ANALISA KRIPTOGRAFI UNTUK KEAMANAN DALAM MANAJEMEN SISTEM TERDISTRIBUSI PERUSAHAAN

Diana Laily Fithri
Program Studi Sistem Informasi Universitas Muria Kudus
diana.laily@umk.ac.id

ABSTRACT

Management of distributed system is using cryptography security. Cryptography in Greek means hidden. In this modern era, cryptography is considered as a branch of mathematics and computer applied in management of distributed system as well as related theories and information. Cryptography nowadays is used by many people such as in a system of ATM card security, passwords of computer, electronic trading, and so forth depend on cryptography. Therefore, in this modern era crytography extremely needs more knowledge and application of modern cryptography challenge, particularly in a field of security management of distributed system.

Keywords: *cryptography, cryptanalysis, cryptology, encryption, decryption*

ABSTRAK

Manajemen dengan sistem terdistribusi menggunakan konsep keamanan kriptografi. Kriptografi dalam bahasa Yunani berarti tersembunyi. Pada zaman modern ini, kriptografi dianggap sebagai cabang dari ilmu matematika dan ilmu komputer diterapkan dalam manajemen dengan sistem terdistribusi, serta teori terkait erat dengan information. Kriptografi saat ini banyak digunakan dalam masyarakat maju, misalnya dalam sistem keamanan kartu ATM, password di komputer, perdagangan elektronik, dan lain-lain yang semua tergantung pada kriptografi. Oleh karena itu, di zaman modern ini masih membutuhkan lebih banyak pengetahuan yang mendalam dan pengenalan penerapan tantangan kriptografi modern, khususnya di bidang manajemen keamanan sistem terdistribusi.

Kata kunci: kriptografi, kriptanalisis, kriptologi, enkripsi, dekripsi

Pendahuluan

Keamanan dan kerahasian data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahanan, sistem perbankan, sistem bandara udara dan sistem-sistem yang lain setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep open system-nya sehingga siapapun, di mananapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka diperlukan beberapa upaya pengamanan guna membuat pesan, data, atau informasi agar tidak dapat diakses atau gagal pada saat pembacaan.

Saat ini telah banyak metode pengamanan pesan, data, atau informasi yang dikembangkan oleh perusahaan ataupun perorangan. Pengamanan tersebut bisa meliputi pengamanan fisik maupun pengamanan secara digital. Dengan adanya sistem keamanan tersebut, pengguna akan lebih terjamin saat berinteraksi ataupun bertukar data melalui jaringan.

Sejarah kriptografi

Kriptografi merupakan teknik penyembunyian informasi rahasia, biasanya berupa teknik matematis, coding, maupun cara lainnya dengan tujuan agar pesan yang disimpan atau ditransmisikan hanya bisa diketahui oleh pihak yang berkepentingan saja.

Sebenarnya kriptografi sudah berkembang sejak 4000 tahun yang lalu, tepatnya di Mesir yaitu berupa Hieroglyph. Semua yang membahas sejarah kriptografi ini dapat secara lengkap kita pelajari dalam buku karangan David Kahn yang berjudul The Codebreakers.Teknik penyembunyian pesan pada zaman dahulu kebanyakan menggunakan metode enkripsi dengan paper and pencil, masih disebut kriptografi klasik. Berbeda dengan kriptografi modern yang sekarang, dimana enkripsi menggunakan sumber daya komputasi yang semakin berkembang.

