PERANCANGAN APLIKASI PENYANDIAN TEKS DENGAN METODE MULTIPLE XOR

Holder Simorangkir
Fakultas Ilmu Komputer, Universitas Esa Unggul
Jalan Arjuna Utara No.9, Kebon Jeruk, 11510 Jakarta Barat
holder@esaunggul.ac.id

Abstract

Many hackers who want to destroy or retrieve data or important information from the company, data or information taken can be useful for others or damage the order of information owned company so as to make the company become problematic. Storage of data or information is necessary and far from the reach of hackers. Encryption is one of the efforts made to obscure the stored text so that the company can avoid the destruction. Frequently used method is MD5, RSA, DES, Symmetric Stream Chipper method, and on this problem used Multiple XOR method with 32 bit. The result of this encryption makes the information into a combination of alphabetically coupled with Greek alphabetics making the hackers have to work and learn more to get results to be chipper text made.

***Keywords** : Encryption, Multiple XOR,Hackers*

Abstrak

Banyak Peretas yang merusak atau mengambil data atau informasi yang penting dari perusahaan, data atau informasi yang diambil bisa bermanfaat bagi orang lain atau merusak tatanan informasi yang dimiliki perusahaan sehingga membuat perusahaan menjadi bermasalah. Penyimpan data atau informasi sangat diperlukan dan jauh dari jangkauan hacker. Penyandian adalah salah satu upaya yang dilakukan untuk mengaburkan teks yang disimpan agar perusahan dapat terhindar dari pengrusakan. Metode yang sering digunakan adalah MD5, RSA, DES, metode Symmetric Stream Chipper, dan pada masalah ini digunakan metode Multiple XOR dengan 32 bit. Hasil dari penyandian ini membuat informasi tersebut menjadi kombinasi dari alpabetik digabung dengan alpabetik Yunani sehingga membuat para peretas harus bekerja dan belajar lebih untuk mendapat hasil dari pen-chipper-an teks yang dilakukan.

Kata kunci : penyandian, multiple xor, peretas

Pendahuluan

Pada era Teknologi Informasi saat ini perusahaan berupaya untuk menyimpan data atau informasi yang dimiliki dengan sangat rapi, karena informasi tersebut menjadi kekuatan yang dimiliki oleh perusahaan dalam maju mundur perusahaan dalam melakukan bisnisnya. Banyak media informasi yang menginformasikan bahwa banyak perusahaan yang di-*hacker* (dirusak) oleh para hacker, para hacker tersebut mang-*hack* bukan di negaranya sendiri bahkan ke berbagai negara dan tidak masalah apakah perusahaan itu perusahaan besar atau sedang dan juga yang menghacker tersebut bukan orang dewasa tetapi anak yang berusia 15 tahun mampu meretas berbagai perusahaan di benua Eropa dan Amerika yang mengakibatkan kerugian yang cukup besar yang dialami perusahaan-perusahaan tersebut.

Cara merusak atau masuk ke sistem dapat dilakukan tanpa sepengetahuan dari para *Database Administrator* (DBA), dan pada waktunya sistem dan *database*nya telah ter-retas yang mangakibatkan sumber data (*database*) telah berubah dan data atau informasinya tersebar atau rusak dan mengakibatkan mengalami kerugian yang cukup besar akibat perusakan data atau informasi yang dimilkinya.

Dengan penjelasan informasi di atas, perusahaan harus berusaha untuk menyimpan data atau informasi yang dimilikinya dengan baik dan aman, karena itu sangat diperlukan bagaimana bentuk penyandian yang sesuai dengan kebutuhan perusahaan sehingga data dan informasi yang dimiliki aman

dari para hacker atau bila data atau informasi yang diperoleh para hacker bisa tidak bermanfaat baginya. Hasil dari penyandian tersebut tidak dapat dipahami atau tidak dapat digunakan oleh para hacker, sehingga data atau informasi aman dari keinginan-keinginan para hacker tersebut.

