

SISTEM KRIPTOGRAFI IDEA

Oleh
Taufik Hidayat
NIM : 23202147

ABSTRAK

*Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apalagi kalau data tersebut berada dalam suatu jaringan komputer yang terhubung / terkoneksi dengan jaringan publik misalnya internet. Tentu saja data yang sangat penting tersebut dilihat atau dibajak oleh orang yang tidak berwenang. Sebab kalau hal ini sampai terjadi kemungkinan data kita akan rusak bahkan bisa hilang yang akan menimbulkan kerugian material yang besar. Pada tulisan ini akan dibahas sistem keamanan pengiriman pesan/data dengan menggunakan penyandian yang bertujuan untuk menjaga kerahasiaan suatu pesan dari akses orang-orang yang tidak berwenang/berhak. Karena sistem keamanan pengiriman ini sangat luas cakupannya maka pada bagian ini dibatasi hanya menguraikan Kriptografi menggunakan Algoritma **IDEA**, yang meliputi proses enkripsi, dekripsi dan contoh manipulasi data dengan menggunakan Algoritma IDEA dan ambaran umum processor yang mengolah kriptografi algoritma IDEA.*

DAFTAR ISI

ABSTRAK	i
DAFTAR ISI	ii
BAB I : PENDAHULUAN	1
1.1 Sejarah Kriptografi	1
1.2 Tujuan Kriptografi	2
1.3 Terminologi dasar Kriptografi	4
1.4 Klasifikasi Algoritma Kriptografi	4
BAB II : ENKRIPSI dan DEKRIPSI	7
2.1 Pengertian Dasar	7
2.2 Cryptographyc System (CryptoSystem)	9
2.2.1 Symetric Crypto System	9
2.2.2 Assymmetric Crypto System	12
BAB III : Kriptogafi IDEA	15
3.1 Diskripsi Umum Algoritma IDEA	15
3.2 Proses Enkripsi IDEA	17
3.3 Proses Dekripsi IDEA	19
3.4 Pembentkan Sub kunci	22
3.5 Arsitektur Umum Proessor Kriptogafi IDEA	22
3.6 Contoh Komputasi Penggunaan Algoritma IDEA	24
BAB IV : PENUTUP	27
DAFTAR PUSTAKA	28

Bab I

PENDAHULUAN

1.1 Sejarah Kriptografi

Kriptografi atau yang sering dikenal dengan Sebutan ilmu penyandian data, adalah suatu bidang ilmu dan seni (art and science) yang bertujuan untuk menjaga kerahasiaan suatu pesan yang berupa data data dari akses oleh orang-orang atau pihak-pihak lain yang tidak berhak sehingga tidak menimbulkan kerugian. Bidang ilmu Kriptografi ini semulanya populer dibidang militer dan bidang intelijen untuk menyandikan pesan-pesan panglima perang kepada pasukan yang berada di garis depan, akan tetapi seiring dengan semakin berkembangnya teknologi utamanya teknologi informasi dan semakin padatnya lalu lintas informasi yang terjadi tentu saja semakin menuntut adanya suatu komunikasi data yang aman, bidang ilmu ini menjadi semakin penting. Sekarang bidang ilmu ini menjadi salah satu isu suatu topik riset yang tidak habis-habisnya diteliti dengan melibatkan banyak peneliti.

Ilmu Kriptografi sebenarnya sudah mulai dipelajari manusia sejak tahun 400 SM, yaitu pada zaman Yunani kuno. Dari catatan bahwa "Penyandian Transposisi" merupakan sistem kriptografi pertama yang digunakan atau dimanfaatkan. Bidang ilmu ini terus berkembang seiring dengan kemajuan peradaban manusia, dan memegang peranan penting dalam strategi peperangan yang terjadi dalam sejarah manusia, mulai dari sistem kriptografi "Caesar Cipher" yang terkenal pada zaman Romawi kuno, "Playfair Cipher" yang digunakan Inggris dan "ADFGVX Cipher" yang digunakan Jerman pada Perang Dunia I,

hingga algoritma-algoritma kriptografi rotor yang populer pada Perang Dunia II , seperti Sigaba / M-134 (Amerika Serikat), Typex (Inggris), Purple (Jepang), dan mesin kriptografi legendaris Enigma (Jermn).

