ILKOM JURNAL ILMIAH

Volume 4, Nomor 1

April 2012

MASHUR RAZAK

Pengamanan Sistem Informasi Melalui Enkripsi Data

PURNAWANSYAH

Implementasi Citra Digital Dengan Menggunakan Fungsi GST (Gray Scale Transformation)

EDY BUDIMAN

Implikasi Teori Konstruktivisme Dalam Perancangan Sistem Pembelajaran Online

NIA KURNIATI

Single-Source Shortest Path Pada Graf Berbobot Menggunakan Algoritma Dijkstra Dan Algoritma Bellman-Ford

HERLINA

Sistem Informasi Objek Wisata Provinsi Sulawesi Barat Berbasis Web

MUSTAFA HASBAR

Enterprise Resource Planning (ERP) (Suatu Kajian Teoritis)

HARLINDA L.

Analisis Tingkat Klorofil Daun Dengan Menggunakan Jaringan Syaraf Tiruan Propagasi Balik

NUR ICHSAN RACHMAN

Sistem Kendali Buka Tutup Pintu Otomatis Berbasis Mikrokontroler

MUHAMMAD DIAH YUSUF

Metodologi Siklus Hidup Sistem

SISKA ANRAENI

Perancangan E-Library Pada SMAN 1 Tellu Limpoe Kabupaten Sidenreng Rappang

FAKULTAS ILMU KOMPUTER - UNIVERSITAS MUSLIM INDONESIA - MAKASSAR

JURNAL
ILKOM JURNAL ILMIAH

Vol. 4

No. 1

Hlm. 1 - 77

Makassar
April 2012

ISSN
2087 - 1716

ISSN 2087-1716

ILKom JURNAL ILMIAH

VOLUME 4, Nomor 1

April 2012

Pemimpin Umum

H. Muhammad Diah Yusuf, Ph.D

Pemimpin Redaksi

Hj. Harlinda L., S.Kom., MM., M.Kom.

Penyunting Pelaksana

Ir. Hamri, MT

Purnawansyah, S.Kom., M.Kom.

St. Hajrah Mansyur, S.Kom., M.Kom

Hadriana Iddas, ST., MT.

Penyunting Ahli

Andi Suryanto, ST., MT.

Ir. Hardi H. Ismail, MT.

Dolly Indra, S.Kom., M.MSi.

Drs. Muslim, MT.

Mitra Bestari

Dr. Ernastuti, S.Kom., M.Kom. (Univ. Gunadarma Jakarta)

Dr. Ahmad Azhari, M.Kom. (UGM Yogyakarta)

Sekretariat

Poetri Lestari, S.Kom.

Siska Anraeni, S.Kom.

Ramdan Satra, S.Kom.

Sirkulasi

Syahrul Mubarak, S.Kom.

Abd. Rachman Manga, S.Kom.

Alamat Redaksi/Penerbit

Fakultas Ilmu Komputer Universitas Muslim Indonesia Makassar
Kampus II Jl. Urip Sumoharjo km 05 Tlp. 0411 453009 Fax. 0411 453009 Makassar 90231

JURNAL ILKom

FAKULTAS ILMU KOMPUTER UMI MAKASSAR
TERBIT TIAP 4 (EMPAT) BULANAN

DAFTAR ISI

ILKom JURNAL ILMIAH

Volume 4, Nomor 1

April 2012

Daftar Isi	i
Pengamanan Sistem Informasi Melalui Enkripsi Data MASHUR RAZAK	1 – 12
Implementasi Citra Digital Dengan Menggunakan Fungsi GST (Gray Scale Transformation) PURNAWANSYAH	13 – 18
Implikasi Teori Konstruktivisme Dalam Perancangan Sistem Pembelajaran Online EDY BUDIMAN	19 – 28
Single-Source Shortest Path Pada Graf Berbobot Menggunakan Algoritma Dijkstra Dan Algoritma Bellman-Ford NIA KURNIATI	29 – 35
Sistem Informasi Objek Wisata Provinsi Sulawesi Barat Berbasis Web HERLINA	36 – 42
Enterprise Resource Planning (ERP) (Suatu Kajian Teoritis) MUSTAFA HASBAR	43 – 48
Analisis Tingkat Klorofil Daun Dengan Menggunakan Jaringan Syaraf Tiruan Propagasi Balik HARLINDA L.	49 – 56
Sistem Kendali Buka Tutup Pintu Otomatis Berbasis Mikrokontroler NUR ICHSAN RACHMAN	57 – 62
Metodologi Siklus Hidup Sistem MUHAMMAD DIAH YUSUF	63 – 67
Perancangan E-Library Pada SMAN 1 Tellu Limpoe Kabupaten Sidenreng Rappang SISKA ANRAENI	68 – 77

