Super Enkripsi Dengan Menggunakan Cipher Substitusi dan Cipher Transposisi

Shanny Avelina Halim (13504027)
Program Studi Teknik Informatika Institut Teknologi Bandung
email: if14027@Students.if.itb.ac.id

Abstrak – Pada makalah ini hanya akan dibahas mengenai kriptografi yang dilakukan dengan menggunakan kertas dan pena, dan merupakan algotitma klasik, yaitu cipher substitusi, cipher transposisi, dan super enkripsi. Super enkripsi dapat dilakukan dengan menggunakan dua jenis cipher sederhana, yaitu cipher substitusi dan cipher transposisi. Dalam dokumen ini akan dibahas mengenai cara melakukan cara melakukan enkripsi dan dekripsi dengan menggunakan super enkripsi, yaitu dengan menggunakan dua jenis cipher tersebut. Selain itu juga akan dilakukan analisis mengenai super enkripsi yang akan dibahas.

Kata Kunci: super enkripsi, cipher substitusi, cipher transposisi, *exhaustive key search, brute force,* plainteks, cipherteks.

1. PENDAHULUAN

Super Enkripsi dapat dilakukan dengan cara mengombinasikan dua buah metode cipher sederhana, yaitu cipher substitusi dan cipher transposisi. Hal tersebut dilakukan dengan tujuan untuk memperoleh cipher yang lebih kuat daripada hanya menggunakan satu cipher saja sehingga tidak mundah untuk dpecahkan.

2. CIPHER SUBSTITUSI

Algoritma ini mula-mula digunakan oleh kaisar Romawi, Julius Caesar sehingga sering disebut caesar cipher. Cipher substitusi dapat dilakukan dengan cara mengganti sebuah karakter dengan karakter lain yang ada pada susunan abjad. Hal tersebut juga dapat dilakukan dengan menggunakan susunan karakter ASCII. Banyaknya pergeseran huruf yang dilakukan merupakan kunci untuk melakukan enkripsi dan dekripsi. Misalnya pergeseran huruf adalah 4, maka kuncinya adalah k = 4, sehingga akan didapat tabel substitusi sebagai berikut:

P_i = A B C D E F G H I J
C_i = E F G H I J A B C D

Contoh:

SAYA BERADA DI BANDUNG

Plainteks tersebut akan dienkripsi menjadi cipherteks berikut:

WECE FIVEHE HC FERHYRA

Bila kita mengkodekan huruf abjad dengan angka yang berurutan, yaitu: A = 0, B = 1, dan seterusnya sampai Z = 25, maka akan didapat rumus enkripsi sebagai berikut:

$$C_i = E(P_i) = (P_i + k) \bmod 26 \quad ...(1)$$

Sedangkan rumus untuk dekripsinya adalah sebagai berikut:

$$P_i = D(C_i) = (C_i - k) \bmod 26 \quad ...(2)$$

dengan C adalah cipherteks yang akan diperoleh, P adalah plainteks mula-mula, $E(P_i)$ adalah fungsi untuk melakukan enkripsi, $D(C_i)$ adalah fungsi untuk melakukan dekripsi, dan k adalah kunci yang merupakan banyaknya pergeseran huruf.

Untuk melakukan enkripsi dan dekripsi dengan menggunakan karakter ASCII yang terdiri dari 256 buah karakter, maka persamaan enkripsi (1) dan persamaan dekripsi (2) di atas dapat ditulis kembali menjadi:

$$C_i = E(P_i) = (P_i + k) \bmod 256 \quad ...(3)$$

dan

$$P_i = D(C_i) = (C_i - k) \bmod 256 \quad ...(4)$$

Cipher substitusi adalah jenis cipher yang sangat sederhana sehingga amat mudah untuk dipecahkan. Cara yang paling baik adalah menggunakan metode *exhaustive key search*, yaitu mendaftarkan semua kemungkinan kunci yang ada dan memilih kunci yang ada. Dengan menggunakan metode ini semua kemungkinan kunci yang ada didaftarkan di dalam sebuah tabel kemungkinan kunci, yaitu 26 buah kunci untuk karakter abjad dan 256 buah kunci untuk karakter ASCII.

