STUDI MENGENAI TEKNIK KRIPTOGRAFI "CHAFFING AND WINNOWING"

Tommy Gunardi (13507109)

Institut Teknologi Bandung
Sekolah Teknik Elektro dan Informatika, Program Studi Teknik Informatika
Jl. Ganesha no 10, Bandung
e-mail: if17109@students.if.itb.ac.id , tommy_gunardi@hotmail.com

ABSTRAK

Seiring berjalannya waktu, teknologi dan komunikasi berkembang dengan sangat pesat. Kita dapat dengan mudah berkomunikasi dengan orang lain dengan bantuan teknologi informasi saat ini. Namun tidak selamanya pesan yang kita kirimkan sampai ke penerima. Tidak jarang pesan kita jatuh ke tangan pihak ketiga. Tentu hal ini tidak kita inginkan. Oleh karena itu diperlukan teknik kriptografi yang tepat untuk merahasiakan pesan. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan sebuah pesan. Dewasa ini, da beberapa teknik kriptografi yang cukup dikenal, yaitu enkripsi (mengubah plainteks menjadi cipherteks) dan steganografi (menyembunyikan pesan di dalam sebuah pesan lain). Kedua teknik ini menarik karena sama-sama dapat menyembunyikan pesan dengan cara yang unik. Namun ternyata ada banyak teknik lain yang tidak kalah menarik. Salah satu teknik tersebut adalah "Chaffing and Winnowing". Dengan teknik ini, kita tidak perlu mengenkripsi pesan menjadi cipherteks. Pesan yang dikirimkanpun tidak disembunyikan, melainkan digabungkan dengan pesan-pesan lainnya. Pada kesempatan kali ini, penulis akan membahas studi tentang teknik kriptografi "Chaffing and Winnowing", dan membandingkannya dengan teknik-teknik kriptografi lainnya.

Kata kunci: kriptografi, enkripsi, chaffing and winnowing.

1. PENDAHULUAN

Tujuan dari teknik sekuritas adalah kerahasiaan. Kita perlu memastikan bahwa pihak ketiga tidak mendapat informasi sedikitpun dari pesan yang kita kirimkan. Teknik Kriptografi dikembangkan terus menerus agar dapat dikatakan sempurna, yaitu aman dari serangan kriptanalisis. Seperti yang dibahas pada abstrak, ada dua macam teknik kriptografi yang cukup dikenal yaitu:

- Enkripsi
  Teknik ini mengubah pesan menjadi cipherteks dimana pihak ketiga yang ingin membaca cipherteks tidak dapat mengetahui isi dari pesan tersebut. Penerima yang memiliki otoritas untuk membuka pesan memiliki sebuah kunci deskripsi yang digunakan untuk mendekripsi pesan tersebut agar kembali ke bentuk plainteks semula. Kunci yang digunakan untuk menenkripsi atau mendekripsi pesan mungkin saja berbeda atau sama, namun pastinya ada relasi antara kedua kunci. Contoh skema enkripsi yang cukup dikenal adalah DES dan RSA.

- Steganografi
  Seni menyembunyikan suatu pesan rahasiadi dalam suatu pesan yang lebih besar dengan suatu cara sehingga pihak ketiga tidak dapat mengetahui keberadaan atau isi dari pesan rahasia. Contohnya, suatu pesan mungkin saja disembunyikan ke dalam suatu gambar dengan cara mengubah least significant bit dari gambar menjadi isi dari pesan.

Pada tahun 1998 Ronald Rivest, seorang mahasiswa computer science dari MIT, mengajukan suatu teknik kriptografi baru yang bernama "Chaffing and Winnowing". Teknik ini tidak menggunakan "encryption keys", namun menggunakan "authentication keys". Dimana pesan yang ingin dikirimkan tidak dienkripsi sama sekali, namun seperti dicampurkan dengan pesan palsu sehingga isi pesan asli tersamarkan.

2. METODE CHAFFING AND WINNOWING

2.1 Sistem

Chaffing and Winnowing menganalogikan metodanya dalam bahasa pertanian. Chaff adalah bagian tidak berguna dari grain, dan Winnowing adalah aksi untuk memisahkan Chaff dari Grain. Chaffing and Winnowing

menggunakan pendekatan yang berbeda untuk merahasiakan pesan. Teknik ini menyediakan kerahasiaan lewat autentikasi. Ada dua tahap yang kita lakukan dalam mengirim pesan, yaitu authenticating (menambahkan MAC) dan menambahkan Chaff.

