Jurnal Matematika Vol. 16, No. 1, Mei 2017
ISSN: 1412-5056
http://ejournal.unisba.ac.id

Diterima: 7/01/2017
Disetujui: 15/04/2017
Publikasi Online: 23/05/2017

Kriptografi Klasik Monoalphabetic

Yurika Permanasari

Program Studi Matematika, FMIPA, Universitas Islam Bandung

yurikape@unisba.ac.id

Abstrak. Kriptografi berdasarkan arah implementasi dan pembabakan jamannya dibedakan menjadi algoritma kriptografi klasik atau konvensional dan algoritma kriptografi modern. Algoritma kriptografi klasik memberikan konsep dasar pemahaman kriptografi dan dijadikan sebagai dasar algoritma kriptografi modern. Teknik dasar dari algoritma kriptografi klasik adalah cipher substitusi dan chiper transposisi. Kriptografi monoalphabetic adalah algoritma kriptografi dengan teknik substitusi yaitu mengganti setiap karakter dari plainteks dengan satu karakter chiperteks. Cryptoanalysis monoalphabetic chiper dapat menggunakan metode terkaan atau Statistik (analisis frekuensi). Informasi yang dibutuhkan untuk kedua metode ini adalah mengetahui bahasa yang digunakan untuk plainteks dan konteks plainteks-nya.

Kata kunci: kriptografi klasik, chiper substitusi, monoalphabetic chiper, metode terkaan, analisis frekuensi

Abstract. (*Classical Monoalphabetic Cryptography*). Cryptography based on the direction of implementation and dissipation of its era is divided into classical or conventional cryptographic algorithms and modern cryptographic algorithms. Classical cryptographic algorithms provide a basic concept of understanding cryptography and serve as the basis for modern cryptographic algorithms. The basic technique of classical cryptographic algorithms is substitution cipher and transposition cipher. Monoalphabetic cryptography is a cryptographic algorithm with a substitution technique that replaces each character from plaintext with one chipertext character. Monoalphabetic chiper cryptoanalysis can use guess or statistical methods (frequency analysis). The information needed for both methods is to know the language used for plaintext and the context of its plaintext.

Keywords: classical cryptography, substitute cipher, monoalphabetic cipher, guess method, frequency analysis

1. Pendahuluan

Kriptografi klasik adalah algoritma kriptorafi (*chiper*) yang berbasis karakter yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Semua algoritma klasik termasuk ke dalam sistrm kriptografi simetris dan digunakan jauh sebelum kriptografi kunci publik ditemukan. Kriptogarfi klasik termasuk ke dalam kriptografi kunci simetris. Pada dasarnya, algoritma kriptografi klasik dapat dikelompokkan ke dalam dua macam cipher, yaitu :

a. Cipher substitusi (*substitution cipher*)

   Di dalam cipher substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu unit di sini berarti satu huruf, pasangan huruf, atau dikelompokkan lebih dari dua huruf.

b. Cipher transposisi (*transposition cipher*)

   Pada cipher transposisi, huruf-huruf di dalam plainteks diubah urutannya. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (*scrambling*) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karkater tersebut. (*Munir.2006*)

2. Chiper Substitusi

Algoritma kriptografi teknik substitusi adalah teknik kriptografi yang mula-mula digunakan oleh kaisar Romawi "Julius Caesar" untuk berkirim pesan dengan para gubernurnya, sehingga dinamakan juga Caesar Cipher. Chiper ini menyandikan pesan yang dikirim dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet). Oleh karena itu caesar chiper disebut juga dengan monoalphabetic chiper. Dalam Caesar chiper, tiap huruf di-substitusi dengan huruf ketiga berikutnya dari susunan abjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu k = 3).