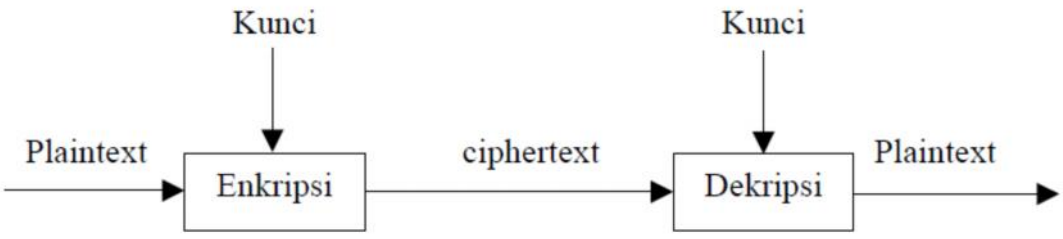
Sejarah kriptografi zaman dulu pun pernah menyebutkan tentang scytale, merupakan penyandian dengan menggunakan daun papyrus yang dililitkan pada batang pohon yang mempunyai diameter tertentu. Pesan (plaintext) ditulis secara horisontal pada daun papyrus, selanjutnya setelah daun dilepas, maka yang akan terlihat pada daun papyrus yang panjang itu hanyalah rangkaian huruf yang tak berarti/tidak membentuk kata (ciphertext). Scytale ini dulu digunakan oleh tentara Sparta di Yunani.

Ada juga Caesar cipher yang digunakan oleh raja Yunani Kuno, Julius Caesar. Metode enkripsi ini dilakukan dengan menggeserkan suatu karakter. Misalkan dengan kunci A = C, kita akan menyandikan KRIPTOGRAFI, maka cipherteksnya NULSWRJUDIL. Caesar cipher ini merupakan metode paling sederhana dalam enkripsi pesan dengan 26 kemungkinan kunci.

Enkripsi dan Deskripsi

Enkripsi adalah hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirim agar terjaga kerahasiaannya.Pesan asli disebut plaintext, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bias diartikan dengan cipher atau kode. Dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.

Keamanan dari kriptografi modern didapat dengan merahasiakan kunci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri. Kunci memiliki fungsi yang sama dengan password. Jika keseluruhan keamanan algoritma tergantung pada kunci yang dipakai, maka algoritma ini bisa dipublikasikan dan dianalisa orang lain.



Gambar 1 : Proses kriptografi enkripsi dan deskripsi

Algoritma Kunci Simetris

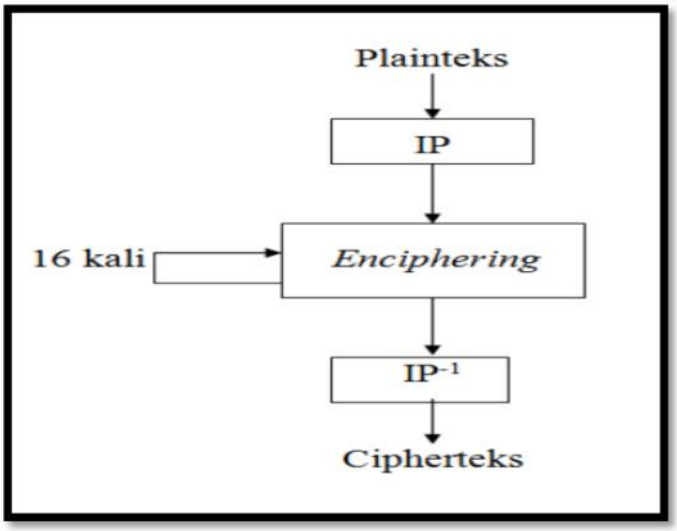
Algoritma kunci simetris adalah algoritma kriptografi yang memiliki kunci yang sama untuk proses enkripsi dan dekripsinya. Kunci tersebut merupakan satu-satunya jalan untuk proses dekripsi (kecuali mencoba membobol algoritma tersebut), sehingga kerahasiaan kunci menjadi nomer satu.

Algoritma DES (*Data Encryption Standard*)

DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. *DES* beroperasi pada ukuran blok 64 bit. *DES* mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*internal key*) atau upa-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit.

Skema global dari algoritma *DES* adalah sebagai berikut :

a. Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).
b. Hasil permutasi awal kemudian di-*enciphering*- sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
c. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan *invers initial permutation* atau IP-1) menjadi blok cipherteks.



