ANALISIS KEAMANAN KRIPTOSISTEM KUNCI PUBLIK BERDASARKAN MATRIKS INVERS TERGENERALISASI PADA Z_2

TUGAS AKHIR

Untuk Memenuhi Sebagian Persyaratan Memperoleh Gelar Sarjana Sains

AYU FITRIA RAHMI
NIM 72983

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS NEGERI PADANG

2011

PERSETUJUAN TUGAS AKHIR

Judul	: Analisis Keamanan Kriptosistem Kunci Publik Berdasarkan Matriks Invers Tergeneralisasi Pada Z_2
Nama	: Ayu Fitria Rahmi
NIM	: 72983
Program Studi	: Matematika
Jurusan	: Matematika
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

Padang, Agustus 2011

Disetujui oleh :

Pembimbing I	Pembimbing II
Dra. Arnellis, M.Si	Drs. Yusmet Rizal, M.Si
NIP 19610502 198703 2 002	NIP 19680121 199303 1 011

PENGESAHAN LULUS UJIAN TUGAS AKHIR

Nama : Ayu Fitria Rahmi

NIM : 72983

Program Studi : Matematika

Jurusan : Matematika

Fakultas : MIPA

dengan judul :

ANALISIS KEAMANAN KRIPTOSISTEM KUNCI PUBLIK BERDASARKAN MATRIKS INVERS TERGENERALISASI PADA Z_2

Dinyatakan lulus setelah dipertahankan di depan Tim Penguji Tugas Akhir
Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Negeri Padang

Padang, Agustus 2011

Tim Penguji

	Nama	Tanda Tangan
Ketua	: Dra. Arnellis, M.Si	_____
Sekretaris	: Drs. Yusmet Rizal, M.Si	_____
Anggota	: Dra. Hj. Minora Longgom Nst, M.Pd	_____
Anggota	: Dra. Dewi Murni, M.Si	_____
Anggota	: Muhammad Subhan, S.Si, M.Si	_____

ABSTRAK

Ayu Fitria Rahmi : Analisis Keamanan Kriptosistem Kunci Publik Berdasarkan Matriks Invers Tergeneralisasi pada Z_2.

Keamanan suatu informasi perlu dijamin sehingga informasi tersebut tidak diketahui oleh pihak lain. Untuk menjaga keamanan suatu informasi digunakan berbagai macam teknik salah satunya adalah dengan menyandikan pesan yang dikenal dengan ilmu kriptografi. Keterbatasan keamanan menggunakan kriptosistem kunci publik yang lain dalam pengkajian proses koreksi kesalahan kode maka dikembangkan kriptosistem kunci publik menggunakan pendekatan matriks invers tergeneralisasi pada Z_2. Sehingga yang menjadi permasalahan dalam penelitian ini adalah bagaimana langkah menganalisis keamanan kriptosistem kunci publik berdasarkan matriks invers tergeneralisasi pada Z_2. Penelitian ini bertujuan untuk menganalisis keamanan kriptosistem kunci publik mengggunakan matriks invers tergeneralisasi pada Z_2.

Jenis penelitian adalah penelitian dasar dengan menganalisis teori-teori yang relevan berdasarkan studi kepustakaan. Langkah-langkah yang peneliti lakukan adalah menentukan pembentukan kunci, menentukan proses enkripsi dan deskripsi data serta menentukan langkah-langkah melindungi pesan yang dikirimkan.

Hasil yang diperoleh dalam penelitian ini adalah proses terbentuknya kunci G, H^-, dan H^-H dengan matriks invers tergeneralisasi pada Z_2. Setelah terbentuknya kunci dilaksanakan adalah proses enkripsi dan deskripsi dengan adanya penambahan kesalahan **E**. Kemudian ditemukan langkah yang dilakukan untuk melindungi pesan yang dikirimkan adalah pemilihan matriks paritas H untuk mendapatkan kunci rahasia $R = H^-H$, pemilihan sebarang vektor **e** untuk menemukan bentuk kesalahan $E = e(H^-)^T$, serta pemilihan sebarang vektor kesalahan **E** untuk mengoreksi kesalahan kode.

Kata kunci : *deskripsi, enkripsi, matriks invers tergeneralisasi.*

KATA PENGANTAR

Alhamdulillah, segala puji syukur peneliti ucapkan ke hadirat Allah Swt, atas rahmat dan hidayah-Nya yang telah diberikan kepada peneliti berupa ketabahan, ketekunan dan keuletan, sehingga peneliti dapat menyelesaikan Tugas Akhir ini yang diberi judul: ***"Analisis Keamanan Kriptosistem Kunci Publik Berdasarkan Matriks Invers Tergeneralisasi pada Z_2".***

Penulisan Tugas Akhir ini bertujuan untuk memenuhi sebagian dari persyaratan memperoleh gelar Sarjana Sains (S.Si) pada Program Studi Matematika Jurusan Matematika FMIPA Universitas Negeri Padang.