PENGAMANAN SISTEM INFORMASI MELALUI ENKRIPSI DATA

Mashur Razak

STMIK Handayani Makassar

E-mail: mashur_razak@yahoo.co.id

Abstract: In the era of "information-based society", information is one of the very important economic resources. The ability to access and provide information quickly and accurately becomes very essential for organizations, whether in the form of commercial organizations or nonprofit organizations. The value of an information leads to the desired information is often can only be accessed by certain people. Therefore, security issue is an important aspect within information system. The developments of information technology, especially in data communications generate information systems more vulnerable to various types of threats that can damage the system or data. Threats can come from the hacker attack and malicious program made up of Trap doors, Logic Bombs, Trojan Horses and Viruses. Therefore, information management has to provide security and control system. One strategy for information security system that can be used is Encryption, which is a process to secure a message (called plain text) into a hidden message (called cipher text). Ciphertext is a message that is not readable. Encryption is used to encrypt the data or information that cannot be read by unauthorized people. By encrypting, the data is encoded using a key. To open (decrypt) the data, a key is needed which can be the same as the key to encrypt (for the case of private key cryptography Based Information Systems Security) or with a different key (for the case of public key cryptography). Implementation of Data Encryption is expected to provide data and system security that covers Confidentiality, Integrity and Availability.

Keyword : encryption, ciphertext, encrypted, Confidentiality, Integrity dan Availability

PENDAHULUAN

Pada dasarnya setiap data yang disimpan dalam bentuk elektronik sangat rentan terhadap berbagai jenis ancaman, baik dari pihak internal maupun dari luar system. Dalam system jaringan komunikasi, system informasi pada lokasi geografis yang berbeda saling berhubungan, sehingga peluang untuk melakukan akses secara tidak sah, penyalahgunaan, penipuan tidak terbatas pada lokasi tunggal, tetapi juga dapat terjadi pada titik akses manapun dalam jaringan (Laudon, 2007). Ancaman terhadap keamanan computer dapat berasal dari faktor teknis, organizational dan lingkungan. Dalam system jaringan gangguan keamanan dapat terjadi

pada setiap lapisan dan di dalam komunikasi antar lapisan. Pengguna pada tingkat klien dapat menyebabkan kerusakan dengan cara melakukan kesalahan, mengakses tanpa izin atau secara tidak sengaja mengunduh (*download*) spyware dan virus. Hacker melalui berbagai tipu muslihat dapat mengakses data yang mengalir dalam jaringan, mencuri data yang penting selama dalam pengiriman atau mengubah pesan tanpa izin.

Dalam jaringan internet keamanan system juga rentan terhadap gangguan karena sifatnya yang terbuka. Salah satu bentuk gangguan keamanan dalam jaringan internet adalah *Denial-of-service*, yaitu serangan penolakan layanan yang dilakukan oleh penyusup

dengan tujuan untuk mengganggu operasi situs web. Program yang menyusup dalam system perusahaan dapat menghancurkan atau mengubah data perusahaan yang tersimpan dalam basis data atau *file*.

Dalam dunia bisnis, Informasi merupakan salah satu sumberdaya yang sangat penting untuk dilindungi. Karena banyak perusahaan semakin bergantung pada jaringan digital untuk pendapatan dan operasi bisnisnya, perusahaan harus mengambil langkah tambahan untuk menjamin bahwa system dan aplikasinya selalu dapat digunakan. Seperti: pemrosesan transaksi *online* (*online transaction processing*), transaksi masuk online dengan segera diproses oleh computer. Dari beberapa fakta tentang kerentanan terhadap pengamanan system tersebut di atas, mendorong manajemen system informasi pada semua organisasi untuk menempatkan pengamanan dan pengendalian system sebagai salah satu prioritas utama. Oleh sebab itu manajemen informasi harus menyediakan pengamanan dan pengendalian system yang mampu menjamin keamanan data dan system dari aspek, *Confidentiality* (Kerahasiaan), *Integrity* (Integritas) maupun *Availability* (ketersediaan).