Pengirim memecah pesan menjadi paket-paket dan mengauhentikasi masing-masing paket dengan menggunakan *authentication key* yang rahasia. Sender menambahkan MAC (*Message Authentication Code*) yang sudah diautentikasi dengan *authentication key* rahasia ke masing-masing paket, sehingga paket sekarang berisi :

(isi pesan, MAC)

Isi dari paket masih jelas. Tidak ada enkripsi yang dilakukan. Kita mengasumsikan mengautentikasi pesan dengan menambahkan MAC tidak dikatakan sebagai enkripsi terhadap pesan. MAC sendiri adalah fungsi (hash) satu arah yang menggunakan kunci rahasia (secret key), dalam pembangkitan nilai hash. Dengan kata lain, nilai hash adalah fungsi dari pesan dan kunci.

Ada sebuah kunci rahasia yang dimiliki bersama antara sender dengan receiver untuk mengautentikasi isi masing-masing paket. Receiver yang berhak, mngetahui authentication key dan dapat mengetahui paket diautentikasi dengan merecomputing MAC dan membandingkannya dengan MAC yang diterima. Jika pembandingan gagal, paket dan MAC yang diperiksa secara otomatis dibuang. Fungsi autentikasi dapat dipilih berdasarkan keinginan, misalnya saja teknik Diffie-Hellman.

Selain MAC, kita juga memerlukan serial number yang khas ke dalam masing-masing paket. Contohnya, jika file yang panjang dipecah menjadi paket-paket yang lebih kecil, dan masing-masing paket memiliki serial number yang unik. Serial number membantu penerima membuang paket yang sudah diduplikasi, mengidentifikasi apabila ada paket yang hilang, dan mengatur urutan paket yang diterima. Sehingga bentuk paket :

(serial number, isi pesan, MAC)

Sebagai contoh, kita mungkin memiliki sekuens sebagai berikut:

(1, Hi Leonardo, 282739)
(2, Meet me at, 384723)
(3, 7PM, 345234)
(4, Love-Xixi, 985734)

Setelah proses pertama, yakni mengautentikasi pesan selesai menjadi bentuk di atas, kita dapat memulai proses yang kedua, yaitu menambahkan paket tiruan dengan MAC palsu. Secara umum, paket-paket palsu (chaff packets) memiliki format yang benar, yakni memiliki serial number dan isi pesan yang masuk akal, namun memiliki MAC yang tidak valid. Paket-paket palsu ini dapat dicampurkan ke dalam paket-paket yang benar (wheat packets) untuk merekayasa isi pesan yang sebenarnya. Sehingga sekuens paket-paket yang kita miliki sekarang adalah sebagai berikut:

(1, Hi Leonardo, 282739)
(1, Hey Arnold, 293841)
(2, Meet me at, 384723)
(2, I'll come to your house at, 948573)
(3, 5PM, 374659)
(3, 7PM, 345234)
(4, Love-Xixi, 985734)
(4, Love-Grace, 875639)

Dalam kasus ini, untuk setiap serial number, ada masing-masing sebuah paket yang benar(wheat) dan sebuah paket palsu(chaff). Selain secara berurutan paket-paket juga dapat dikirim secara acak.

Untuk mendapatkan pesan sebenarnya, penerima harus membuang semua paket palsu, sehingga memperoleh paket-paket sebenarnya.

2.2 Tingkat Kerahasiaan

Tingkat kerahasiaan dari Chaffing and Winnowing dapat dipengaruhi oleh beberapa faktor. Faktor pertama yakni mengenai algoritma MAC yang digunakan. Algoritma MAC harus aman dan jarang sekali menghasilkan nilai MAC ganda. Maksud nilai MAC ganda di sini adalah nilai MAC untuk dua pesan yang berlainan sama. Contohnya **(Hi Amber, 203948)** dan **(How are You, 203948)**. Pada kasus ini hasil fungsi MAC untuk kedua pesan yang berbeda sama.

Hal lain yang perlu diperhatikan adalah bagaimana membagi pesan menjadi paket-paket. Sebaik apapun teknik *Chaffing & Winnowing* yang digunakan, jika pembagian pesan menjadi paket dilakukan dengan sembrono, maka pihak lawan dapat dengan mudah mengetahui isi dari pesan asli yang dikirimkan. Semakin kecil isi paket yang akan dikirimkan, semakin aman tingkat kerahasiaannya.