Pada penyelesaian Tugas Akhir ini, peneliti banyak mengalami kesulitan, terutama disebabkan oleh kurangnya ilmu pengetahuan. Namun berkat bimbingan, arahan, dan dukungan dari berbagai pihak akhirnya Tugas Akhir ini dapat diselesaikan. Atas bimbingan, arahan dan dukungannya peneliti menyampaikan rasa terima kasih yang sebesar-besarnya kepada :

1. Ibu Dra. Arnellis, M. Si, Dosen Pembimbing I dan Penasehat Akademis.
2. Bapak Drs. Yusmet Rizal, M. Si, Dosen Pembimbing II.
3. Bapak Muhammad Subhan, S. Si, M. Si, Dosen Penguji Tugas Akhir dan Ketua Program Studi Matematika FMIPA UNP.

4. Ibu Dra. Hj. Minora Longgom Nst, M. Pd dan Ibu Dra. Dewi Murni, M. Si, Dosen Penguji Tugas Akhir.

5. Bapak dan Ibu staf Pengajar dan Labor Jurusan Matematika FMIPA UNP.

6. Seluruh rekan Mahasiswa Jurusan Matematika khususnya angkatan 2006 FMIPA UNP.

7. Semua pihak yang telah rela memberikan bantuan moril dan materil sehingga sampai terlaksananya penyusunan skripsi ini.

Semoga bimbingan, dorongan serta pengorbanan yang telah diberikan mendapat ridho dari Allah SWT.

Peneliti menyadari Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, saran dan kritikan yang membangun sangat diharapkan demi kesempurnaan Tugas Akhir ini. Semoga Tugas Akhir ini bermanfaat bagi Jurusan Matematika serta para pembaca pada umumnya.

Padang, Agustus 2011

Peneliti

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

1.1. Latar Belakang

Informasi memiliki arti yang sangat penting bagi kehidupan manusia karena tanpa informasi hampir semuanya tidak dapat dilakukan dengan baik. Suatu informasi atau dokumen pada saat sekarang ini tidak hanya dalam bentuk konvensional di atas kertas, tetapi informasi sudah dapat disimpan sebagai arsip elektronis di dalam perangkat komputer.

Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat sangat berguna bagi sebuah organisasi, baik organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan maupun individu. Hal ini disebabkan oleh perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Apalagi informasi juga lebih mudah dengan adanya jaringan komputer seperti LAN (*Local Area Network*) dan internet, yang semuanya menyediakan informasi secara cepat dan akurat.

Kemajuan sistem informasi memberikan banyak kemudahan bagi kehidupan manusia. Namun ada pula dampak negatifnya seperti adanya pencurian, penyadapan saluran informasi, pemerasan. Informasi dapat berpindah ke pihak lain akan menimbulkan kerugian bagi pemilik informasi. Dalam penyimpanan dokumen atau penyampaian suatu informasi diperlukan suatu sistem keamanan.

Namun masalah keamanan sering kurang mendapat perhatian dari pengelola sistem informasi. Malah masalah keamanan kadang diabaikan atau berada di urutan terakhir. Aspek keamanan yang perlu dijamin dalam penyampaian informasi adalah kerahasiaan, dimana informasi tersebut tidak boleh diketahui oleh pihak lain yang tidak berkepentingan. Selain itu masalah keamanan yang perlu diperhatikan adalah pesan yang dikirim harus sesuai dengan yang asli dan benar-benar diterima dari pengirim bukan dari pihak ketiga yang menyamar sebagai pengirim pesan.

Untuk menjaga aspek keamanan dari informasi tersebut maka dikembangkanlah berbagai macam teknik. Salah satu teknik yang dipakai adalah dengan cara menyandikan pesan tersebut ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Ilmu yang mempelajari penyandian data tersebut adalah kriptografi. Dalam kriptografi pesan yang asli atau disebut juga *plaintext* akan disandikan ke bentuk lain melalui proses enkripsi. Bentuk pesan yang tersandikan tersebut adalah *ciphertext*. Pesan yang telah disandikan tersebut oleh penerima pesan akan ditransformasikan kembali menjadi *plaintext* semula melalui proses dekripsi.

Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi kriptografi kunci simetri dan kriptografi kunci asimetri. Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi (kriptosistem).

Pada kriptosistem kunci simetri, kunci untuk enkripsi sama dengan kunci dekripsi. Kriptosistem kunci simetri disebut juga kriptografi kunci privat. Contoh

kriptosistem kunci privat adalah *Data Encryption Standard* (DES), *Blowfish*, *Twofish*, *Triple DES, IDEA,* dan *Serpent*. Sedangkan pada kriptosistem kunci asimetri, kunci untuk enkripsi tidak sama dengan kunci untuk dekripsi. Kriptosistem kunci asimetri disebut juga kriptosistem kunci publik, hal ini disebabkan kunci untuk enkripsi dapat diketahui oleh publik. Pada kriptosistem kunci publik, pengirim mengenkripsi pesan dengan menggunakan kunci publik penerima pesan. Hanya penerima pesan yang dapat mendekripsi pesan karena hanya dia yang mengetahui kunci privatnya sendiri. Contoh algoritma kriptosistem kunci publik diantaranya RSA (*Rivert-Shamir-Adelman*), El Gamal, DSA (*Digital Signature Algorithm*), Knapsack, dan sebagainya.