Gambar 2 : Hasil enchipering Kriptografi pada DES

Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah *K*1, *K*2, …,*K*16, maka pada proses dekripsi urutan kunci yang digunakan adalah *K*16, *K*15, …, *K*1.

DES sudah diimplementasikan dalam bentuk perangkat keras. Dalam bentuk perangkat keras, DES diimplementasikan didalam *chip*. Setiap detik *chip* ini dapat mengenkripsikan16,8 juta blok (atau1 gigabit per detik). Implementasi DES kedalam perangkat lunak dapat melakukan enkripsi 32.000 blokper detik (pada computer *mainframe* IBM 3090).

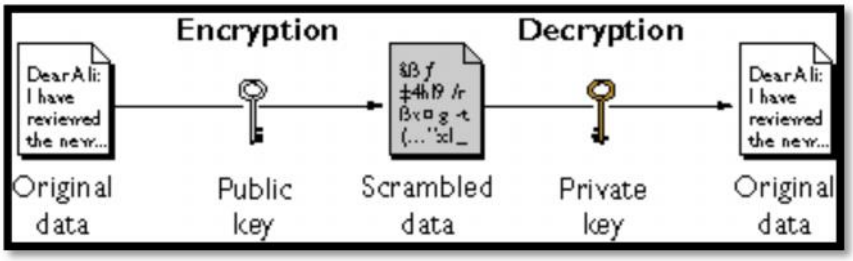
***Advanced Encryption Standart* (AES)**

AES adalah *Advanced Encryption Standard.* AES adalah block cipher yang akan menggantikan DES tetapi diantisipasi bahwa Triple DES tetap akan menjadi algoritma yang disetujui untuk penggunaan pemerintah USA. Pada Januari 1997 inisiatif AES diumumkan dan pada September 1997 publik diundang untuk mengajukan proposal block cipheryang cocok sebagai kandidat untuk AES. Pada tahun 1999 NIST mengumumkan lima kandidat finalis yaitu MARS, RC6, Rijndael, Serpent, dan Twofish. Algoritma AES dipilih pada Oktober 2001 dan standarnya dipublish pada November 2002. AES mendukung ukuran kunci 128 bit, 192 bit, dan 256 bit,

berbeda dengan kunci 56-bit yang ditawarkan DES.