P : 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 (plainteks)
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 (chiperteks)

Contoh 1:

Pesan : AWASI MAHASISWA MUKIDI KALAU BERORASI disamarkan (enskripsi) menjadi : DZDVL PDKDVLVZD PXNLGL NDODX EHURUDVL. Penerima pesan men-dekripsi cipherteks dengan menggunakan tabel substitusi, sehingga cipherteks DZDVL PDKDVLVZD PXNLGL NDODX EHURUDVL dapat dikembalikan menjadi plainteks semula: AWASI MAHASISWA MUKIDI KALAU BERORASI· Dengan mengkodekan setiap huruf abjad dengan integer sebagai berikut: $A = 0$, $B = 1$, …, $Z = 25$, maka secara matematis caesar cipher menyandikan plainteks p_i menjadi c_i dengan aturan:

$$C = E(P) = (p + 3) \bmod 26 \quad (1)$$

dan dekripsi cipherteks c_i menjadi p_i dengan aturan:

$$P = D(C) = (c - 3) \bmod 26 \quad (2)$$

Karena hanya ada 26 huruf abjad, maka pergeseran huruf yang mungkin dilakukan adalah dari 0 sampai 25. Secara umum, untuk pergeseran huruf sejauh k (dalam hal ini k adalah kunci enkripsi dan dekripsi), fungsi enkripsi adalah

$$C = E(P) = (p + k) \bmod 26 \quad (3)$$

dan fungsi dekripsi adalah

$$P = D(C) = (c - k) \bmod 26 \quad (4)$$

Catatan:

1. Pergeseran 0 sama dengan pergeseran 26 (susunan huruf tidak berubah)
2. Pergeseran lain untuk $k > 25$ dapat juga dilakukan namun hasilnya akan kongruen dengan bilangan bulat dalam modulo 26. Misalnya k = 37 kongruen dengan 11 dalam modulo 26, atau $37 \equiv 11 \pmod{26}$.
3. Karena ada operasi penjumlahan dalam persamaan (3) dan (4), maka *Caesar Cipher* kadang-kadang dinamakan juga *Additive Cipher*.
4. Untuk meng-enkripsi/dekripsi pesan yang disusun oleh karakter-karakter teks (ASCII, 256 karakter), maka persamaan (3) dan (4) ditulis

$$C = E(P) = (p + k) \bmod 256 \quad (5)$$

$$P = D(C) = (c - k) \bmod 256 \quad (6)$$

3. Monoalphabetic Chiper

Monoalphabetic adalah teknik kriptografi substutusi yang mengganti setiap karakter plainteksnya menjadi karakter lain pada chiperteks. Huruf yang sama pada plainteks, akan memiliki huruf pengganti yang sama pula pada chiperteksnya. Seperti pada contoh Caesar chiper, huruf A pada plainteks akan selalu diganti dengan huruf *D* pada chiperteks. Metoda lain pada monoalphabetic chiper adalah ROT13 yang mengganti setiap huruf pada plainteksnya dengan huruf yang letaknya 13 posisi darinya. Oleh karena itu hubungan antara plainteks dengan chiperteksnya mudah diterka, karena huruf yang sering muncul pada palinteks akan sering muncul pula pada chiperteks.

Dengan informasi bahasa yang digunakan dan konteks pesan, cryptoanalysis dapat menggunakan 2 metode berikut untuk memecahkan pesan :

a. Metode Terkaan

Bahasa yang digunakan : *English*
Cipherteks: **HATTPT**
Plainteks: salah satu dari **T** atau **P** merepresentasikan huruf vokal, misal:

CHEESE
MISSES
CANNON

Konteks pesan : diketahui bahwa pesan tersebut adalah nama negara
Maka plainteks : GREECE

b. Analisis Frekuensi

Setiap bahasa memiliki huruf yang sering digunakan atau jarang digunakan. Misalnya huruf *a* sering sekali digunakan dalam bahasa Indonesia, dan *q* atau *x* jarang sekali muncul. Setiap bahasa memiliki pola frekuensi tertentu, yang menunjukkan frekuensi relatif dari digunakannya huruf-huruf dalam bahasa tersebut. Bahasa inggris mempunyai tabel frekuensi yang dibedakan dalam tiga kategori yaitu :

i. *Top* 10 huruf yang sering muncul dalam teks Bahasa Inggris: E, T, A, O, I, N, S, H, R, D, L, U

ii. Top 10 huruf *bigram* yang sering muncul dalam teks Bahasa Inggris: TH, HE, IN, EN, NT, RE, ER, AN, TI, dan ES

iii. Top 10 huruf *trigram* yang sering muncul dalam teks Bahasa Inggris: THE, AND, THA, ENT, ING, ION, TIO, FOR, NDE, dan HAS

Sedangkan bahasa Indonesia memiliki tabel kebenaran yang dibedakan atas bahasa formal dan bahasa non formal. Teknis analisis frekuensi ini menggunakan asumsi plainteks di-enkripsi dengan *cipher* monoalphabetic. Setelah menghitung frekuensi kemunculan relatif huruf-huruf di dalam cipherteks, bandingkan hasil perhitungan dengan Tabel frekuensi.

Contoh 2 :

Huruf yang sering muncul dalam plainteks adalah Z dan P, dalam tabel frekuesi probabilitas tertinggi kemunculan huruf dalam bahasa Inggris adalah E dan T, maka kemungkinan Z disubstitusi dengan E dan P disubstitusi dengan T, demikian dilakukan beberapa iterasi hingga plainteks dapat dipecahkan.

4. Penutup

Monoalphabetic Cipher mengenkripsi setiap karakter dalam pesan, sehingga memiliki Kunci 26!. Algoritma telah dikenal sehingga mudah didekripsi tanpa kunci menggunakan metode terkaan. Teknik monoalphabetic chiper juga tidak dapat menyembunyikan hubungan antara plainteks dengan cipherteks. Huruf yang sama di-enkripsi menjadi huruf cipherteks yang sama, sehingga huruf yang sering muncul di dalam plainteks, sering muncul pula di dalam cipherteks-nya. Oleh karena itu monoalphabetic chiper akan mudah dipecahkan dengan menggunakan analisis frekuensi kemunculan huruf.

Referensi

[1] Munir, Rinaldi, Kriptografi, Informatika, Bandung, 2009

[2] Menezes, Alfred J., Paul C. van Oorschot and Scott A.Vanstone, "*Handbook of Applied Cryptography*", 5th printing,CRC Press, 2001

[3] Schenier, Bruce, *Applied Cryptography (Protocol ,Algorithm,and Source Code in C)*, 2nd edition, John Wiley & Sons, New York, 1996.

[4] Stallings, William, *Cryptography and Network Security Principles and Practices*, International Edition 3rd edition, Prentice Hall USA, 2003

[5] Y. Permanasari, E. Harahap. *Algoritma Data Encryption Standard (DES) Pada Electronic Code Book (ECB)*. Jurnal Matematika UNISBA, Vol. 6, No. 1. 2007. pp. 77-84.

[6] R. Tennekoon, J. Wijekoon, E. Harahap, dan H. Nishi. *Per-hop data encryption protocol for transmitting data securely over public netrwork*. Procedia Computer Science. Volume. 32. 2014. pp. 965-972. DOI: 10.1016/i.procs.2014.05.519

[7] R. Tennekoon, J. Wijekoon, E. Harahap, H. Nishi, E. Saito, S *Katsura. Per hop data encryption protocol for transmission of motion control data over public networks*. Proceeding Advanced Motion Control (AMC) on IEEE 13th International Workshop, Yokohama, Japan. 2014. Pp.128-133

[8] A. Tulloh, Y. Permanasari, E. Harahap. 2016. *Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen*. Jurnal Matematika UNISBA. Vol. 15 No 1, Mei 2016. pp. 7-14.