Sistem kunci publik RSA yang ditemukan oleh River,Shamir dan Adleman dikembangkan berdasarkan teori bilangan. Keamanan sistem RSA terletak pada kesulitan pemfaktoran bilangan-bilangan besar. Kelemahan sistem RSA adalah jika pemfaktoran bilangan besar dapat dijadikan faktor-faktor prima maka keamanan tidak terjamin. Algoritma El Gamal yang dikembangkan berdasarkan logaritma diskrit memiliki keterbatasan karena keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit. Sedangkan algoritma Knapsack keamanannya terletak pada sulitnya memecahkan persoalan Knapsack. Knapsack (karung) mempunyai kapasitas terbatas.

Keterbatasan keamanan dari jenis kunci publik RSA, algoritma El Gamal, Knapsack masih kurang dalam pengkajian proses koreksi kesalahan kode (*error correcting code*). Sedangkan pengkajian proses koreksi kesalahan kode (*error correcting code)* sangat dibutuhkan dalam pembentukan kunci. Terutama dalam

proses enkripsi data dimana akan ditambahkan bentuk kesalahan sebagai proses koreksi kesalahan dari *ciphertext*. Ide dasar desain algoritma dalam kriptografi dapat dilakukan dengan teknik matriks invers tergeneralisasi. Teori matriks invers tergeneralisasi telah berkembang sejak awal tahun 1970-an.

Kriptosistem kunci publik yang menggunakan pendekatan matrik invers tergeneralisasi atas bilangan bulat modulo 2 (Z_2) dalam pengembangannya, telah menjadi alternatif baru dalam bidang enkripsi dan deskripsi data. Pemakaian modulo 2 karena operasi yang digunakan adalah operasi logika XOR. Tujuan utama melakukan enkripsi dan deskripsi data adalah untuk menjamin keamanan dari data yang akan dikirimkan. Dengan mengkaji proses koreksi kesalahan kode dengan matriks invers tergeneralisasi pada Z_2 dapat meningkatkan keamanan data atau memperkecil resiko-resiko yang disebabkan oleh enkripsi data. Jika data telah terjamin keamanannya maka akan menyulitkan penyusup mendapatkan kunci rahasia yang akhirnya penyusup sulit mendapatkan *plaintext* dari pesan yang dikirimkan.

Sehingga dengan menganalisis keamanan kriptosistem maka dapat ditunjukkan bahwa matriks invers tergeneralisasi pada Z_2 memberikan alternatif lain pada bidang kriptografi. Untuk itu peneliti tertarik menganalisis keamanan kriptosistem kunci publik berdasarkan matriks invers tergeneralisasi pada Z_2.

1.2. Perumusan Masalah

Berdasarkan latar belakang maka yang menjadi permasalahan dalam penelitian ini adalah : Bagaimana langkah menganalisis keamanan kriptosistem kunci publik berdasarkan matriks invers tergeneralisasi pada Z_2?

1.3. Pendekatan dan Pertanyaan Penelitian

Pendekatan yang digunakan pada penelitian ini adalah studi kepustakaan yaitu mengumpulkan data melalui buku-buku dan jurnal ilmiah yang berhubungan dengan masalah yang akan dibahas. Kemudian akan dilakukan analisis untuk menyelesaikan permasalahan yang diteliti.

Adapun pertanyaan penelitian yang muncul adalah :

1. Bagaimana prosedur pembentukan kunci dengan matriks invers tergeneralisasi pada Z_2?
2. Bagaimana proses enkripsi dan deskripsi data dengan adanya penambahan koreksi kesalahan dalam Z_2 ?
3. Apa saja yang dapat dilakukan untuk melindungi pesan yang dikirimkan?

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk :

1. Mengetahui prosedur pembentukan kunci dengan matriks invers tergeneralisasi pada Z_2.
2. Mengetahui proses enkripsi dan deskripsi data dengan adanya penambahan koreksi kesalahan dalam Z_2 .
3. Mengetahui langkah yang dapat dilakukan untuk melindungi pesan yang dikirimkan.

1.5. Metode Penelitian

Penelitian ini merupakan penelitian dasar. Metode yang digunakan adalah metode deskriptif dengan cara menganalisis teori yang relevan dengan

permasalahan yang akan dibahas dan berlandaskan pada studi kepustakaan. Dalam melakukan penelitian ini, peneliti memulai dengan meninjau permasalan, mengumpulkan dan mengaitkan teori-teori yang diperoleh dengan permasalahan yang dibahas sebagai penunjang untuk menjawab permasalahan.