Kriptografi kunci Asimetris

Algoritma sandi dapat dikelompokkan menjadi 3 kategori yaitu : sistem sandi simetris, sistem sandi asimetris dan sistem sandi hashing. Masing-masing sistem sandi ini memiliki cara yang berbeda dalam metode penyandiannya. Sistem sandi asimetris atau dikenal juga sebagai sistem sandi kunci publik adalah sistem sandi yang metode menyandi dan membuka sandinya menggunakan kunci yang berbeda. Tidak seperti sistem sandi simetris, sistem sandi ini relatif masih baru.Algoritma sandi jenis ini yang telah terkenal diantaranya RSA (*Rivest-Shamir-Adleman*), ElGamal, dan Diffie-Hellman.Sistem ini memiliki sepasang kunci yang disebut kunci publik yaitu kunci yang didistribusikan secara umum dan kunci privat yaitu kunci yang dirahasiakan yang hanya dimiliki oleh pihak yang berhak. Umumnya kunci publik digunakan untuk menyandi dan kunci privat digunakan untuk membuka sandi. Sistem sandi asimetrik bekerja lebih lambat dari sistem sandi simetris, sehingga sistem sandi ini lebih sering digunakan untuk menyandi data dengan ukuran bit yang kecil. Sistem sandi ini sering pula digunakan untuk mendistribusikan kunci sistem sandi simetris. Penggunaan lain sistem sandi asimetris adalah dalam tandatangan digital. Tandatangan digital seperti halnya tandatangan biasa digunakan untuk membuktikan keaslian dari suatu dokumen yang dikirimkan. Kunci privat digunakan untuk menandatangani, sedangkan kunci publik digunakan untuk membuktikan keaslian tandatangan itu. Karena kunci publik didistribusikan secara umum, kita mempunyai permasalahan yang berbeda dengan sistem sandi simetris. Permasalahan utamanya adalah apakah kunci publik-nya berada ditangan yang tepat. Untuk mengatasi masalah tersebut maka Infrastruktur Kunci Publik (PKI) mencoba memberikan pemecahannya. Namun karena masih dalam tahap pengembangan, PKI tidak memberikan jaminan. Masih membutuhkan waktu lama untuk dapat menerima solusi PKI ini. System kriptografi kunci-simetri secara tipikal menggunakan enkripsi dan dekripsi yang sama meskipun pesan ini memiliki kunci berbeda satu sama lain. Secara signifikan, ketidakuntungan dari siem ini adalah manajemen kunci yang diperlukan untuk keamanan. Setiap pasang komunikasi yang berjarak jauh harus memiliki kunci yang berbeda. Setiap kunci yang bertambah akan menambahkan jarak dari anggota jaringan yang mana akan membutuhkan menajemen kunci yang lebih teliti lagi agar terjamin keamanannya. Hal yang membuat sulit adalah kesulitan dalam menempatkan kunci rahasia diantara kelompok yang berkomunikasi. Algoritma kunci publik ini biasanya berdasarkan kompleksitas komputasional dari masalah yang “sulit”, biasanya dari teori angka. Sebagai contoh, kekerasan dari RSA biasanya berhubungan dengan masalah faktorisasi integer, ketika Diffie-Hellman dan DSA berkaitan dengan masalah logaritma doskrit. Lebih jauh lagi, kriptografi kurva cekung telah berkembang dari msalah keamaanan yang ada. Karena kesulitan dari masalah tersebut, algoritma kunci-publik termasuk operasi modular seperti perkalian dan eksponensial yang mana hal tersebut secara komputasi lebih mahal daripada teknik lain yang digunakan oleh chipertext, terutama yang menggunakan kunci spesifik. Hasilnya, system criptografi kunci-publik merupakan kriptosistem hibrid secara umum, yang mana algoritma kunci-simetrik kualitas tinggi digunakan sebagai pesan tersebut. Persamaannya, skema tanda tangan hibrid lebih sering digunakan, yang mana fungsi kriptografi diperhitungkan dan hasilnya akan berlaku secara digital.



Gambar 3 :Proses Enkripsi ke Deskripsi

Kripnatalis

Tujuan dari kriptanalisis ini adalah untuk menemukan beberapa kelemahan atau ketidakamanan dalam skema kriptografi, untuk itu dilakukan izin untuk subversi atau penghindaran. Kriptanalisis mungkin dianggap remeh bagi beberapa penyerang, dikarenakan system yang mudah ditumbangkan. Dalam praktik modernnya, algoritma kriptografi dan protocol harus dicek ulang secara teliti dan dites untuk memberikan jaminan system keamanan. Jika kriptanalisis murni menggunakan kelemahan dalam algoritma, kriptosystem yang lain berdasarkan penggunaan *actual* dari algoritma dalam alat yang real dan disebut sebagai serangan sisi samping. Jika seorang kriptoanalis memiliki akses untuk memasukkan waktu yang diperlukan untuk enkripsi pesan kesalahan dari masukan sandi lewat atau karakter PIN, ia akan dapat melakuakan serangan waktu untuk membongkar chipertext yang tahan terhadap analis sekalipun. Seorang penyerang mungkin juga belajar pola dan ukuran pesan untuk mendapatkan informasi yang berharga.