ANCAMAN KEMAMAN SISTEM KOMPUTER

Secara umum terdapat 2 (dua) ancaman paling signifikan terhadap keamanan system computer, yaitu : 1) *Intrudes* dan 2) *Malicious Program* (Ali, 2007). *Intrudes* biasanya dikenal dengan istilah "hackers/crackers". *Hacker* adalah seorang yang ingin mendapatkan akses tidak sah

keseluruh sistem komputer dalam komunitas hacking, istilah *cracker* secara khusus digunakan untuk menunjukkan seorang hacker yang memiliki maksud kriminal, meskipun dalam isi pers publik, istilah hacker dan cracker digunakan secara bergiliran. *Hacker* dan *cracker* mendapatkan akses secara tidak sah dengan cara mencari kelemahan perlindungan keamanan yang digunakan oleh sistus dan system computer. Selain itu hackers adalah suka bertukar informasi dengan siapa saja sehingga teknik-teknik keamanan terbaru mungkin saja dengan mudah didapat dan dipelajari kelemahannya. Kehadiran Hacker antara lain disebabkan oleh *Globalization, The move to client/server* dan *Hackers' steep learning curve*. Aktivitas hacker yang semakin meluas, tidak hanya sekedar menyusup ke dalam system, tetapi juga melputi pencuria barang dan informasi serta merusak system dan melakukan Vandalisme Maya (*cybervandalism*).

Malicious Program terdiri dari *Need Host Program* dan *Independent*. Beberapa jenis ancaman kewan system computer yang termasuk dalam kelompok *Need Host Program* adalah 1) *Trapdoors* : Akses masuk rahasia ke dalam suatu program tanpa melalui prosedur yang seharusnya. Biasanya dibuat pada saat melakukan ujicoba suatu program, 2) *Logic Bombs* : Perintah yang dituliskan dalam suatu program yang akan meledak apabila suatu kondisi terpenuhi, 3) *Trojan Horses* : Perintah rahasia yang dibuat secara tidak terlihat dalam suatu program untuk melakukan suatu tindakan apabila program dijalankan dan 3) *Viruses* :

Program/perintah yang diselipkan ke dalam suatu program lain yang akan memperbanyak dirinya sendiri dan memasukkannya kembali ke dalam program lainnya. Pada saat menjangkiti, akan timbul suatu tindakan tidak diinginkan/merusak.

KEJAHATAN KOMPUTER DAN TERORISME MAYA

Kejahatan computer pada dasarnya adalah pelanggaran hukum criminal apapun yang melibatkan pengetahuan teknologi computer untuk tujuan kejahatan, penyelidikan atau penuntutan Menurut Loudon (2007), sebagian besar aktivitas **hacker** adalah kejahatan kriminal, dan kerentanan system yang telah dijelaskan membuat sistem-sistem tersebut menjadi sasaran juga untuk kejahatan komputer jenis lainnya. Hasil penelitian Computer Crime Research Centre, perusahaan AS mengalami kerugian sekitar 14 milyar dollar setiap tahunnya akibat kejahatan dalam dunia maya. Bahkan mungkin jauh lebih besar lagi sebab

banyak perusahaan yang enggan untuk melaporkan kejahatan computer karena kejahatan tersebut mungkin melibatkan karyawan perusahaan yang bersangkutan.

Bentuk kejahatan lain dalam perdagangan elektronik adalah **Pencurian identitas** yang merupakan kejahatan dimana seorang penipu mendapatkan informasi yang penting, seperti nomor jaminan sosial, untuk menyamar sebagai orang lain. Bentuk yang paling populer adalah sejenis *spoofing* yang dinamakan *phishing*. *Phishing* merupakan kegiatan membuat situs palsu atau mengirim pesan email yang mirip dengan pesan dari perusahaan yang sah untuk meminta pengguna mengisi data pribadi mereka yang rahasia. Sedangkan **Pharming** adalah kegiatan mengalihkan pengguna kehalaman Web yang palsu, bahkan ketika seseorang mengetikkan alamat Web yang benar pada aplikasi penjelajahnya.

KOMPUTER SEBAGAI TARGET KEJAHATAN	KOMPUTER SEBAGAI ALAT KEJAHATAN
Menerobos kerahasiaan data terkomputerisasi yang dilindungi.	Pencurian rahasia dan penyalinan piranti lunak atau penjiplakan hak cipta yang tidak syah seperti : artikel, buku, music, video.
Mengakses system informasi tanpa otorisasi	Pola-pola penipuan
Dengan sengaja mengakses computer yang dilindungi untuk melakukan penipuan	Menggunakan e-mail untuk mengacau atau melecehkan
Dengan sengaja mengakses computer yang dilindungi dan menyebabkan kerusakan secara sembrono atau disengaja	Dengan sengaja membajak komunikasi elektronik
Dengan sengaja mengirim sebuah program, kode program atau program	Secara illegal mengakses komunikasi elektronik yang tersimpan, termasuk e-

yang menyebabkan kerusakan pada program yang dilindungi.	mail dan pesan suara
Mengancam hingga menyebabkan kerusakan pada computer yang dilindungi.	Mengirim atau memiliki materi pornografi anak di komputer