Induk dari keilmuan dari kriptografi sebenarnya adalah matematika, khususnya teori aljabar yang mendasar ilmu bilangan . Oleh karena itu kriptografi semakin berkembang ketika komputer ditemukan. Sebab dengan penemuan komputer memungkinkan dilakukanya perhitungan yang rumit dan komplekdalam waktu yang relatif sangat singkat, suatu hal yang sebelumnya tidak dapat dilakukan. Dari hal tersebut lahirlah banyak teori dan algotitma penyandian data yang semakin kompleks dan sulit dipecahkan.

Dewasa ini bidang ilmu kriptografi memiliki kemungkinan aplikasi yang sangat luas, mulai dari bidang militer, telekomunikasi, jaringan komputer, keuangan dan perbakan, pendidikan dan singkatnya dimana suatu kerahasiaan data amatdiperlkan disitulah kriptografi memegang peranan pentingh. Produk-produk yang menggunakan kriptografi sebagai dasarnyapun cukup beragam, mulai dari kartu ATM, E-Commerce, secure e-mail dan lain-lain.

1.2 Tujuan Kriptografi

Dalam teknologi informasi, telah dan sedang sedang dikembangkan cara cara untuk menangkal berbagai bentuk serangan semacam penyadapan dan pengubahan data yang dikirimkan. Salah satu cara yang ditempuh mengatasi masalah ini ialah dengan menggunakan kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak yang tidak berhak mengakses. Transformasi ini meberikan solusi

pada dua macam masalah keamanan data, yaitu masalah privasi (privacy) dan keotentikan (authentication). Privasi mengandung arti bahwa data yang diimkan hanya dapat dimengerti informasinya oleh penerima yang sah atau berhak. Sedangkan keotentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan .

Adapun tujuan sistem kriptografi adalah sebagai berikut :

- Confidentiality
Yaitu memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi.
- Message Integrity
Yaitu memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat data dibuat/dikirim sampai dengan saat data tersebut dibuka.
- Non-repudiation
Yaitu memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.
- Authentication
Yaitu memberikan dua layanan. Pertama mengidentifikasi keaslian suatu pesan dan memberikan jaminan keotentikannya. Kedua untuk menguji identitas seseorang apabila ia akan memasuki sebuah sistem.

1.3 Terminologi dasar Kriptografi

Kriptografi merupakan kumpulan teknik untuk Mengencode data dan pesan sedemikian sehingga data dan pesan tersebut dapat disimpan dan ditransmisikan dengan aman. Berikut ini beberapa terminologi dasar dari kriptografi serta hal-hal yang berkaitan dengan terminologi tersebut,

- Kriptografi dapat digunakan untuk meningkatkan keamanan komunikasi meskipun komunikasi tersebut dilakukan dengan media komunikasi yang sangat tidak aman (misalnya Internet). Kita juga dapat menggunakan kriptografi untuk melakukan enkripsi file-file sensitif kita, sehingga orang lain tidak dapat mengartikan data-data yang ada
- Kriptografi dapat digunakan untuk memberikan jaminan integritas data serta menjaga kerahasiaan
- Dengan menggunakan kriptografi, maka sangat mungkin untuk meverifikasi asal data dan pesan yang ada menggunakan digital signature
- Pada saat menggunakan metoda kriptografi, hanya kunci sesi yang harus tetap dijaga kerahasiannya. Algoritma, ukuran kunci dan format file dapat dibaca oleh siapapun tanpa mempengaruhi keamanan.