Misalkan ada sebuah potongan cipherteks GZQFS dan terdapat asumsi bahwa plainteks tersebut disusun dengan menggunakan Bahasa Indonesia, maka yang

perlu dilakukan adalah dekripsi cipherteks tersebut dengan menggunakan metode *exhaustive key search,* yaitu mencari semua solusi yang mungkin sehingga hasil akhirnya akan didapatkan 26 buah kunci mulai dari $k = 0$ sampai dengan $k = 25$. Proses tersebut akan memberikan hasil sebagai berikut:

k = 1 >> FYPER	k = 14 >> SLCRE
k = 2 >> EXODQ	k = 15 >> RKBQD
k = 3 >> DWNCP	k = 16 >> QJAPC
k = 4 >> CVMBO	k = 17 >> PIZOB
k = 5 >> BULAN	k = 18 >> OHYNA
k = 6 >> ATKZM	k = 19 >> NGXMZ
k = 7 >> ZSJYL	k = 20 >> MFWLY
k = 8 >> YRIXK	k = 21 >> LEVKX
k = 9 >> XQHWJ	k = 22 >> KDUJW
k = 10 >> WPGVI	k = 23 >> JCTIV
k = 11 >> VOFUH	k = 24 >> IBSHU
k = 12 >> UNETG	k = 25 >> HARGT
k = 13 >> TMDSF	k = 26 >> GZQFS

Dengan melihat hasil dekripsi di atas, maka akan didapat sebuah kata yang masuk akal dalam Bahasa Indonesia, yaitu kata bulan pada kunci dekripsi k = 5. Yang perlu dilakukan adalah melakukan dekripsi terhadap semua bagian cipherteks dengan menggunakan kunci $k = 5$ tersebut.

Metode lain yang dapat digunakan adalah metode analisis frekuensi. Dengan metode ini, dibuat tabel yang berisi masing-masing huruf beserta jumlah kemunculannya, lalu disesuaikan dengan menggunakan karakter-karakter yang sering muncul dalam bahasa yang bersangkutan. Contoh di bawah ini adalah sebuah cipherteks yang disusun dari plainteks dalam Bahasa Indonesia

VDBD WLGDN DGD GL EDQGXQJ

Cipherteks di atas tidak diketahui panjang kuncinya, maka yang dapat dilakukan adalah membuat tabel kemunculan masing-masing karakter.

V = 1
D = 6
B = 1
W = 1
L = 2
G = 4
N = 1
E = 1
Q = 2
X = 1
J = 1

Berdasarkan hasil yang didapat, huruf D adalah yang paling banyak sehingga kita dapat coba untuk menggantinya dengan huruf A karena huruf A adalah huruf yang paling banyak muncul dalam Bahasa Indonesia.

VABA WLGAN AGA GL EAQGXQJ

Huruf G pada cipherteks kemungkinan besar adalah huruf D, P, atau S karena dalam Bahasa Indonesia hanya ada kata ADA, APA, atau ASA yang memiliki makna. Selanjutnya, kata dari Bahasa Indonesia yang terdiri dari 2 huruf hampir dapat dipastikan bahwa huruf keduanya adalah huruf vokal. Kata yang paling sering muncul adalah kata DI dan KE. Dari 2 argumen tersebut, yang paling memungkinkan adalah huruf D dan huruf vokal I. Kemudian hanya perlu mengganti huruf G pada cipherteks dengan huruf D, dan huruf L pada cipherteks menjadi huruf I.

VABA WIDAN ADA DI EAQDXQJ

Sampai sini kriptanalis harus mulai menebak huruf selanjutnya. Huruf lain yang cukup sering muncul dalam Bahasa Indonesia adalah huruf N sehingga kriptanalisis dapat mencoba mengganti huruf Q pada cipherteks dengan huruf N.