Bagian terakhir adalah prosedur penambahan paket *Chaff* yang digunakan. Penambahan paket *Chaff* sebaiknya memiliki format yang sejenis dengan paket *Wheat*, memiliki nomor serial yang masuk akal, isi pesan yang rasional, dan memiliki MAC yang tidak valid terhadap kunci autentikasi yang digunakan pada paket *Wheat*. Nilai MAC palsu juga harus dibuat mirip dengan aslinya.

2.4 Teknik-teknik Chaffing and Winnowing

Setelah mengetahui metoda pengiriman pesan, kita dapat menggunakan beberapa istilah sebagai berikut:

- *Chaffing*
  Menambahkan paket tiruan dengan MAC palsu ke dalam sekuens paket
- *Winnowing*
  Proses menghapus paket tiruan dengan MAC palsu
- *Wheat*
  Paket asli dengan MAC yang memang diauhentikasi
- *Chaff*
  Paket tiruan dengan MAC palsu

Kelebihan adanya chaff untuk setiap wheat adalah pihak ketiga harus memecahkan algoritma MAC untuk membedakan wheat dan chaff.
Chaffing and Winnowing dapat diimplementasikan dengan beberapa cara berikut:

1. Bit-by-bit method
   Metoda ini membuat pesan dikirimkan per bit. Pertama-tama paket diubah ke dalam bentuk bit, lalu masing-masing bit tersebut dimasukkan ke dalam fungsi untuk menghasilkan MAC yang valid. Lalu paket dipecah dan diberi serial number yang valid. Paket memiliki bentuk:

   Paket valid: (serial, bit, MAC)

   Dalam metoda ini, paket harus diselipkan chaff yang juga "terlihat" valid. Paket palsu memiliki bentuk:

   Paket tidak valid: (serial, bit lawan, MAC palsu)

   Untuk menjaga tingkat keamanan, untuk setiap wheat, harus diberikan masing masing sebuah chaff. Hal ini dikarenakan apabila tidak ada chaff dengan serial number yang sama dengan wheat, maka pihak ketiga dapat mengetahui bahwa itu adalah wheat. Contoh paket :

   (1,0,382392)
   (1,1,293842)
   (2,0,948573)
   (2,1,736420)
   (3,0,172362)
   (3,1,857302)
   (4,0,673028)
   (4,1,039590)
   Dst..

   Dengan adanya chaff di atas, pesan asli tersamarkan benar-benar tersamarkan. Kelebihan metoda ini adalah pihak ketiga yang ingin mengetahui isi pesan harus menggabungkan bit-bit isi pesan menjadi pesan utuh yang isinya adalah 0 dan 1.

   Kekurangan metoda ini adalah ukuran paket yang dikirimkan sangat banyak dan sangat besar. Misalkan saja, pesan yang dikirimkan besarnya adalah 20 Kbyte. 20 Kbyte kira-kira terdiri dari 160.000 bit. 160.000 bit tersebut dipisahkan menjadi 160.000 paket berbeda karena masing – masing paket terdiri dari 1 bit isi pesan.Lalu masing-masing paket kemudian ditambahkan dengan serial number yang besarnya 17 bit(karena jumlah paket 160 buah). Lalu penambahan MAC sebesar 64 bit (besar MAC tergantung dari algoritma MAC yang digunakan). Identitas receiver dan sender juga ditambahkan ke dalam paket. Asumsikan panjang paket 100 bit. Karena ada 160.000 paket, maka besar total pesan menjadi 16.000.000 bit atau 2 Mbyte. Belum lagi penambahan chaff pada paket sehingga besar pesan yang dikirimkan menjadi 4 Mbyte. Tentu hal ini sangat tidak efisien dalam pengiriman pesan.

2. All-or-Nothing-Transform
   Untuk membuat chaffing and winnowing menjadi lebih efisien, Rivest mengajukan AONT, yakni All-Or-Nothing-Transform. Konsepnya adalah mengubah pesan menjadi sebuah paket dimana pesan hanya dapat dibaca jika seluruh bagian paket diterima. Konsep ini tanpa kunci, dan membuat pesan original menjadi terlihat sepeti noise acak.