1.4 Klasifikasi Algoritm Kriptografi

Tingkat keamanan suatu algoritma diperoleh dengan

menyembunyikan secara rahasia bagaimana algoritma itu bekerja, algoritma ini disebut dengan algoritma rahasia (restricted algorithm). Pada awalnya algoritma jenis ini yang berkembang, namun algoritma jenis ini mempunyai banyak kelemahan seperti setiap pengguna harus menggunakan algoritmanya sendiri dan jika algoritma ini telah diketahui orang, algoritma ini harus diganti dengan yang baru.

Kelemahan lain dari algoritma jenis ini adalah tidak memungkinkan dilakukan standardisasi sebagai kendali mutu, dimana setiap kelompok pengguna harus mempunyai algoritma sendiri-sendiri dan unik.

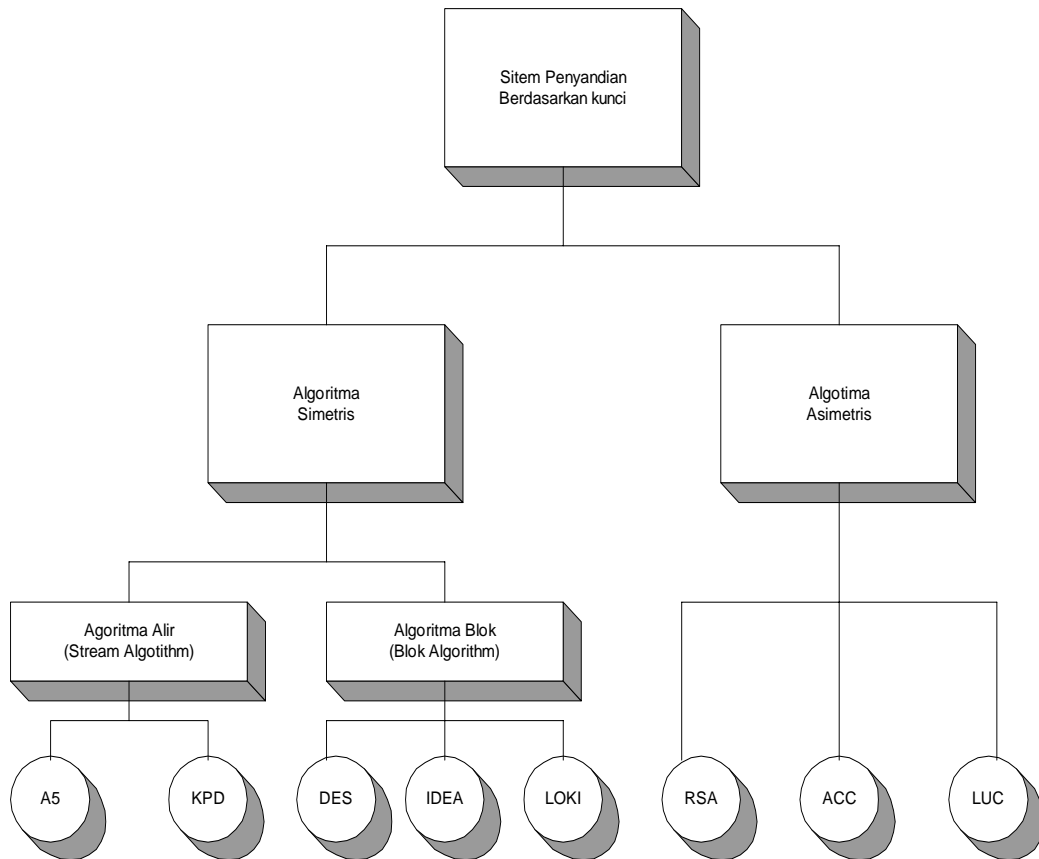
Kriptografi modern dapat memecahkan masalah algoritma tersebut diatas yaitu dengan algoritma kunci. Kunci ini dapat berupa sembarang dari suatu nilai dari sejumlah angka. Dengan demikian tingkat keamanan dari algoritma yang menggunakan kunci adalah berdasarkan kerahasiaan kuncinya, tidak berdasarkan detail dari algoritma itu sendiri. Oleh karena itu algoritma ini dapat dapat dipublikasikan dan dianalisa, dan algoritma ini dapat diproduksi secara masal.