Langkah-langkah yang peneliti laksanakan dalam penelitian ini adalah mengkaji :

1. Langkah-langkah pembentukan kunci.

   Dalam pembentukan kunci publik dan kunci privat digunakan matriks generator dan matriks invers tergeneralisasi.

2. Proses enkripsi dan deskripsi data dengan adanya penambahan koreksi kesalahan dalam Z_2 .

   Setelah terbentuknya matriks kunci maka dilakukan proses enkripsi data dengan penambahan bentuk kesalahan sebagai proses koreksi kesalahan katakode/*ciphertext*. Dari *ciphertext* yang telah terbentuk dilakukan proses deskripsi menggunakan kunci privat yang dimiliki oleh si penerima pesan.

3. Langkah melindungi pesan yang dikirimkan.

   Ada beberapa kemungkinan untuk melindungi pesan yang dikirimkan. Oleh sebab itu akan dianalisis kemungkinan terbesar sehingga pesan dapat aman dan diterima oleh orang yang dituju.

1.6. Manfaat Penelitian

Adapun manfaat penelitian ini adalah :

1. Menambah wawasan dan ilmu pengetahuan tentang kriptosistem kunci publik.
2. Dapat mengetahui aplikasi Matriks Invers Tergeneralisasi pada kriptosistem.
3. Sebagai bahan masukan untuk pengembangan dan perluasan cakupan penelitian untuk penelitian selanjutnya.

BAB II

TINJAUAN KEPUSTAKAAN

2.1 Bilangan Biner

Sistem bilangan biner atau sistem bilangan basis dua adalah sebuah sistem penulisan angka dengan menggunakan dua simbol yaitu 0 dan 1. Dalam kriptografi sistem bilangan biner digunakan dalam pengolahan pada software, sedangkan dalam analisis keamanan kriptosistem, sistem bilangan biner digunakan dalam pengolahan pesan yang dikirimkan.

Sistem bilangan ini merupakan dasar dari semua sistem bilangan berbasis digital, terutama sekali dalam penggunaannya pada mesin-mesin elektronik atau komputer. Komputer dalam operasi-operasinya menggunakan bilangan-bilangan dengan basis dua. Sebagai contoh adalah pembacaan huruf pada komputer menggunakan sistem biner.

Dari sistem biner dapat dikonversikan ke sistem bilangan Oktal atau Hexadesimal. Sistem ini juga dapat kita sebut dengan istilah *bit*, atau *Binary Digit*. Pengelompokan biner dalam komputer selalu berjumlah 8, dengan istilah 1 Byte/bita. Dalam istilah komputer, 1 Byte = 8 bit. Kode-kode rancang bangun komputer, seperti ASCII (*American Standard Code for Information Interchange)* menggunakan sistem peng-*kode*-an 1 Byte.

(http://en.wikipedia.org/wiki/bilangan_biner)

Dalam penelitian ini menggunakan bilangan biner yang ada dalam tabel ASCII. Konversi huruf dan angka bisa dilihat pada lampiran 1.

Bilangan biner dan kode ASCII tersebut dalam menyandikan pesan digunakan dalam operasi matriks dan logika XOR .

2.2 Sistem Persamaan Linear

Menurut Anton (2004: 4) suatu sistem sebarang dari *m* persamaan linear dengan *n* faktor yang tidak diketahui dapat ditulis sebagai :

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2 \\ \vdots \quad & \quad \vdots \quad \quad \vdots \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

Dapat dilihat bahwa sistem persamaan linear tersebut dapat dipresentasikan sebagai persamaan perkalian matriks $Ax = b$, dengan

$$Ax = b$$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}_{m\times n} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}_{n\times 1} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}_{m\times 1}$$

Untuk menyelesaikan sistem persamaan linear tersebut salah satu metode yang digunakan adalah operasi baris elementer, caranya adalah :

1) Mengalikan baris dengan konstanta tak nol.
2) Menukarkan posisi dua baris.
3) Menambahkan kelipatan satu baris ke baris lainnya.

Operasi baris elementer sering juga digunakan untuk mencari invers suatu matriks.

2.3 Invers Matriks

Definisi dari invers matriks secara umum adalah :

Definisi 2.3.1

Jika A adalah matriks persegi, dan dapat ditemukan matriks B sehingga AB = BA = I, maka A dikatakan dapat dibalik (*invertibel*) dan B dinamakan invers dari A, ditulis $B = A^{-1}$.