   Misalkan Alice memaketkan pesannya yang akan dikirimkan kepada Bob. Selanjutnya Alice memecah paket tersebut menjadi blok sebesar 1024 bit, mengautentikasikan setiap blok dengan MAC, dan mengirimkan hasilnya ke Bob. Cara ini akan lebih efisien dibandingkan dengan variasi pertama, dimana setiap paket hanya berisi satu bit pesan.

   Untuk perhitungan efisiensi, maka kita lihat sebuah contoh sebagai berikut:
   Misalkan kita ingin mengirimkan sebuah pesan sepanjang 20 Kbyte. Alice kemudian membungkus pesannya tersebut dan membaginya menjadi 20 paket dengan panjang masing-masing paket sebesar 1024 bit. Misalkan panjang bit untuk nomor serial adalah 32 bit, dan untuk

MAC adalah 64 bit. Maka 32 bit + 1024 bit + 64 bit = 1.100 bit untuk setiap paket. Untuk seluruh paket yang ada, maka besar totalnya adalah kira-kira 1,1 MB. Jumlah ini tentunya jauh lebih kecil dibandingkan dengan variasi pertama tadi. Walaupun mengikutsertakan *Chaff*, maka jika ditambahkan satu paket *Chaff* untuk setiap paket *Wheat*, maka jumlah totalnya hanya akan menjadi 2,2 MB. Variasi ini tentunya lebih efisien dan lebih memungkinksn untuk diimplementasikan dibandingkan dengan variasi dimana memerlukan 100 MB paket *Chaff* untuk setiap 1 MB pesan yang ada.

Semakin panjang pesan yang dikirmkan, maka jumlah paket chaff yang diperlukan akan semakin sedikit. Dari 8.192 paket *wheat*, jika ditambahkan 8 paket *chaff* saja akan menghasilkan total paket sebanyak 8.200 paket. Untuk memilih 8.192 paket yang benar dari total 8.200 paket yang ada, maka terdapat kombinasi sebanyak $5{,}0525 * 10^{26}$. Jumlah paket ini tidak akan menghasilkan besar bandwith yang terlalu berbeda jauh dengan 1,1 MB sebelumnya, tetapi tingkat kesulitan untuk memecahkannya tanpa memiliki kunci autentikasi sungguh besar.

2.5 Hukum

Teknik Chaffing dan Winnowing ternyata memiliki beberapa celah hukum yang sebenarnya dapat digunakan untuk kejahatan. Beberapa kasusnya adalah :

1. Keamanan

Walaupun dengan hukum yang berlaku saat ini pemerintah dapat memaksa meminta kunci enkripsi, tetapi tidak sama halnya dengan kunci autentikasi. Jika kunci autentikasi dapat diminta secara hukum, maka hal tersebut akan memungkinkan pemerintah dapat membuat paket pesan otentik yang dipalsukan untuk pihak mana saja yang sedang melakukan komunikasi.

Hal ini tentunya tidak diinginkan, karena akan menciptakan kekacauan dari struktur dan integritas dari internet. Hal ini kemudian dapat berlanjut pada *hacker* untuk menyadap seluruh pesan pribadi, bahkan untuk mengontrol komputer. Misalnya untuk mematikan sistem komputer pembangkit listrik ataupun sistem kendali lalu lintas udara. Hal ini tentunya sama sekali tidak diinginkan untuk terjadi oleh pemerintah.

Hal ini disebabkan karena kekuatan untuk melakukan autentikasi sama saja dengan kekuatan untuk mengendalikan, dan menangani seluruh kekuatan autentikasi bagi pemerintah adalah suatu hal yang tidak masuk akal, walaupun didasarkan dengan alasan keamanan. Tidak ada satu pihakpun yang dapat menerima resiko atas keamanan yang sangat tinggi jika hal itu sampai terjadi.

2. Nir-Penyangkalan (*Deniable Repudiation*)

Salah satu aspek dari kriptografi yaitu menyangkut masalah Nir-penyangkalan (*Deniable Repudiation*), yaitu menyangkal telah melakukan pengiriman suatu pesan yang dituduhkan kepada satu pihak.