Sejarah Kriptografi

Seni kriptografi ini lahir bersama-sama dengan seni menulis. Di mana pada waktu itu manusia ingin menyampaikan sebuah pesan yang tanpa harus diketahui orang lain tentang pesan yang dibawa oleh seseorang ke orang yang ingin disampaikan pesan tersebut. Beberapa abad yang lalu di Mesir, seorang raja ingin menyampaikan pesannya ke seseorang pejabat kerajaan tersebut yang dihantar oleh seorang pelayan kerajaan, untuk itu sang raja mencoba untuk merahasiakan pesan yang dikirimkan itu dengan cara menyandikan informasi tersebut dan kemudian pesan yang disampaikan dapat dibaca oleh penerima pesan dengan cara yang disepakati.

Kemudian datanglah para ahli Taurat mencoba untuk membuat penyandian dengan atas nama raja seperti teknik penyandian di bawah ini :

Gambar 1
Teknik Penyandian Ahli Taurat

Masalah yang Dihadapi

Banyak teknik mengenkripsi dan mendekripsi yang dibangun dalam penyandian, agar informasi yang disimpan atau dikirim tidak berubah atau benar-benar belum di-hack oleh hacker. Dalam masalah ini adalah bagaimana melihat proses *Enkripsi* dan *Dekripsi* yang dapat dilakukan dan bagaimana untuk membangun enkripsi dengan tingkat kesulitan yang lebih demi untuk menjaga keamanan data atau informasi yang dimiliki. Pada masalah ini dibangun pengenkripsian dengan metode Multiple XOR, demikian juga untuk mendekripsi data atau informasi tadi.

Metode Penelitian

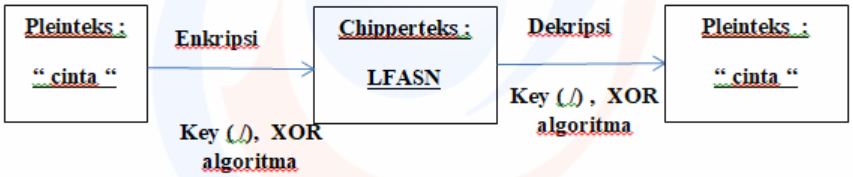
Kriptografi adalah sebuah sistem untuk menyandikan teks yang dapat dipahami menjadi teks yang diacak sehingga tidak dapat dimengerti oleh penerimanya. Kriptografi berasal dari bahasa Yunani, dibagi menjadi 2 kata, yaitu *Crypto* adalah menyembunyikan dan *Graphia* adalah tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data serta authentikasi data.

Kriptografi dapat juga disebut sebagai suatu ilmu atau seni untuk mengamankan/merahasiakan suatu informasi atau pesan yang dimiliki (Yusuf, 2004).

Keamanan Data adalah bagaimana dapat melindungi data digital seperti data dalam database dari kekuatan yang merusak dan dari tindakan penggunaan tidak sah yang tidak diinginkan.

Kerahasiaan Data adalah bagaimana cara untuk dapat menjaga data dari serangan-serangan dari para hacker atau orang yang tidak berhak pada data tersebut.

Keabsahan Data adalah bagaimana cara agar konsep penting ini dapat diperbaharui dari konsep keteralihan data dan keandalannya. Dalam kabsahan data ini perlu diperhatikan tentang derajat kepercayaan, keteralihan, ketergantungan dan kepastiannya.



Gambar 1
Dasar teknik kriptografi

Integritas Data adalah bagaimana dapat dipastikan keakuratan data karena sangat diperlukan untuk dipastikan keakuratan, konsistensi, aksessibilitasi dan kulitas dari data tersebut selama dalam pengirimana berlangsung. Data tersebut tidak/belum dimodifikasi oleh orang yang tidak berkenan pada data tersebut, sehingga dapat mengikuti aturan pengintegrasian datanya. Di dalam masalah ini sangat diperlukan akurasi dan kebenaran data (URL 2)

Autentikasi Data adalah bagaimana cara untuk dapat mengenal atau memastikan atau memvalidasi terhadap seorang pengguna untuk masuk ke sistem.

Teknik Pengumpulan Data

Dalam masalah pengumpulan data yang berkaitan dari masalah ini, dapat dilakukan dengan dua cara :

a. Studi Pustaka

Berdasarkan informasi yang ada, perlu dilakukan penyelesaian masalah yang berkaitan dengan masalah peretas, karena itu dicari metode-metode yang berkaitan dengan masalah tersebut.

b. Survei

Langsung mencari data kelapangan untuk mengetahui sejauh mana permasalahan tentang peretas yang terjadi dalam kehidupan perusahaan maupun perorangan.