Sumber : Louden (2007)

KEBIJAKAN DAN KEAMANAN SISTEM INFORMASI

Pengamanan merupakan kebijakan, prosedur, dan pengukuran teknik yang digunakan untuk mencegah yang tidak sah, penggantian, pencurian, kerusakan fisik pada sistem informasi. Pengendalian terdiri atas semua metode, kebijakan, dan prosedur organisasi yang menjamin keselamatan aset – aset organisasi. (Laudon, 2007). Kebijakan pengaman (*security policy*) terdiri atas pernyataan yang menilai risiko informasi, mengidentifikasi tujuan pengamanan yang berterima, dan mengidentifikasi mekanisme untuk mencapai tujuan ini.

Kebijakan pengamanan mengatur kebijakan yang menentukan penggunaan sumber-sumber informasi perusahaan yang dapat diterima dan anggota mana dari perusahaan yang memiliki akses ke aset informasinya. Kebijakan penggunaan yang dapat diterima (*acceptable use policy-AUP*) mengidentifikasi penggunaan sumber-sumber informasi perusahaan dan perangkat komputasi, termasuk PC dan laptop, perangkat nirkabel, telepon, dan internet, yang diizinkan.

Kebijakan otorisasi (*authorization policy*) menentukan tingkat akses yang berbeda ke aset informasi untuk tingkat pengguna yang berbeda pula. System manajemen otorisasi (*authorization*

management sistem) menentukan dimana dan kapan seorang pengguna diizinkan untuk mengakses bagian tertentu dari situs atau basis data perusahaan. Perlindungan sumber-sumber informasi membutuhkan kebijakan pengamanan dan seperangkat pengendalian yang kuat. ISO 17799 merupakan salah satu standar internasional dalam pengamanan dan pengendalian, memberikan panduan yang membantu. ISO 17799 menyatakan praktik-praktik terbaik dalam pengamanan dan pengendalian system informasi, termasuk kebijakan pengamanan, rencana kontinuitas bisnis, pengamanan fisik, pengendalian akses, kepatuhan, dan pembuatan fisik pengamanan dalam organisasi.

Menurut Thaief (2008), keamanan system informasi pada dasarnya terdiri dari perlindungan terhadap aspek-aspek berikut :

1. **Confidentiality** (Kerahasiaan), yaitu aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan
2. **Integrity** (Integritas), yaitu aspek yang menjamin bahwa data tidak diubah tanpa ada izin dari pihak yang berwenang (*authorized*), menjaga keakuratan dan kutuhan

informasi serta metode prosesnya untuk menjamin aspek integritas tersebut.

3. **Availability** (ketersediaan), aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user dapat menggunakan informasi dan perangkat diperoleh terkait.

PENGAMANAN SISTEM INFORMASI MELALUI ENKRIPSI DATA

Enkripsi (*encryption*) pada dasarnya adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah (Raharjo, 2002). Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah "*encipher*". Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut **dekripsi** (*decryption*). Menurut ISO 7498-2, terminologi yang lebih tepat untuk proses ini adalah "*decipher*". *Cryptanalysis* adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci. *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis*. *Cryptology* merupakan gabungan dari *cryptography* dan *cryptanalysis*.

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data anda disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci

untuk mengenkripsi (untuk kasus *private key* Keamanan Sistem Informasi Berbasis *cryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*). Gambar 1 menunjukkan contoh proses enkripsi dan dekripsi dengan dua kunci yang berbeda.

Gambar 1. Diagram proses enkripsi dan dan dekripsi

Sumber : Raharjo (2002)

Secara matematis, proses atau fungsi enkripsi (E) dapat dituliskan sebagai: $E(M) = C$, dimana: M dalah *plaintext* (*message*) dan C adalah *ciphertext*. Sedangkan Proses atau fungsi dekripsi (D) dapat dituliskan sebagai $D(C) = M$

ELEMEN DARI ENKRIPSI

Menurutu Raharjo (2002), ada beberapa elemen dari enkripsi yang akan dijabarkan dalam beberapa bagian, antara lain :

Algoritma dari Enkripsi dan Dekripsi. Algoritma dari enkripsi adalah fungsi-fungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi. Algoritma yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika. Berdasarkan cara memproses teks (*plaintext*), cipher

dapat dikategorikan menjadi dua jenis: *block cipher* and *stream cipher*. Block cipher bekerja dengan memproses data secara blok, dimana beberapa karakter / data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga. Sementara itu stream cipher bekerja memproses masukan (karakter atau data) secara terus menerus dan menghasilkan data pada saat yang bersamaan.