Pada uji aplikasi akan dicoba tentang chaffing and winnowing nir-penyangkalan. Terdapat dua buah pesan, asli dan palsu. Kedua pesan sama –sama memiliki arti dan di autentikasi dengan MAC yang sebenarnya namun dengan kunci yang berbeda. Pada kasus ini, kita dapat menyangkal telah menulis pesan dengan cara memberi kunci palsu. Karena dengan kunci palsu pun pesan ternyata memiliki arti, maka kita dapat menyangkal isis pesan tersebut.

2.6 Uji aplikasi

Pada kesempatan kali ini penulis mencoba membuat suatu model program chaffing and winnowing sederhana. Di sini penulis ingin menguji cara kerja sebenarnya dari chaffing dan winnowing.

Pada kasus ini terdapat dua buah pesan yang ingin dimasukkan ke dalam proses chaffing and winnowing. Sebuah pesan asli dan sebuah pesan palsu. Kedua pesan dimasukkan secara manual. Terdapat dua proses utama dalam program, yaitu

1. Chaffing

Proses mencampurkan pesan asli dengan pesan palsu dan penambahan serial number. Di sini juga dilakukan fungsi MD5 untuk membuat MAC dari kunci yang dimasukkan dan isi pesan.

Intinya, pesan dimasukkan ke dalam array of string yang berisi:

[integer serial number, isi pesan, MAC]

Prosesnya adalah membagi pesan per karakter ke dalam ukuran byte, yaitu ke dalam heksadesimal. Serial number yang digunakan adalah nilai integer dari 1 sampai panjang file. Dan fungsi MAC menggunakan fungsi random C# berdasarkan hasil kali dari nilai integer dari kunci dan hasil heksadesimal yang diconvert ke integer. Apabila seed dari fungsi random ini tetap, maka setiap kali program dieksekusi, fungsi random akan menghasilkan nilai MAC yang sama untuk

setiap hasil kali kunci dan isi pesan. Lalu fungsi ini akan mencampurkan semua pesan “asli” dan “palsu” ke dalam sebuah array pesan.

2. Winnowing
   Proses untuk memisahkan pesan palsu dan pesan asli. Masukan dari fungsi ini adalah array pesan yang berisi serial number, isi pesan, MAC, dan tentu saja kunci autentikasi. Inti dari fungsi ini adalah membandingkan nilai MAC yang dalam array dengan fungsi random dari hasil kali dari nilai integer dari kunci dan hasil heksadesimal yang diconvert ke integer.

Untuk lebih jelasnya, kita dapat menyimulasikan program. Program dieksekusi sebagai berikut:

1. Pertama-tama user memasukkan isi pesan yang ingin dimasukkan ke fungsi chaffing. Kali ini penulis memasukkan dua buah pesan, yakni pesan:
   “Hi Leonardo meet me at 7PM Love-Xixi” dan “Hi Adiputra call me at 9AM Love-Angel”
   Setelah memasukkan pesan pertama, kita mengisi key dengan “tommy” dan menekan tombol insert chaff. Seelanjutnya, setelah memasukkan pesan kedua, kita mengisi key dengan “kripto” dan menekan tombol chaffing.