(Anton, 2004: 46)

Jika matriks B tidak dapat didefinisikan, maka A dinyatakan sebagai matriks singular. Salah satu metode sederhana mencari invers dari matriks yang dapat dibalik adalah dengan mencari urutan operasi baris elementer tereduksi A menjadi matriks identitas, kemudian melakukan urutan operasi yang sama pada I_n untuk mendapatkan A^{-1}, yang dapat ditulis ke persamaan berikut :

$$[A \mid I] \sim [I \mid A^{-1}]$$

Selanjutnya akan diperlihatkan hubungan dari invers matriks dengan determinan matriks.

Definisi 2.3.2

Jika A adalah matriks persegi, maka **minor entri** a_{ij} dinyatakan oleh M_{ij} didefenisikan sebagai determinan submatriks yang tetap setelah baris ke-i dan kolom ke-j dihapuskan dari A. Bilangan $(-1)^{i+j}$ M_{ij} dinyatakan oleh C_{ij} dan dinamakan **kofaktor entri** a_{ij} .

(Anton, 2004: 115)

Setelah mendapatkan kofaktor entri a_{ij} didapatkan matriks kofaktor A yang didefinisikan sebagai berikut :

Definisi 2.3.3.

Jika A adalah sebarang matriks persegi $n \times n$ dan C_{ij} adalah kofaktor a_{ij}, maka matriks

$$\begin{bmatrix} C_{11} & C_{12} & \dots & C_{1n} \\ C_{21} & C_{22} & \dots & C_{2n} \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ C_{n1} & C_{n2} & \dots & C_{nn} \end{bmatrix}$$

dinamakan *matriks kofaktor* A. Transpos matriks ini dinamakan *adjoin A* dan dinotasikan dengan **Adj(A)**.

(Anton, 2004: 120)

Dari adjoin A dapat dicari invers dari matriks yang dapat dibalik. Teorema berikut untuk menentukan invers dari suatu matriks persegi jika ada.

Teorema 2.3.4.

Jika A adalah matriks yang dapat dibalik, maka

$$A^{-1} = \frac{1}{\det(A)} adj(A)$$

(Anton, 2004: 120)

Dari teorema tersebut, dapat disimpulkan jika suatu matriks mempunyai nilai determinan nol maka matriks tersebut tidak punya invers. Bukti dari teorema tersebut dapat dilihat pada lampiran 2.

Sedangkan pemakaian ilmu matriks lainnya yang dipakai adalah matriks invers tergeneralisasi.

2.4 Matriks Invers Tergeneralisasi

Diketahui matriks umum A yang berukuran $k \times n$. Suatu matriks B yang berukuran $n \times k$ adalah matriks invers tergeneralisasi dari matriks A, jika berlaku ABA = A. Jika A^+ menyatakan matriks invers tergeneralisasi dari A, maka :

$$A\, A^+ A = A \qquad \ldots (1)$$

Sebaliknya, untuk matriks A yang berukuran $k \times n$, matriks re-invers tergeneralisasi dari matriks A adalah suatu matriks X berukuran $n \times k$ sedemikian sehingga A adalah *generalized inverse* dari X, jadi berlaku XAX = X. Jika A^- menyatakan matriks re-invers tergeneralisasi (MRIT) dari A, maka :

$$A^- A A^- = A^- \qquad \ldots (2)$$

Menurut Wu dan Dawson (1998) untuk matriks A berukuran $m \times n$ yang mempunyai rank **(A)** = *m*, dengan membawa **A=** $[\mathbf{Im} \quad \mathbf{0}]\mathbf{Q}$ dengan **0** matriks nol berukuran $m \times (n-m)$ dan **Q** matriks nonsingular berukuran $n \times n$, MRIT dari A adalah :

$$A^- = Q^{-1} \begin{bmatrix} X \\ Y \end{bmatrix} \qquad \ldots (3)$$

untuk suatu matriks X berukuran $m \times m$ dan Y berukuran $(n-m) \times m$ tertentu. Dalam hal ini X dan Y adalah suatu matriks sedemikian sehingga :

$$X^2 = X \text{ dan } YX = Y \qquad \ldots (4)$$

Untuk menentukan kodenya diperlukan matriks paritas dan matriks generator.

2.5 Matriks Paritas

Definisi 2.5.1

Matriks paritas merupakan bagian matriksdari kode blok linear **C** adalah matriks generator dari kode ganda .

(http://en.wikipedia.org/wiki/Parity-check_matrix**)**

Dengan demikian, c merupakan *ciphertext* anggota bagian **C** jika dan hanya jika vektor biner matriks produk $\mathbf{H}^{\mathbf{T}}$ c = **0.** Matriks paritas merupakan bagian dari kode. Artinya, matriks paritas menunjukkan bagaimana kombinasi linier angka tertentu setiap *ciphertext* sama dengan nol.

Selain matriks paritas diperlukan juga matriks generator dalam pembentukan kunci.

2.6 Matriks Generator

Definisi 2.6.1

Misalkan C adalah (*n,k*)-*code*. Suatu matriks generator G untuk C adalah matriks ukuran $k \times n$ yang barisnya adalah anggota-anggota basis dari C.