Berdasarkan observasi yang diamati di lapangan, peretas tidak hanya mengambil data dari database pada saat user sedang akses, juga peretas dapat mengambil data atau informasi yang penting pada saat berlangsung pengiriman data. Sering juga peretas menyusupkan virus pada saat user sedang melakukan pengiriman data sehingga membuat sistem yang sedang digunakan bisa menjadi *error*.

Pada masalah ini yang dibahas adalah masalah tentang penyandian informasi agar informasi yang disandikan itu pada saat dikirim oleh user dapat diambil oleh para peretas tapi peretas tidak memahami informasi yang sedang dikirim tersebut atau data yang telah disandi disimpan dalam database.

Aplikasi dan Pembahasan

Pada dasarnya Kriptografi memiliki 4 komponen besar, yaitu : Pleinteks digunakan sebagai input, *Key* untuk mengenkripsi atau dekripsi dan disebut juga *Secret Key*, pengolahan menggunakan XOR dan chiperteks sebagai outputnya. *Pleinteks* adalah bahasa tingkat tinggi atau yang dipakai oleh manusia kemudian diproses atau diubah ke bilangan biner (bahasa mesin) dalam bentuk ASCII kemudian diolah dengan menggunakan key untuk mengenkripsi atau deskripsi kemudian dihasilkan bahasa mesin atau bilangan biner dan dikonversi ke bahasa tingkat tinggi menghasilkan teks yang acak sesuai dengan alpabetik yang ada.

Dalam masalah yang akan dibahas adalah bagaimana melakukan proses enkripsi dan hasil enkripsi ini yang dikirimkan ke penerima informasi dan kemudian penerima mendekripsi informasi atau teks yang telah dichiper kemudian penerima informasi mendekripsi *chiperteks* yang dikirim dengan menggunakan key yang sudah ditentukan sehingga penerima informasi dapat mengetahui informasi yang dikirim kepada penerima.

Kasus Enkripsi I

Pada kasus pengenkripsian ini diberikan pleintext dan kunci yang berbeda, input yang diberikan dalam bentuk teks sebagai berikut " cinta "dapat diolah ke basis 2 dengan menggunakan tabel ASCII adalah :

Tabel 1
Pleinteks

Karakter	Basis 10	Basis 2
c	99	01100011
i	105	01101001
n	110	01101110
t	116	01111100
a	97	01100001

Key yang diberikan untuk kasus ini adalah / = 47 basis 10 = 00101111 basis 2 key ini dapat juga menggunakan karakter.

Untuk proses pengolahan datanya diperlukan model biimplikasi (Samuel,2008), sebagai berikut :

Tabel 2
XOR

p	q	$p \leftrightarrow q$
0	0	0
0	1	1
1	0	1
1	1	0

Hasil yang diperoleh dari input (*pleintexts*) yang diberikan seperti diatas dengan operasi menggunakan XOR, maka hasil yang diperoleh adalah

Tabel 3
Chiperteks

Karakter	Basis 2	Basis 10
L	01001100	76
F	01000110	70
A	01000001	65
S	01010011	83
N	01001110	78

Dari pleintexts (input) yang diberikan adalah " cinta" maka setelah dilakukan penyandian maka informasinya atau *chipertext*nya yang dihasilkan "LFASN" dan informasi inilah yang akan dikirimkan ke si penerima informasi yang disebut dengan Enkripsi, setelah diterima oleh penerima, informasi dilakukan Dekripsi dengan Key yang sama dan operasi yang sama juga akan menghasilkan informasi semula.

Kasus Enkripsi ke II

Pada kasus pengenkripsian ini diberikan pleintexts dan kunci di mana memiliki karakter yang sama, input yang diberikan dalam bentuk texts sebagai berikut " cinta " seperti pada table 1, dapat diolah ke basis 2. Kemudian diberikan key sebagai berikut "siapa " dengan basis 2 sebagai berikut :

Tabel 4
Key

Karakter	Basis 10	Basis 2
s	115	01110011
i	105	01101001
a	97	01100001
p	112	01110000
a	97	01100001

Bila dilakukan operasi dengan XOR, akan menghasilkan :

Tabel 5
*Chipertext*s

Pleintexts	XOR	Basis 2	*Chipertext*s
c		00010000	Del
i		00000000	0
n		00001111	SI
t		00001100	FF
a		00000000	0

Masalah yang terjadi dalam peng-engkripsian ini, bila input (pleintexts) memiliki posisi karakter dengan key-nya adalah sama maka karakter yang dihasilkan adalah nol seperti yang ditunjukkan pada baris ke-2 dengan karakter (i) dan baris ke-5 dengan karakter (a) yang mengakibatkan karakter yang dienkripsi menjadi error, dan untuk mengatasi masalah ini perlu dilakukan pendeklarasian karakter bila memiliki posisi yang sama atau memisalkan karakter di pleintexts dengan karakter yang lainnya.