Kunci yang digunakan dan panjangnya kunci. Kekuatan dari penyandian bergantung kepada kunci yang digunakan. Beberapa algoritma enkripsi memiliki kelemahan pada kunci yang digunakan. Untuk itu, kunci yang lemah tersebut tidak boleh digunakan. Selain itu, panjangnya kunci, yang biasanya dalam ukuran *bit*, juga menentukan kekuatan dari enkripsi. Kunci yang lebih panjang biasanya lebih aman dari kunci yang pendek. Jadi enkripsi dengan menggunakan kunci 128-bit lebih sukar dipecahkan dengan algoritma enkripsi yang sama tetapi dengan kunci 56-bit. Semakin panjang sebuah kunci, semakin besar keyspace yang harus dijalan untuk mencari kunci dengan cara *brute force attack* atau coba-coba karena keyspace yang harus dilihat merupakan pangkat dari bilangan 2. Jadi kunci 128-bit memiliki keyspace 2128, sedangkan kunci 56-bit memiliki keyspace 256. Artinya semakin lama kunci baru bisa ketahuan.

Plaintext. Plaintext adalah pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca atau dalam bentuk aslinya.
Ciphertext. Ciphertext adalah

informasi yang sudah dienkripsi. Keamanan sebuah algoritma yang digunakan dalam enkripsi atau dekripsi bergantung kepada beberapa aspek. Salah satu aspek yang cukup penting adalah sifat algoritma yang digunakan. Apabila kekuatan dari sebuah algoritma sangat tergantung kepada pengetahuan (tahu atau tidaknya) orang terhadap algoritma yang digunakan, maka algoritma tersebut disebut "restricted algorithm". Apabila algoritma tersebut bocor atau ketahuan oleh orang banyak, maka pesan-pesan dapat terbaca. Tentunya hal ini masih bergantung kepada adanya kriptografer yang baik. Jika tidak ada yang tahu, maka sistem tersebut dapat dianggap aman (meskipun semu). Meskipun kurang aman, metoda pengamanan dengan *restricted algorithm* ini cukup banyak digunakan karena mudah implementasinya dan tidak perlu diuji secara mendalam. Contoh penggunaan metoda ini adalah enkripsi yang menggantikan huruf yang digunakan untuk mengirim pesan dengan huruf lain. Ini disebut dengan "*substitution cipher*".

SUBSTITUTION CIPHER DENGAN CAESAR CIPHER

Salah satu contoh dari "*substitution cipher*" adalah Caesar Cipher yang digunakan oleh Julius Caesar. Pada prinsipnya, setiap huruf digantikan dengan huruf yang berada tiga (3) posisi dalam urutan alfabet. Sebagai contoh huruf "a" digantikan dengan huruf "D" dan seterusnya. Transformasi yang digunakan adalah:


```
plain: 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
cipher: 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
```

ROT13

Substitution cipher yang masih umum digunakan di sistem UNIX adalah ROT13. Pada sistem ini sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya. Sebagai contoh, huruf "A" digantikan dengan huruf "N", huruf "B" digantikan dengan huruf "O", dan seterusnya. Secara matematis, hal ini dapat dituliskan sebagai:

$$C = ROT13(M)$$

Untuk mengembalikan kembali ke bentuk semulanya dilakukan proses enkripsi ROT13 dua kali [37].

$$M = ROT13(ROT13(M))$$

ROT13 memang tidak didisain untuk keamanan tingkat tinggi. ROT13, misalnya digunakan untuk menyelubungi isi dari artikel (*posting*) di *Usenet news* yang berbau ofensif. Sehingga hanya orang yang betul-betul ingin membaca dapat melihat isinya. Contoh penggunaan lain adalah untuk menutupi jawaban dari sebuah teka teki (*puzzle*).