VABA WIDAN ADA DI EANDXNJ

Kata terakhir dapat dipastikan adalah nama tempat, dan karakter X dapat dipastikan adalah huruf vokal karena dalam Bahasa Indonesia tidak ada 4 buah konsonan dengan komposisi ND*N sehingga huruf X pada cipherteks dapat diganti dengan huruf vokal U, E, atau O. Bila huruf U yang dimasukkan, maka dapat diketahui bahwa kata yang terakhir adalah BANDUNG.

VABA WIDAN ADA DI BANDUNG

Dengan mempertimbangkan jenis huruf kemunculannya jarang pada Bahasa Indonesia, kriptanalisis dapat mengetahui bahwa kata kedua adalah TIDAK dan kata pertama adalah kata SAYA sehingga isi plainteks tersebut dapat dibaca, yaitu:

SAYA TIDAK BERADA DI BANDUNG.

Jenis cipher substitusi lain seperti cipher abjad-tunggal atau cipher substitusi poligram tidak akan dibahas di dalam makalah ini

3. CIPHER TRANSPOSISI

Cipher Transformasi dapat dilakukan dengan cara mengubah susunan karakter pada plainteks sehingga menjadi susunan karakter atau kata baru yang tidak memiliki makna. Jumlah total karakter dan jumlah masing-masing karakter pada plainteks sama dengan jumlah total karakter dan jumlah masing-masing karakter pada cipherteksnya karena hanya mengubah susunan karakter saja.

Enkrispi dengan menggunakan cipher transposisi yang paling sederhana dapat dilakukan dengan cara membagi karakter pada plainteks ke dalam beberapa blok berisi karakter dengan kunci enkripsi dan dekripsinya adalah jumlah karakter pada tiap-tiap blok.

Untuk melakukan dekripsi, karakter pada cipherteks juga dibagi ke dalam beberapa blok namun pembaginya belum tentu adalah kunci mula-mula, dan jumlah karakter pada tiap-tiap blok yang baru belum tentu sama dengan jumlah karakter pada blok awal.

Misalnya ada sebuah plainteks A B C D E F G H I J. Bila plainteks tersebut dienkripsi dengan kunci yang merupakan hasil baginya seperti k = 5, plainteks tersebut ditulis secara horizontal dengan lebar kolom tetap, yaitu 5.

A B C D E
F G H I J

Kemudian cipherteksnya akan dibaca secara vertikal menjadi:

A F B G C H D I E J

Untuk melakukan dekripsi, cipherteks tersebut hanya perlu dienkripsi sekali lagi karena algoritma yang digunakan sama. Namun kunci yang digunakan adalah hasil bagi dari panjang karakter dalam plainteks, yaitu 10 dengan panjang kunci mula-mula, yaitu 5, sehingga didapat kunci yang baru, yaitu 2. Cipherteks tersebut kemudian ditulis secara horizontal dengan lebar kolom tetap, yaitu 2.

A F
B G
C H
D I
E J

Kemudian plainteksnya akan didapat bila pembacaan dilakukan secara vertikal.

A B C D E F G H I J

Bila kunci mula-mula bukan merupakan hasil baginya, maka ada maka ada 2 cara yang dapat dilakukan. Cara yang pertama adalah menambahkan karakter yang sama dan tidak bermakna di ujung plainteks sampai jumlahnya merupakan kelipatan dari kunci. Misalnya kunci untuk plainteks yang sama adalah k = 3. Maka kita perlu menambahkan 2 buah karakter agar jumlahnya sesuai.

A B C D E F G H I J Z Z

sehingga bila dilakukan enkripsi jumlah karakter untuk tiap bloknya akan sama.

A B C
D E F
G H I
J Z Z

Dengan demikian, cipherteks yang didapat adalah sebagai berikut:

A D G J B E H Z C F I Z

Dekripsinya dilakukan dengan cara yang sama dengan proses enkripsi. Hanya saja kunci yng baru nilainya adalah 4.