   Masukan 1 :
   Hi Leonardo meet me at 7PM Love-Xixi

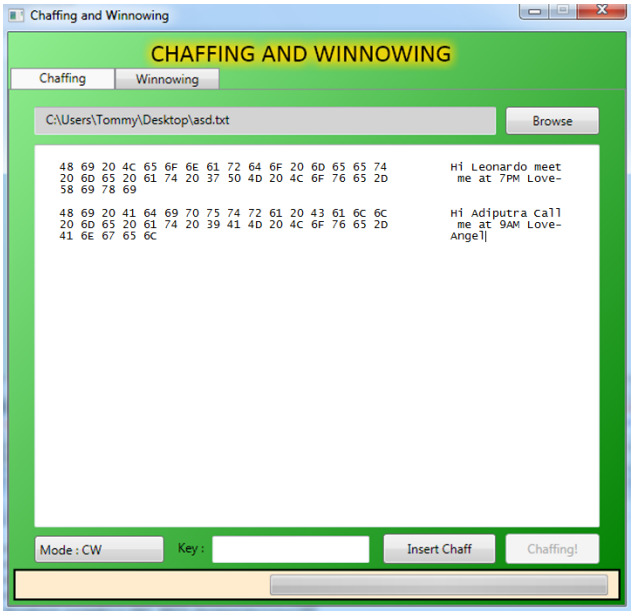
   Kunci 1: tommy

   Masukan 2:
   Oe Adiputra call me at 9AM Love-Angel

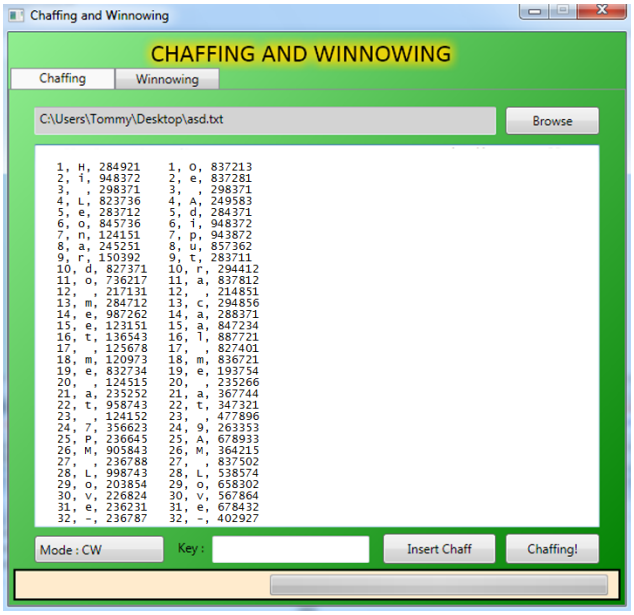
   Kunci 2: kripto

   Hasil eksekusi:

1, H, 284921	1, O, 837213
2, i, 948372	2, e, 837281
3, , 298371	3, , 298371
4, L, 823736	4, A, 249583
5, e, 283712	5, d, 284371
6, o, 845736	6, i, 948372
7, n, 124151	7, p, 943872
8, a, 245251	8, u, 857362
9, r, 150392	9, t, 283711
10, d, 827371	10, r, 294412
11, o, 736217	11, a, 837812
12, , 217131	12, , 214851
13, m, 284712	13, c, 294856
14, e, 987262	14, a, 288371
15, e, 123151	15, a, 847234
16, t, 136543	16, l, 887721
17, , 125678	17, , 827401
18, m, 120973	18, m, 836721
19, e, 832734	19, e, 193754
20, , 124515	20, , 235266
21, a, 235252	21, a, 367744
22, t, 958743	22, t, 347321
23, , 124152	23, , 477896
24, 7, 356623	24, 9, 263353
25, P, 236645	25, A, 678933
26, M, 905843	26, M, 364215
27, , 236788	27, , 837502
28, L, 998743	28, L, 538574
29, o, 203854	29, o, 658302
30, v, 226824	30, v, 567864
31, e, 236231	31, e, 678432
32, -, 236787	32, -, 402927
33, X, 764365	33, A, 927471
34, i, 285721	34, n, 151332
35, x, 899583	35, g, 236262
36, i, 998473	36, e, 957123
	37, l, 415243