Algoritma untuk enkripsi dan dekripsinya adalah sebagai berikut :

Enkripsi :

Mulai

Input : plaintext dan key

Lakukan XOR antara Pleintext versus key dengan ketentuan :

Proses XOR pertama :

1. Jika plaintext sama dengan key maka outputnya adalah ASCII(180)
2. Jika hasil plaintext dengan key di bawah ASCII(32) maka hasil XOR nya ditambah ASCII(180)

Setelah itu dilakukan flipping characters hasil dari XOR tadi.

Contoh " cinta " menjadi "atnic".

Proses XOR kedua

Kemudian hasil dari flipping characters di XOR dengan key maka diperoleh hasil *Chipertext*. Hasil dari *chipertext* inilah yang akan dikirimkan ke si penerima informasi yang dituju.

Deskripsi

Mulai

Input : *Chipertext*s dan key

Proses XOR pertama :

Lakukan XOR antara *Chipertext*s versus key.

Hasil XOR, pertama dilakukan flipping characters.

Proses XOR kedua :

Kemudian dilakukan XOR antara flipping characters dengan key, dengan ketentuan :

1. Jika hasil flipping characters nya sama dengan ASCII(180), maka plaintext sama dengan key.
2. Jika hasil flipping charactersnya lebih besar dari ASCII(180) maka hasil pleintextnya dikurangi ASCII(180), kemudian di XOR dengan keynya

Diperoleh hasil yang sama dengan antara plaintext ke chippertext dan chippertext ke *plaintext*. Maka si penerima informasi memperoleh informasi yang sama dengan informasi yang dikirimkan oleh si pengirim informasi.

Kesimpulan

Dari hasil analisis dan pembahasan di atas dapat diambil kesimpulan, sebagai berikut : Untuk pengenkripsian data, bila input data di mana *character* berbeda dengan key maka pengenkripsian data dapat dilakukan langsung. Bila input data di mana character inputannya ada yang sama dengan key maka hasil XOR-nya adalah nol maka hasil cipertextnya di tempatkan pada ASCII(180) agar menghasilkan characters yang tidak berbeda, maka harus dibalik *charactersnya*. Hasil *Plaeintext* ke *chipertext* dan *chipertext* ke plaintext harus sama supaya informasi yang dikirim sama dengan yang diterima.

Daftar Pustaka

Abdul Halim Hasugian, Implementasi Algoritma Hill Chipher Dalam Penyandian Data, Jurnal Pelita Informatika Budi Darma, Volume IV, No,2 Agustus 2013, ISSN : 2301-9425

C. Paar, J. Pelzl, 2010 ”Understanding Cryptography-Textbook for Student and Practitioners”. Springer

HCA Van Tilborg, “ Fundamentals of cryptography”, Kluwer Academic Publisher. London

Menezes, P. Van Oorschot, and S. Vanstone, 1996, “Handbook of Applied Cryptography”, CRC Press. USA

Samuel Wibisono, 2008, Matematika Diskrit, Graha Ilmu, Yogyakarta

Suprianto, Sistem pengkodean Data Pada File Teks Pada Keamanan Informasi Dengan Menggunakan Metode SKIPJACK, Jurnal Computech dan Bisnis, Vol. 1 N0.2, Desember 2007, hal 105-118.ISSN 1978-9629

Yusuf Kurniawan, 2004, Kriptografi, Penerbit Informatika, Bandung

A. URL

- http://www.asciitable.com/
- http://ondigitalforensics.weebly.com/cryptography/pengertian-dan-contoh-kriptografi-dengan-proses-enkripsi-dan-dekripsi#.Wl1_E3kxW1s
- https://andinox.wordpress.com/2011/11/29/program-enkripsi-dekripsi-dengan-c/
-