A D G J
B E H Z
C F I Z

Selanjutnya dengan pembacaan secara vertikal, akan didapat plainteks mula-mula.

A B C D E F G H I J Z Z

Cara lain yang dapat kita lakukan adalah dengan melakukan enkripsi secara langsung tanpa menambah jumlah karakter, namun dengan menggunakan cara yang ini, proses dekripsinya menjadi lebih sulit untuk dilakukan.

A B C
D E F
G H I
J

Di ujungnya tidak ditambahkan karakter baru sehingga dari blok-blok tersebut akan didapatkan cipherteks sebagai berikut:

A D G J B E H C F I

Dari cipherteks di atas, didapat 1 buah blok yang karakternya penuh, dan berisi 4 buah karakter yaitu A D G J, serta 2 buah blok tidak penuh yang masing-masing hanya berisi 3 karakter, yaitu karakter B E H dan C F I.

Proses dekripsi dilakukan dengan cara menuliskan kembali isi dari cipherteks dengan jumlah barisnya didapat dari rumus sebagai berikut:

N div k ...(5)

dengan N adalah panjang karakter dan k adalah panjang kunci. Dengan demikian, hasil yang didapat adalah 10 div 3 = 3.

Selanjutnya rincian jumlah karakter untuk tiap bari adalah sebagai berikut. Sisa dari N div k adalah 1, maka hanya 1 baris yang berisi karakter penuh

sejumlah (N div k) + 1 = 4, dan baris sisanya hanya berisi sejumlah karakter tidak penuh, yaitu sebanyak N div k = 3 karakter. Sehingga penulisannya adalah sebagai berikut:

A D G J
B E H
C F I

Selanjutnya yang perlu dilakukan hanya membaca blok-blok tersebut secara vertikal sehingga akan didapat plainteks semula.

A B C D E F G H I J

Bila kita tidak mengetahui kunci pada cipher transposisi, proses untuk memecahkan cipherteksnya menjadi lebih lama karena tidak seperti cipher substitusi yang bisa menggunakan hanya sebagian isi saja dari plainteks, cipher transposisi memerlukan seluruh isi dari plainteks tersebut. Hal tersebut disebabkan oleh perubahan letak suatu huruf pada plainteks, sehingga mungkin saja huruf kedua dari kata pertama yang dicari ada pada setengah terakhir bagian cipherteks, dan seterusnya.

Jumlah total kemungkinan paling banyak kunci yang harus dicoba untuk memecahkan cipherteks yang menggunakan cipher transposisi dengan membagi ke dalam blok dengan menambahkan karakter tambahan adalah:

N – 1 ...(6)

dengan N adalah panjang karakter dalam plainteks atau sejumlah karakter pada cipherteks. Sedangkan jumlah paling banyak kunci yang harus dicoba untuk memecahkan cipherteks yang tidak menambahkan karakter tambahan adalah sebanyak panjang karakter pada plainteks atau cipherteks.

Selain membagi isi plainteks mejadi beberapa blok ada jenis cipher transposisi yang lain, yaitu disusun diagonal ke bawah dan ke atas. Misalnya terdapat plainteks berikut:

SAYA BERADA DI BANDUNG

Plainteks tersebut kemudian disusun secara diagonal sebagai berikut:

S B D B U
A A E A A I A D N
Y R D N G

Berdasarkan susunan di atas, akan didapat cipherteks sebagai berikut:

SBDBUAAEAAIADNYRDNG

Selain itu masih banyak lagi jenis-jenis cipher transposisi yang lainnya karena jenis-jenis pertukaran karakter pada cipher ini dapat ditentukan sendiri oleh pembuat cipherteks tersebut, dan jenis-jenis cipher lain tersebut tidak akan dibahas lebih lanjut di dalam makalah ini.