(http://en.wikipedia.org/wiki/Generator_matrix)

Jika G suatu matriks generator untuk C dengan G = [I_k A], I matriks identitas $k \times k$, A matriks $k \times (n-k)$, maka G dikatakan **bentuk standar**. Matriks generator merupakan dasar untuk kode linear , menghasilkan semua kemungkinan kata kode. Jika matriks *G* dan kode linier adalah *C,*

$$c = m\,G$$

Sebuah matriks generator dapat digunakan untuk membangun matriks paritas memeriksa kode dan sebaliknya.

Selanjutnya diberikan definisi kode linear.

2.7 Kode Linear

Definisi 2.7.1

Diketahui *k, n* bilangan bulat positif dengan $k \leq n$ dan himpunan terhingga Z_2. Kode linier C yang mempunyai ukuran *k,* dinyatakan dengan **C-(*n,k*),** adalah ruang bagian (*subspace*) dari ruang vektor $Vn(Z_2)$.

(Vanstone dan Oorschot, 1989)

Kode linier **C-(*n,k*)** yang mempunyai ukuran *k,* berarti **C** dapat dibangun oleh k buah vektor yang bebas linier. Jika satu basis dari **C** dipilih, maka ada korespondensi satu-satu antara ruang pesan (data) berukuran *k* dengan kode **C**. Dalam hal ini, untuk pesan **m**, jika ditentukan **G** adalah matriks yang baris-barisnya merupakan vektor basis dari kode **C**, maka **mG** adalah kata kode dari pesan **m** tersebut.

2.8 Kriptografi

2.8.1. Pengertian Kriptografi

Menurut Rinaldi Munir (2006 : 2) kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan. Selain itu kriptografi juga bisa didefenisikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, autentifikasi, serta non-repudiasi.

1) **Kerahasiaan,** adalah layanan yang digunakan untuk menjaga isi informasi dari siapapun kecuali yang memiliki kunci rahasia atau otoritas untuk membuka informasi yang telah disandikan.
2) **Integritas Data,** berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk dapat menjaga integritas data, suatu sistem harus memiliki kemampuan untuk mendeteksi manipulasi data yang dilakukan pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pendistribusian data lain ke dalam data yang asli.
3) **Autentifikasi**, berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diautentifikasi keasliannya, isi datanya, waktu pengiriman dan lain sebagainya.
4) **Non-repudiasi**, merupakan usaha untuk mencegah terjadinya penyangkalan terhadappengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

2.8.2. Macam-macam Kriptografi

Kriptografi dapat dibedakan berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi. Berdasarkan hal tersebut kriptografi dibedakan menjadi kriptografi simetri dan asimetri.

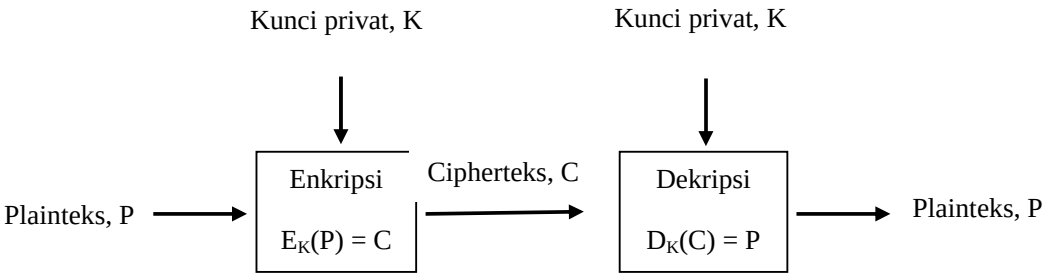
1) Kriptografi Simetri

Kriptografi simetri digunakan sebuah kunci rahasia yang sama untuk melakukan proses enkripsi dan dekripsinya, tetapi sebuah kunci dapat diturunkan

dari kunci lainnya. Kunci-kunci ini harus dirahasiakan, oleh karena itu sistem ini sering disebut dengan *secret-key ciphersystem*.

Fungsi kriptografi simetri yang utama adalah melindungi kerahasiaan data yang dikirim melalui saluran tidak aman dan melindungi kerahasiaan data yang disimpan pada media yang tidak aman. Kelebihan sistem kriptografi simetri ini adalah kecepatan proses enkripsi dan dekripsinya yang jauh lebih cepat dibandingkan dengan algoritma kriptografi asimetri, hal ini disebabkan karena efisiensi yang terjadi pada pembangkit kunci.