Program dalam bahasa *Perl* untuk melakukan ROT13 dapat dilihat dalam listing di bawah ini.

```
#!/usr/bin/perl
# rot13: rotate 13
# usage: perl rot13 < filename.txt
# bugs: only works with lower case
#
# Copyright 1998, Budi Rahardjo
```

```
# <rahard@paume.itb.ac.id>,
# <budi@vlsi.itb.ac.id>
# Electrical Engineering
# Institut Teknologi Bandung (ITB),
# Indonesia
#
while (<>) {
# read a line into $_
for ($i=0 ; $i < length($_) ; $i++) {
$ch = substr($_,$i,1);
# only process if it's within a-z
# otherwise skip
if ( (ord($ch)>=97) and
(ord($ch)<=122) ) {
$newch = &rot13($ch); # rotate it
printf("%c", $newch);
} else {
# just print character that was not
processed
print $ch;
}
} # end for loop
} # done...
sub rot13 {
local($ch) = @_;
$asch = ord($ch) - 97; # get the ascii
value and normalize it
$rotasch = $asch + 13; # rotate 13 it
# send it back to ascii
$rotasch = $rotasch % 26;
$rotasch = $rotasch + 97;
return($rotasch);
}
```

Sumber : Raharjo (2002)

Caesar cipher dan ROT13 disebut juga "*monoalphabetic ciphers*" karena setiap huruf digantikan dengan sebuah huruf. Huruf yang sama akan memiliki pengganti yang sama. Misalnya huruf "a" digantikan dengan huruf "e", maka setiap huruf "a" akan digantikan dengan huruf "e". Mono alphabetic cipher ini agak mudah dipecahkan dengan menganalisa ciphertext apabila beberapa informasi lain (seperti bahasa yang digunakan) dapat

diketahui. Salah satu cara penyerangan (*attack*) yang dapat dilakukan adalah dengan menganalisa statistik dari frekuensi huruf yang muncul. Cara ini disebut *frequency analysis*.

Frequency analysis bermanfaat jika teks yang tersedia cukup panjang. Teks yang pendek, dengan jumlah huruf yang lebih sedikit, biasanya memiliki deviasi dari data-data statistik munculnya huruf. Selain itu ada beberapa kasus dimana sengaja dibuat teks yang “merusak” struktur frekuensi tersebut. Sebagai contoh, pengarang Perancis yang bernama Georges Perec di tahun 1969 menulis “*La Disparition*” (sebuah novel dengan 200 halaman) tanpa kata yang menggunakan huruf “e”. Karya ini kemudian diterjemahkan oleh ke dalam bahasa Inggris oleh seorang pengarang Inggris yang bernama Gilbert Adair dengan tetap tanpa menggunakan huruf “e”. Judul terjemahannya adalah “*A Void*”.

Multiple-letter encryption

Untuk meningkatkan keamanan, enkripsi dapat dilakukan dengan mengelompokkan beberapa huruf menjadi sebuah kesatuan (unit) yang kemudian dienkripsi. Ini disebut *multiple-letter encryption*. Salah satu contoh *multiple-letter encryption* adalah “*Playfair*”.

Enigma Rotor Machine

Enigma rotor machine merupakan sebuah alat enkripsi dan dekripsi mekanik yang digunakan dalam perang dunia ke dua. Dia terdiri atas beberapa rotor dan kabel yang silang menyilang menyebabkan substitusi

alfabet yang selalu berubah sehingga Enigma mengimplementasikan polyalphabetic cipher.

Penggunaan Kunci

Salah satu cara untuk menambah tingkat keamanan sebuah algoritma enkripsi dan dekripsi adalah dengan menggunakan sebuah kunci (*key*) yang biasanya disebut *K*. Kunci *K* ini dapat memiliki rentang (*range*) yang cukup lebar. Rentang dari kemungkinan angka (harga) dari kunci *K* ini disebut *keyspace*. Kunci *K* ini digunakan dalam proses enkripsi dan dekripsi sehingga persamaan matematisnya menjadi:

$$EK(M) = C$$

$$DK(M) = M$$

Keamanan sistem yang digunakan kemudian tidak bergantung kepada pengetahuan algoritma yang digunakan, melainkan bergantung kepada kunci yang digunakan. Artinya, algoritma dapat diketahui oleh umum atau dipublikasikan. Usaha untuk memecahkan keamanan sistem menjadi usaha untuk memecahkan atau mencari kunci yang digunakan. Usaha mencari kunci sangat bergantung kepada *keyspace* dari kunci *K*. Apabila *keyspace* ini cukup kecil, maka cara *brute force* atau mencoba semua kunci dapat dilakukan. Akan tetapi apabila *keyspace* dari kunci yang digunakan cukup besar, maka usaha untuk mencoba semua kombinasi kunci menjadi tidak realistis. *Keyspace* dari *DES*, misalnya, memiliki 56-bit. Untuk mencoba semua kombinasi yang ada diperlukan kombinasi.