4. SUPER ENKRIPSI

Super enkripsi adalah salah satu kriptografi berbasis karakter yang menggabungkan cipher substitusi dan cipher transposisi. Hal tersebut bertujuan utnuk mendapatkan cipher yang lebih kuat dari hanya menggunakan satu cipher saja, sehingga tidak mudah untuk dipecahkan. Enkripsi dan dekripsi dapat dilakukan dengan urutan cipher substitusi kemudian cipher transposisi, atau sebaliknya. Super enkripsi dapat dilakukan dengan menggunakan kedua cipher tersebut secara berulang-ulang, namun pada makalah ini hanya akan dibahas mengenai proses enkripsi dan dekripsi satu kali dengan menggunakan cipher substitusi dan satu kali dengan menggunakan cipher transposisi.

4.1 Enkripsi

Super enkripsi dapat dilakukan dengan melakukan enkripsi dengan menggunakan kedua cipher tersebut secara berurutan. Misalnya ada sebuah plainteks sebagai berikut.

SAYA BERADA DI BANDUNG

Plainteks tersebut akan dienkripsi dengan menggunakan kunci k = 3. Mula-mula lakukan enkripsi dengan menggunakan dengan menggunakan cipher substitusi sehingga akan didapatkan cipherteks sebagai berikut.

VDBD EHUDGD GL EDQGXQJ

Selanjutnya enkripsi kembali cipherteks tersebut dengan menggunakan cipher transposisi dengan panjang kunci yang sama, yaitu 3 sehingga akan didapatkan hasil sebagai berikut.

V D B
D E H
U D G
D G L
E D Q
G X Q
J X X

Di akhir ditambahkan dua buah karakter tambahan, yaitu 2 buah huruf X. Huruf X dipilih karena jumlahnya hanya 1 buah saja. Karena cipherteks tersebut didapatkan juga dengan menggunakan cipher substitusi, pemilihan huruf X dapat menyulitkan

kriptanalisis untuk memecahkan cipherteks tersebut dengan menggunakan metode analisis frekuensi karena adanya perubahan jumlah untuk jumlah karakter X. Selanjutnya hanya perlu membaca blok-blok di atas dan akan didapat cipherteks akhir sebagai berikut.

VDUDEGJDEDGDXXBHGLQQX

4.2 Dekripsi

Untuk mengembalikan cipherteks tersebut menjadi plainteks yang memiliki makna, kita hanya perlu melakukan dekripsi secara berurutan dengan menggunakan cipher substitusi dan cipher transposisi namun urutannya dekripsinya ditukar. Mula-mula lakukan dekrispi dengan menggunakan cipher transposisi dengan jumlah kolom yang ada adalah 21 dibagi 3, yaitu 7 sehingga akan didapatkan blok-blok sebagai berikut:

V D U D E G J
D E D G D X X
B H G L Q Q X

Berdasarkan blok yang ada di atas, akan didapatkan cipherteks baru sebagai berikut:

VDBDEHUDGDGLEDQGXQJXX

Karena kita tidak tahu apakah dua karakter di akhir merupakan karakter tambahan atau bukan, maka kita tidak bisa langsung menghilangkan karakter tersebut. Selanjutnya cipherteks tersebut didekripsi sekali lagi dengan menggunakan cipher substitusi dengan panjang kunci k = 3 sehingga akan kita dapatkan plainteks sebagai berikut:

SAYABERADADIBANDUNGUU

Dengan cepat dapat kita pisah plainteks tersebut menjadi susunan kata yang memiliki makna sebagai berikut.

SAYA BERADA DI BANDUNG UU

Saat ini dapat dipastikan bahwa dua huruf di belakang plainteks adalah karakter tambahan karena kata tersebut tidak memiliki makna yang bersesuaian dengan isi plainteks yang lain sehingga kita bisa menghilangkannya.

Bila kita tidak menambahkan karakter tambahan di ujung plainteks, maka akan didapat cipherteks yang jumlah karakternya sama dengan jumlah karakter pada plainteks awal sehingga cipherteks skhir yang didapat adalah sebagai berikut:

VDUDEGJDEDGDXBHGLQQ

dan bila dilakukan dekripsi terhadap cipherteks tersebut dengan menggunakan cipher transposisi, maka akan didapatkan cipherteks baru, yaitu sebagai berikut.