Fungsi Hash

One-way function adalah fungsi matematika yang secara signifikan mudah untuk dihitung pada satu arah (arah maju) daripada dengan arah sebaliknya (inverse). Dimungkinkan, sebagai contoh, untuk menghitung fungsi dengan arah maju pada beberapa detik namun untuk menghitung dapat memakan waktu berbulan-bulan atau bertahun-tahun, jika semua dimungkinkan. *Trapdoor oneway function* adalah fungsi satu arah dimana arah inversnya mudah diberikan sebuah informasi (trapdoor), tetapi sulit untuk melakukan hal sebaliknya. Public-key cryptosystems berdasar pada (dianggap) trapdoor one-way functions. Kunci public memberikan informasi tentang instans tertentu dari fungsi, kunci privat memberikan informasi tentang trapdoor. Siapapun yang mengetahui trapdoor dapat menghitung fungsi dengan mudah dalam dua arah, tetapi siapapun yang tidak memiliki trapdoor hanya dapat menjalankan fungsidengan mudah pada arah maju. Arah maju digunakan untuk enkripsi dan verifikasi tandatangan,arah invers digunakan untuk dekripsi dan pembuatan tandatangan. Fungsi hash adalah fungsi yang memproduksi output dengan panjang tetap dari input yang berukuran variabel. Output dari fungsi hash disebut dengan message digest. Fungsi hash memiliki karakteristik fungsi satu arah karena file asli tidak dapat dibuat dari message digest.

Jenis penyerangan pada kriptografi

a. *Ciphertext-only attack*. Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
b. *Known-plaintext attack*. Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan-pesan tersebut.
c. *Chosen-plaintext attack*. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.
d. *Adaptive-chosen-plaintext attack*. Penyerangan tipe ini merupakan suatu kasus khusus chosen-plaintext attack.

Cryptanalyst tidak hanya dapat memilih plaintext yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya. Dalam chosen-plaintext attack, cryptanalyst mungkin hanya dapat memiliki plaintext dalam suatu blok besar untuk dienkripsi; dalam adaptive-chosen-plaintext attack ini ia dapat memilih blok plaintext yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, proses ini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.

e. *Chosen-ciphertext attack*. Pada tipe ini, cryptanalyst dapat memilih ciphertext yang berbeda untuk didekripsi dan memiliki akses atas plaintext yang didekripsi.
f. *Chosen-key attack*. Cryptanalyst pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci-kunci yang berbeda.
g. *Rubber-hose cryptanalysis*. Pada tipe penyerangan ini, cryptanalyst mengancam, memeras, atau bahkan memaksa seseorang hingga mereka memberikan kuncinya.

Analisis

Ada berbagai macam definisi tentang manajemen system terdistribusi dalam sebuah perusahaan. Manajemen system terdistribusi adalah Dalam kaitannya dengan Teknologi Informasi dalam manajemen system terdistribusi, sampai saat ini belum ada acuan yang jelas berapa banyak jumlah tenaga kerja TI yang dipekerjakan, malahan sebagian besar perusahaan di Indonesia tidak memilikidivisi khusus untuk TI. Melihat dari lingkup perusahaan, sumber dayanya baik sumber daya manusia maupun infrastruktur TI dan biaya, ada beberapa aplikasi kriptografi yang mungkin diterapkan dalam lingkungan Perusahaan. Untuk perusahaan yang telah memiliki divisi TI sendiri, penerapan aplikasi kriptografi ini akan lebih murah dan mudah.

Aplikasi-aplikasi kriptografi yang dapat diterapkan antara lain enkripsi pada password, file, dan email. Pengguna diberikan ID dan password untuk mengakses sistem yang ada. Password dienkripsi untuk mencegah terjadinya akses illegal terhadap sistem misalnya pencurian data-data penting olehmereka yang tidak berhak.Demikian juga enkripsi pada file-file penting dapat dilakukan (misalnyafile yang berisi data keuangan).