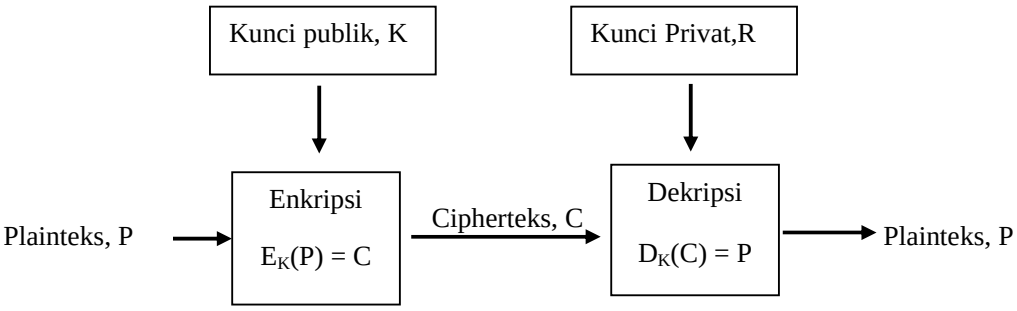
Sedangkan kelemahan dari kriptografi simetri adalah baik pengirim maupun penerima pesan harus memiliki kunci yang sama, sehingga pengirim pesan harus mencari cara yang aman untuk memberitahukan kunci kepada penerima pesan. Kelemahan lain adalah masalah efisiensi jumlah kunci, jika jumlah user yang sangat banyak, sistem ini tidak efisien lagi. Untuk tiap pasang pengguna dibutuhkan sebuah kunci yang berbeda, sedangkan sangat sulit untuk menyimpan dan mengingat kunci yang banyak secara aman. Apabila kunci sampai hilang atau dapat ditebak maka kriptosistem ini tidak aman lagi.Contoh skema enkripsi kunci simetrik adalah : DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) dan FEAL.



Gambar 1. Skema kriptografi simetri

2) Kriptografi Asimetri

Pada kriptografi asimetri digunakan algoritma unci publik, dimana menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Disebut juga kriptografi kunci publik karena kunci untuk enkripsi dibuat untuk diketahui oleh umum (*public-key*) atau dapat diketahui siapa saja, tapi untuk proses dekripsinya hanya dapat dilakukan oleh yang berwenang yang memiliki kunci rahasia untuk mendekripsinya, disebut *private-key*. Contoh algoritma kriptografi kunci publik diantaranya RSA (Rivert-Shamir-Adelman), El Gamal, DSA (Digital Signature Algorithm), Knapsack, dan sebagainya.



Gambar 2. Skema kriptografi asimetri

2.8.3. Keamanan Kriptografi

Tujuan utama dari kriptografi adalah menjaga kerahasiaan plainteks atau kunci, atau keduanya dari penyadap. Penyadap akan berusaha mendapatkan data yang digunakan untuk kegiatan kriptanalis. Penyadap bisa merangkap sebagai kriptanalis.

Suatu sistem kriptografi dikatakan aman jika para penyusup (*adversary*) dengan kemampuan yang dimilikinya tidak dapat memecahkan atau membobol

sistem tersebut. Berdasarkan kemampuan yang dimiliki penyusup, terdapat dua jenis keamanan sistem kriptografi, yaitu:

1) Keamanan tak kondisional, jika penyusup tidak dapat membobol sistem dengan kemampuan komputer yang tidak terbatas. Keamanan ini berhubungan dengan teori informasi dan teori probabilitas.
2) Keamanan kondisional, jika secara teoritis mungkin bagi penyusup untuk membobol sistem tapi secara komputasi tidaklah mungkin (karena keterbatasan sumberdaya dan kemampuan penyusup untuk mengakses informasi). Keamanan ini berhubungan dengan teori kompleksitas.

Sistem kriptografi dikatakan aman bila memiliki keadaan sebagai berikut :

1) Jika harga untuk membobol sistem lebih besar daripada nilai informasi yang dibuka.

   Contoh : nilai informasi yang akan dibobol tidak bisa menghasilkan uang banyak seperti sandi suatu brankas keuangan namun biaya yang dikeluarkan untuk mengetahui pesan tersebut sangat mahal.

2) Bila waktu yang diperlukan untuk membobol sistem tersebut lebih lama daripada lamanya waktu yang diperlukan oleh informasi itu untuk tetap aman .

   Contoh : suatu informasi harus dijaga keamanannya sampai batas 3 hari dan jika lewat dari 3 hari pesan itu tidak terpakai lagi namun untuk mendapatkan pesan tersebut dibutuhkan waktu seminggu sehingga bisa diketahui apa isi pesan tersebut.

3) Bila jumlah data yang dienkripsi dengan kunci dan algoritma yang sama lebih sedikit dari jumlah data yang diperlukan untuk menembus algoritma tersebut.

Jika hasil deskripsi pesan lebih panjang dari *ciphertext* maka pesan yang asli sulit ditemukan.