Public-key cryptography lawan symmetric cryptography

Perbedaan prinsip dan penggunaan *public-key cryptography* dan *symmetric cryptography* membutuhkan diskusi tersendiri. Pada *symmetric cryptography*, satu kunci yang sama digunakan untuk melakukan enkripsi dan dekripsi. Pada sistem *public-key cryptography*, enkripsi dan dekripsi menggunakan kunci yang berbeda. Sejak dikembangkannya *public-key cryptography*, selalu timbul pertanyaan mana yang lebih baik. Para pakar kriptografi mengatakan bahwa keduanya tidak dapat dibandingkan karena mereka memecahkan masalah dalam domain yang berbeda. *Symmetric cryptography* merupakan hal yang terbaik untuk mengenkripsi data. Kecepatannya dan keamanan akan *choosenciphertext attack* merupakan kelebihanannya. Sementara itu *public-key cryptography* dapat melakukan hal-hal lain lebih baik daripada *symmetric cryptography*, misalnya dalam hal key management.

Data Encryption Standard (DES)

DES, atau juga dikenal sebagai *Data Encryption Algorithm* (DEA) oleh ANSI dan DEA-1 oleh ISO, merupakan algoritma kriptografi simetris yang paling umum digunakan saat ini. Sejarahnya DES dimulai dari permintaan pemerintah Amerika Serikat untuk memasukkan proposal enkripsi. Horst Feistel merupakan salah satu periset yang mula-mula mengembangkan DES ketika bekerja di IBM Watson Laboratory di Yorktown Heights, New York. DES baru secara resmi

digunakan oleh pemerintah Amerika Serikat (diadopsi oleh National Bureau of Standards) di tahun 1977. Ia dikenal sebagai Federal Information Processing Standard 46 (FIPS PUB46). Aplikasi yang menggunakan DES antara lain: enkripsi dari password di sistem UNIX dan berbagai aplikasi di bidang perbankan

Memecahkan DES

DES merupakan block cipher yang beroperasi dengan menggunakan blok berukuran 64-bit dan kunci berukuran 56-bit. Brute force attack dengan mencoba segala kombinasi membutuhkan 256 kombinasi atau sekitar 7×10^{17} atau 70 juta milyar kombinasi. DES dengan penggunaan yang biasa (*cookbook mode*) dengan panjang kunci 56 bit saat ini sudah dapat dianggap tidak aman karena sudah berhasil dipecahkan dengan metoda coba-coba (*brute force attack*).

Ada berbagai group yang mencoba memecahkan DES dengan berbagai cara. Salah satu group yang bernama *distributed.net* menggunakan teknologi Internet untuk memecahkan problem ini menjadi sub-problem yang kecil (dalam ukuran blok). Pengguna dapat menjalankan sebuah program yang khusus dikembangkan oleh tim ini untuk mengambil beberapa blok, via Internet, kemudian memecahkannya di computer pribadinya. Program yang disediakan meliputi berbagai operating system seperti Windows, DOS, berbagai variasi Unix, Macintosh. Blok yang sudah diproses dikembalikan ke *distributed.net* via Internet. Dengan cara ini puluhan

ribu orang, termasuk penulis, membantu memecahkan DES. Mekanisme ini dapat memecahkan DES dalam waktu 30 hari.

Sebuah group lain yang disebut *Electronic Frontier Foundation* (EFF) membuat sebuah komputer yang dilengkapi dengan *Integrated Circuit chip DES cracker*. Dengan mesin seharga US\$50.000 ini mereka dapat memecahkan DES 56-bit dalam waktu rata-rata empat (4) sampai lima (5) hari. DES cracker yang mereka kembangkan dapat melakukan eksplorasi keseluruhan dari 56-bit *keyspace* dalam waktu sembilan (9) hari.

Dikarenakan 56-bit memiliki 216 (atau 65536) *keyspace* dibandingkan DES dengan 40-bit, maka untuk memecahkan DES 40-bit hanya dibutuhkan waktu sekitar 12 detik. Dikarenakan hukum average, waktu rata-rata untuk memecahkan DES 40-bit adalah 6 detik. Perlu diingat bahwa group seperti EFF merupakan group kecil dengan budget yang terbatas. Dapat dibayangkan sistem yang dimiliki oleh *National Security Agency* (NSA) dari pemerintah Amerika Serikat.