VDBDEHUDGDGLEDQGXQJ

dan dapat dipastikan bahwa tidak ada karakter tambahan pada cipherteks tersebut sehingga kita hanya perlu untuk melakukan dekripsi dengan menggunakan cipher substitusi sehingga akan didapatkan plainteks mula-mula tanpa adanya karakter tambahan.

SAYABERADADIBANDUNG

Plainteks tersebut kemudian dipisahkan menjadi kata-kata dalam Bahasa Indonesia yang dapat diketaui, yaitu:

SAYA BERADA DI BANDUNG

Untuk melakukan enkripsi dan dekripsi dengan urutan yang sebaliknya, proses yang dilakukan sama, namun urutannya terbalik.

4.3 Analisis

Ada beberapa keuntungan yang didapat dengan menggunakan super enkripsi dibandingkan dengan hanya menggunakan cipher substitusi atau cipher transposisi saja, yaitu cipherteks yang dihasilkan dari super enkripsi lebih sulit untuk dipecahkan karena proses enkripsinya dilakukan sebanyak dua kali atau lebih sehingga cipherteks yang dihasilkan juga jumlahnya sebanyak dua buah atau lebih. Selain itu, dengan banyaknya jenis cipher transposisi yang dapat digunakan, kemungkinan dari solusi yang harus dibuat untuk memecahkan cipherteks tersebut juga menjadi lebih banyak.

Namun sama seperti cipher substitusi dan cipher transposisi, cipherteks yang dibuat dengan menggunakan super enkripsi sederhana, yaitu dengan menggunakan cipher substitusi dan cipher transposisi dengan pembagian blok, pasti dapat dipecahkan dengan metode *brute force*, yaitu dengan mencoba semua kemungkinan kunci yang ada, walaupun dalam proses pemecahannya memerlukan waktu yang sangat lama.

3. HASIL DAN PEMBAHASAN

Cipherteks yang dibuat dengan menggunakan super enkripsi, yaitu cipher substitusi dan cipher transposisi dengan menggunakan pembagian blok pasti dapat dipecahkan dengan menggunaka metode *brute force*, yaitu mencoba semua kemungkinan kunci yang ada. Jumlah paling banyak kunci yang harus dicoba adalah

sebanyak:

$$2 \times K_{substitusi} \times K_{transposisi} \quad ...(7)$$

dengan $K_{substitusi}$ adalah jumlah paling banyak kunci pada cipher substitusi, yaitu 26 buah, dan $K_{transposisi}$ adalah jumlah paling banyak kunci pada cipher transposisi, yaitu sebanyak persamaan (6) atau sebanyak panjang karakter pada plainteks.

Hasil kali dari kunci cipher substitusi dan cipher transposisi tersebut harus dikalikan kembali dengan bilangan 2 karena adanya 2 buah urutan yang mungkin dilakukan untuk membuat cipherteks tersebut, yaitu cipher substitusi dahulu kemudian cipher transposisi, dan sebaliknya.

4. KESIMPULAN

Kesimpulan dari pembahasan yang telah dilakukan tersebut adalah:

1. Super enkripsi sederhana pasti dapat dipecahkan dengan metode *brute force*, yaitu mencoba semua kemungkinan kunci yang ada.
2. Super enkripsi lebih sulit dipecahkan dengan daripada hanya menggunakan cipher substitusi atau cipher transposisi saja karena jumlah kunci yang harus dicoba lebih banyak.

DAFTAR REFERENSI

[1] R. Munir, *Diktat Kuliah IF5054 Kriptografi*, Program Studi Teknik Informatika Institut Teknologi Bandung, 2006.

[2] http://download.itp.ac.id/bahankuliah/psk/Algoritma%20Kriptografi%20Klasik%20(lanjutan).ppt

[3] http://203.130.205.68/dosen/aji/computer_security/bab_2.pdf