Akan tetapi tidak ditemui kasus seperti pengujian kedua, yaitu munculnya potongan cipherteks yang sama seperti plainteksnya. Hal ini disebabkan karena pada pengujian yang ketiga ini, gambar yang digunakan sebagai kunci tidak mengandung deretan pixel berwarna hitam yang bersebelahan.

4. Kelebihan dan Kekurangan

Kelebihan yang dapat dirasakan dari hasil implementasi teknik kriptografi ini adalah :

- Kunci yang berupa gambar sangatlah mudah untuk ditemukan atau dibuat (praktis) dan pendistribusian kunci ini ke pihak penerima pesan dapat dilakukan dengan lebih mudah dan relatif lebih aman.
- Proses enkripsi dan dekripsi yang relatif cepat karena dalam algoritmanya tidak melibatkan operasi matematis yang rumit (hanya melibatkan penambahan dan pengurangan).
- Kualitas gambar yang dijadikan kunci dapat diketahui.
- Cukup baik untuk digunakan dalam mengenkripsi file-file teks.

Adapun kekurangan dari implementasi teknik kriptografi ini antara lain :

- Ukuran kunci yang relatif besar karena harus meyesuaikan dengan panjang plainteks.
- Proses pembuatan kunci (memindahkan dari gambar ke struktur internal aplikasi) membutuhkan waktu yang cukup lama untuk gambar-gambar berukuran besar.
- Aplikasi belum dapat menerima file binary untuk diproses.

5. Kesimpulan dan Saran Pengembangan

Kesimpulan yang dapat diambil dari pembahasan makalah ini adalah :

- Penggunaan kunci yang benar-benar random dalam algoritma *one-time pad* bertujuan untuk menghilangkan hubungan statistik dalam cipherteks yang dihasilkan dari proses enkripsinya, sehingga kriptanalis tidak dapat melakukan analisis frekuensi terhadap cipherteks.
- Pengembangan teknik kriptografi *one-time pad* yang penulis telah lakukan ini dapat mengatasi masalah kepraktisan kunci yang pada awalnya menjadi kendala utama bagi teknik *one-time pad* pada mulanya.
- Gambar menyimpan informasi nilai intensitas keabuan pada setiap pixelnya dan dapat dimanfaatkan sebagai kunci yang bersifat random.
- Tingkat keacakan gambar yang digunakan sebagai kunci juga turut mempengaruhi kualitas hasil enkripsi dalam teknik kriptografi hasil pengembangan ini.
- Sekumpulan pixel berwarna hitam yang bersebelahan pada gambar dapat mengakibatkan hasil enkripsi pada posisi tersebut sama dengan plainteksnya pada posisi yang bersesuaian. Sehingga gambar yang mengandung sekumpulan pixel berwarna hitam pada daerah tertentu sebaiknya tidak dijadikan sebagai kunci.

Adapun saran yang dapat penulis sampaikan kepada pembaca agar suatu saat penelitian kecil ini dapat dikembangkan lebih lanjut adalah sebagai berikut :

- Kemampuan aplikasi untuk melakukan proses terhadap file binary belum dapat terealisasikan oleh penulis karena satu dan lain hal. Sehingga penulis menyarankan pengembangan lebih lanjut agar dapat dilakukan proses terhadap file binary.
- Menggunakan tipe file lain seperti wav atau midi (file suara dengan ukuran relatif kecil) sebagai kunci untuk teknik kriptografi *one-time pad*.

- Pengujian sebaiknya dilakukan dengan menggunakan sampel file teks yang panjang dan dianalisis dalam bentuk heksadesimal agar hasil analisis menjadi lebih presisi.
- Dapat digabungkan dengan algoritma-algoritma kriptografi yang beroperasi pada block data (*block cipher*), sehingga akan didapatkan suatu teknik kriptografi baru yang lebih kuat.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. *Kriptografi*, Penerbit Informatika, 2006.