2.9. Operasi Logika XOR (*Exclusive OR,* ⊕)

Kata "atau" (*or*) digunakan secara eksklusif (*exclusive or*) yaitu dalam bentuk "*p* atau *q* tetapi bukan keduanya". Menurut Munir(2007: 10) untuk membedakan disjungsi eksklusif dengan *inclusive or* digunakan operator logika XOR yang definisinya adalah sebagai berikut :

Definisi 2.9.1

Misalkan *p* dan *q* adalah proposisi. *Exclusive or p* dan *q,* dinyatakan dengan notasi $p \oplus q$, adalah proposisi yang bernilai benar bila hanya salah satu dari *p* dan *q* benar, selain itu salah.Pemakaian operasi XOR dapat dilihat dari tabel berikut :

Tabel 1 Operasi Logika XOR

Input		Output (*XOR*)
1	1	0
1	0	1
0	1	1
0	0	0

(Brookshear, 2003: 23)

Berdasarkan tabel di atas operasi logika XOR sesuai dengan operasi dalam modulo 2.

BAB IV

KESIMPULAN

4.1 Kesimpulan

4.1.1 Proses pembentukan kunci **G**, **H**, dan $\mathbf{H}^-$ adalah sebagai berikut :

a) Pilih matriks generator $\mathbf{G} = [\mathbf{I}_k \quad \mathbf{A}]$, dengan sembarang **A** berukuran $k \times (n-k)$.

b) Bentuk $\mathbf{H}_1 = [\mathbf{A}^T \quad \mathbf{I}_{n-k}]$

c) Pilih sembarang **S** berukuran $(n-k)\times(n-k)$ yang non singular.

d) Bentuk matriks paritas $\mathbf{H} = \mathbf{SH}_1$.

e) Bawa **H** ke bentuk $\mathbf{H} = [\mathbf{I}_{n-k} \quad \mathbf{0}]\mathbf{Q}$, dengan **0** berukuran $(n-k)\times k$ matriks nol dan **Q** berukuran $n \times n$ matriks nonsingular.

f) Pilih matriks **X** berukuran $(n-k)\times(n-k)$ dan **Y** berukuran $k \times (n-k)$ yang memenuhi persamaan 2.3.4.

g) MRIT dari **H** adalah $\mathbf{H}^- = \mathbf{Q}^{-1}\begin{bmatrix} X \\ Y \end{bmatrix}$.

h) Kunci rahasia (*privat key*) $R = H^- H$.

Kunci publik adalah **G** dan $\mathbf{H}^-$ dipublikasikan sedangkan kunci privatnya $R = H^- H$ disimpan oleh penerima pesan.

4.1.2 Proses enkripsi dan deskripsi dapat dirangkum sebagaimana sebagai berikut :

Kunci Publik : **G, $\mathbf{H}^-$**

Kunci Rahasia : $\mathbf{H}^-\mathbf{H}$

Proses Enkripsi : $\mathbf{c = mG \oplus e(H^{-})^{T}}$

Proses Deskripsi : 1). $\mathbf{mG = c\,(I_n \oplus (H^{-}H)^{T})}$

2). Dapatkan **m** dari **mG**

4.1 3 Langkah melindungi pesan yang dikirimkan adalah :

a) Pemilihan mariks paritas **H** untuk melindungi kunci rahasia $\mathbf{R= H^{-}H.}$

b) Pemilihan sebarang vektor biner untuk menemukan bentuk kesalahan $\mathbf{E= e(H^{-})^{T}}$.

c) Pemilihan sebarang vektor kesalahan **E** untuk mengoreksi kesalahan kode.

4.2 Saran

Kriptosistem kunci publik yang dibangun berdasarkan matriks invers tergeneralisasi masih memerlukan penelitian lebih lanjut, misalnya dalam hal autentikasi dan pertukaran kunci. Penelitian lebih lanjut di bidang keamanan kriptosistem ini masih terbuka lebar khususnya untuk meyakinkan para pengguna, apakah disain kriptosistem ini cukup aman atau tidak untuk melakukan penyandian data.

DAFTAR KEPUSTAKAAN

Achmad, Ikhwanudin.2007. *Aplikasi Invers Matriks Tergeneralisi Pada Cipher Hill.* http://www.ikhwan.web.ugm.ac.id diakses tanggal 18 Februari 2010

Anton,Howard. 2004. *Aljabar Linear Elementer versi Aplikasi*. Erlangga : Jakarta.

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi*. Andi Offset : Yogyakarta.

Brookshear, J. Glen. 2003. *Computer Science-Suatu Pengantar*. Marquette University : USA.

Munir, Rinaldi. 2006. *Kriptografi*. Informatika : Jakarta.

Munir, Rinaldi. 2007. *Matematika Diskrit*. Informatika : Bamdung

Universitas Negeri Padang. 2007. *Pedoman Penyusunan Skripsi Mahasiswa MIPA.*

http://en.wikipedia.org/wiki/bilangan_biner diakses tanggal 15 Juni 2010

http://en.wikipedia.org/wiki/Generator_matrix diakses tanggal 6 Juni 2010

http://en.wikipedia.org/wiki/Parity-check_matrix diakses tanggal 6 Juni 2010