Hash function - integrity checking

Salah satu cara untuk menguji integritas sebuah data adalah dengan memberikan "checksum" atau tanda bahwa data tersebut tidak berubah. Cara yang paling mudah dilakukan adalah dengan menjumlahkan karakter-karakter atau data-data yang ada sehingga apabila terjadi perubahan, hasil penjumlahan menjadi berbeda. Cara ini tentunya mudah dipecahkan

dengan menggunakan kombinasi data yang berbeda akan tetapi menghasilkan hasil penjumlahan yang sama.

Pada sistem digital biasanya ada beberapa mekanisme pengujian integritas seperti antara lain:

- parity checking
- checksum
- hash function

Hash function merupakan fungsi yang bersifat satu arah dimana jika kita masukkan data, maka dia akan menghasilkan sebuah "checksum" atau "fingerprint" dari data tersebut. Ada beberapa hash function yang umum digunakan, antara lain:

- MD5
- SHA

Gambar-2. Penggunaan fungsi hash yang menghasilkan fingerprint

Sumber : Raharjo (2002)

Fungsi hash ini biasanya digabungkan dengan enkripsi untuk menjaga integritas. Sebagai contoh, dalam pengiriman email yang tidak rahasia (dapat dibaca orang) akan tetapi ingin dijaga integritasnya, isi (*body*) dari email dapat dilewatkan ke fungsi hash sehingga menghasilkan fingerprint dari isi email tersebut. Keluaran dari hash ini dapat disertakan dalam email. Ketika email diterima, penerima juga menjalankan fungsi hash terhadap isi email dan kemudian membandingkannya dengan hash

yang dikirim. Jika email diubah di tengah jalan, maka kedua hash tersebut berbeda.

Untuk lebih meningkatkan keamanan, hasil dari hash juga dapat dienkripsi sehingga hanya penerima saja yang dapat membuka hasil dari hash tersebut. Atau dapat juga hasil hash dienkripsi dengan kunci privat pengirim sehingga oleh penerima dapat dibuka dengan kunci publik pengirim dan diyakinkan bahwa integritas dari isi terjamin serta pengirim betul-betul berasal dari pemilik kunci publik tersebut. Inilah yang sering disebut digital signature dalam email.

SIMPULAN

Salah satu strategi pengamanan system informasi yang dapat digunakan adalah Enkripsi (*encryption*) sebuah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*). Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Elemen dari sebuah enkripsi data terdiri dari Algoritma dari Enkripsi dan Dekripsi. Algoritma dari enkripsi merupakan fungsi-fungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi. Algoritma yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika. Unsur lain dalam enkripsi adalah Kunci yang digunakan dan panjangnya kunci. Kekuatan dari penyandian bergantung kepada kunci yang digunakan. Plaintext. Plaintext

adalah pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca atau dalam bentuk aslinya.

DAFTAR PUSTAKA

- Ali, Amir, 2007, *Kemanan dan kerahasiaan data dalam system computer*, Materi Kuliah, STMIK Handayani Makassar.
- Baroto, Wisnu. 2003 *Memahami Dasar – Dasar Firewall Keluaran Check Point Versi Next Generation*. Penerbit PT. Elex Media Komputindo
- B.U, Donny. Juni 2004 *4-M Pembangkit Aksi Deface*, (Download), <http://www.familycode.com>
- B.U, Donny. Juli 2004 *Sebab Akibat dan Kepastian Hukum* Majalah Warta Ekonomi, edisi No.15, tahun XVI, 28 Juli 2004
- B.U, Donny. Oktober 2001 *Hacker, Riwayatmu Kini.....* .Majalah Neotek, Vol.II - No. 1
- Kristanto, Andi. (2003). *Perancangan Sistem Informasi dan Aplikasinya*, Gava Media, Yogyakarta.
- Phayzer, Juli 2003 *Konsep Dasar TCP/IP*, (Online), tersedia : <http://k-elektronik.org>

Rahardjo, Budi. 2002 *Keamanan Sistem Informasi Berbasis Internet*. Versi 5.1 Penerbit PT Insan Infonesia - Bandung & PT INDOCISC - Jakarta

Sudirman, Ivan. 2003 *TCP/IP dan Praktek Sekuriti Jaringan*. Tersedia : Kuliah Umum Ilmukomputer.Com

Thaief, Ilham (2008), Standar Sistem Manajemen Keamanan Informasi, Jurnal : *JETC Jurnal elektronika telekomunikasi &*

Computer, Fakultas Teknik Universitas Negeri Makassar.

Visual Basic Community site (2007). *Applikasi keamanan data* (on line), Tersedia : <http://www.vbBeGo.com>, diakses [12 Februari 2008].