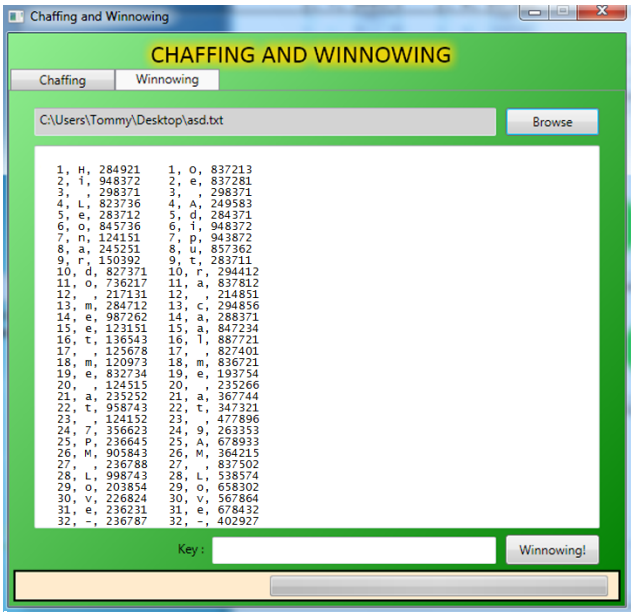


Gambar 1 masukan user

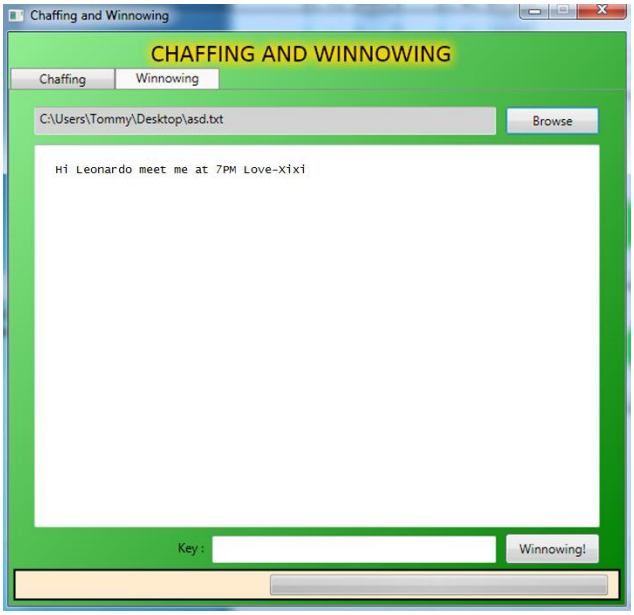


Gambar 2 setelah menekan Chaffing

2. Selanjutnya setelah mendapat aray pesan seperti di atas, kita tinggal memasukkan ke fungsi winnowing dengan kunci yang kita miliki. Apabila kita memasukkan kunci "tommy" maka pesan 1 akan muncul dan pesan kedua dibuang. Begitu sebaliknya apabila kita memasukkan kunci kripto. Apabila kita salah memasukkan kunci, maka tidak akan ada hasil yang keluar karena semua pesan dianggap tidak valid.



Gambar 3 Load array



Gambar 4 Hasil akhir setelah memasukkan kunci "tommy"

2.7 Kelebihan dan Kekurangan

Menurut aplikasi yang dicoba, Chaffing and Winnowing memiliki beberapa kelebihan dan kekurangan.
Kelebihan:

1. Tingkat keamanan chaffing and winnowing. Pihak ketiga yang berusaha mengintersepsi pesan tidak mengetahui pesan mana yang asli dan pesan mana yang palsu
2. Dapat menyangkal isi pesan sebenarnya. Apabila kita menggunakan teknik aplikasi, orang yang ingin mengetahui isi pesan sebenarnya dapat menggunakan kunci kedua.
3. Tidak dapat disentuh oleh tangan hukum, karena proses autentikasi adalah proses yang sangat penting dalam dunia komunikasi, dimana siapapun tidak boleh memiliki kuasa penuh terhadapnya.

Kekurangan:

1. *Overhead* yang cukup besar
2. Untuk kasus aplikasi, panjang pesan harus sama agar dapat memberikan hasil maksimal, selain itu perbedaan huruf yang digunakan juga mempengaruhi pesan, contohnya apabila per huruf, spasi mempengaruhi isi kalimat yang sebenarnya.

3. KESIMPULAN

Setelah melakukan percobaan, penulis dapat menyimpulkan beberapa kesimpulan sebagai berikut :

- Metoda Chaffing and Winnowing menjanjikan kerahasiaan tanpa melakukan enkripsi sedikitpun terhadap pesan
- Pemerintah dapat diperdaya dengan teknik ini karena kita tidak memiliki kunci enkripsi atau dekripsi, namun kunci autentikasi.

REFERENSI

[1] Munir, Rinaldi.2005. "Kriptografi". Departemen Teknik Informatika, Institut Teknologi Bandung. Diakses tanggal 25 Maret 2010 pukul 20.45

[2] http://www.cacr.math.uwaterloo.ca/~dstinson/papers/chaff2.pdf. Diakses tanggal 25 Maret 2010 pukul 21.00

[3] http:/searchsecurity.techtarget.com/sDefinition/ 0,,sid14_ gci786707,0 0.html Diakses tanggal 25 Maret 2010 pukul 21.10

[4] http://people.csail.mit.edu/rivest/Chaffing.txt Diakses tanggal 25 Maret 2010 pukul 21.15

[5] http://en.wikipedia.org/wiki/Steganography Diakses tanggal 25 Maret 2010 pukul 21.23

[6] http://en.wikipedia.org/wiki/Chaffing_and_winnowing Diakses tanggal 25 Maret 2010 pukul 21.34