Metode enkripsi yang digunakan dapat berbentuk enkripsi kunci simetris,misalnya menggunakan algoritma DES, RSA, dll. Untuk mendapatkan algoritma enkripisi ini tidak dibutuhkan biaya karena telah dipublikasikan secara umum. Biaya yang dibutuhkan hanyalah biayapengembangan dan biasanya biaya ini tidak terlalu besar jika pengembangannya dilakukan sendiri oleh divisi TI yang dimiliki manajemen perusahaan Jika dibutuhkan mekanisme enkripsi password lainyang lebih aman sesuai dengan kebutuhan keamanandata yang lebih tinggi dalam perusahaan dapat digunakan mekanisme *One Time Password* untuk menggantikan mekanisme password statis. Keunggulan dari mekanisme *One Time Password* dimana password hanya digunakan satu kali saja setiap pengguna akan *log on* ke dalam sistem ini adalah walaupun penyerang berhasil mendapatkan password namun ia tidak dapat menggunakannya lagi untuk melakukan akses terhadap sistem. Teknik enkripsi yang dapat digunakan untuk mekanisme ini adalah teknik-teknik enkripsi simetris/kunci rahasia.

Banyak algoritma yang dapat digunakan untuk mengenkripsi password misalnya DES, AES,Blowfish, RC6, dll.Sekali lagi yang dibutuhkan disini adalah sumber daya manusia yang mampu untuk mengimplementasikan algoritma ini. Aplikasi kriptografi lain yang dapat diimplementasikan dalam system terdistribusi adalah enkripsi email. Enkripsi email dibutuhkan untuk melindungi surat-surat penting perusahaan yang akan dikirim dari maupun keluar perusahaan. Misalnya saja pengiriman data-data laporan rugi laba perusahaan kepada pihak penagih pajak maupun pengiriman surat-surat berharga lainnya. Untuk mengimplementasikan enkripsi email ini

perusahaan harus sudah terkoneksi Internet. Aplikasi enkripsi email yang dapat diadopsi misalnya *PrettyGood Privacy* (PGP) yang dapat diperoleh secaragratis.

Simpulan

Kriptografi merupakan salah satu dari media komunikasi dan informasi kuno yang masih dimanfaatkan hingga saat ini.Kriptografi di Indonesia disebut persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi dari pihak-pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan.Sedangkan ilmu persandiannya disebut kriptologi yaitu ilmu yang mempelajari tentang bagaimana tehnik melindungi data dan informasi tersebut beserta seluruh ikutannya.Pengguna diberikan ID dan password untuk mengakses sistem yang ada. Password dienkripsi untuk mencegah terjadinya akses illegal terhadap sistem misalnya pencurian data-data penting oleh mereka yang tidak berhak. Demikian juga enkripsi pada file-file penting dapat dilakukan (misalnya file yang berisi data keuangan). Metode enkripsi yang digunakan dapat berbentuk enkripsi kunci simetris, misalnya menggunakan algoritma DES, RSA, dll.Untuk mendapatkan algoritma enkripisi ini tidak dibutuhkan biaya karena telah dipublikasikan secara umum. Oleh karena itu, dapat disimpulkan bahwa kriptografi masih merupakan sistem yang efektif dalam hal keamanan dan proteksi serta dapat digunakan secara luas di berbagai bidang usaha dan teknologi.

Daftar Pustaka

Mollin, Richard, “An Introduction to Cryptography, Second Edition (Discrete Mathematics and Its Applications)”, Chapman &Hall/CRC, 2006, pp.9-13.

Mukodim, Didin. 2002. Teknik Pengamanan Data dengan RSA. *Proceedings, Komputer dan*

Sistem Intelijen (KOMMIT 2002). Jakarta: Universitas Gunadarma.

Riyanto, M. Zaki., & Ardhi Ardian. 2008. *Kriptografi Kunci Publik: Sandi RSA*.

http://sandi.math.web.id

Setiawan, Deris. 2002. *Sistem Keamanan Komputer*. Jakarta: PT Elex Media Komputindo