Dewasa ini algoritma rahasia hanya digunakan terbatas pada aplikasi yang relatif kurang membutuhkan tingkat keamanan yang tinggi misalkan pada teknik pengacakan (scrambling) video, sedangkan algoritma algoritma kunci digunakan pada berbagai aplikasi yang membutuhkan tingkat keamanan yang sangat tinggi, misalkan pada kartu ATM dan secure mail.

Secara umum ada dua tipe algoritma yang berdasarkan kunci yaitu algoritma simetris (symmetric algorithm) dan algoritma kunci publik (public-key algorithm). Perbedaan utama antara Symetric algorithm dengan public-key algorithm adalah pada kunci enkripsi

K_1 dan kunci dekripsi K_2 . Selain itu juga terdapat perbedaan dalam kecepatan proses dan keamanannya.

Berikut ini bagan suatu sistem penyandian berdasarkan kunci beserta contoh-contoh algoritma yang digunakan.



Gambar : Blok Diagram Pembagian sistem Kriptografi Berdasarkan Kunci

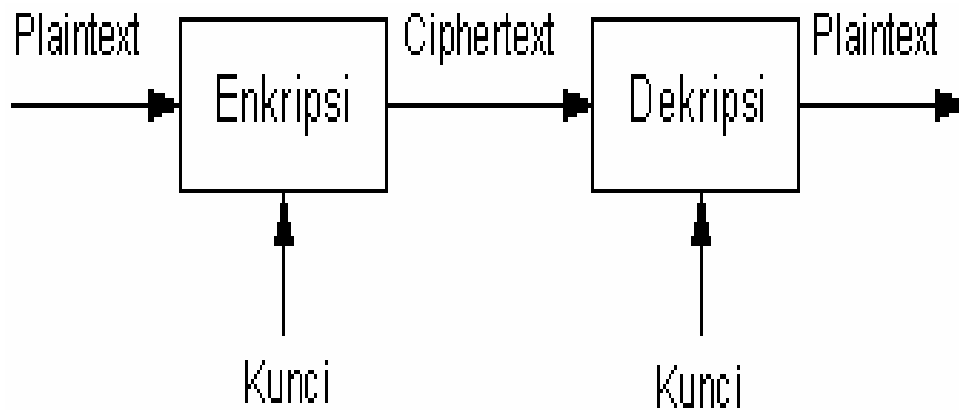
Bab II

ENKRIPSI DAN DEKRIPSI

2.1 Pengertian Dasar

Suatu pesan yang tidak disandikan disebut sebagai *plaintext* ataupun dapat disebut juga sebagai *cleartext*. Proses yang dilakukan untuk mengubah *plaintext* ke dalam *ciphertext* disebut *encryption* (enkripsi) atau *encipherment*. Sedangkan proses untuk mengubah *ciphertext* kembali ke *plaintext* disebut *decryption* (dekripsi) atau *decipherment*. Secara sederhana istilah-istilah di atas dapat digambarkan

sebagai berikut :



Gambar : Proses Enkripsi/Dekripsi Sederhana

Cryptography adalah suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh *cryptographer*. Sedang, *cryptanalysis* adalah suatu ilmu dan seni membuka

(breaking) ciphertext dan orang yang melakukannya disebut *cryptanalyst*.

Cryptographic system atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi. Secara umum, kunci-kunci yang digunakan untuk proses pengenkripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan.

Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut :

$$EK (M) = C \quad (\text{Proses Enkripsi})$$

$$DK (C) = M \quad (\text{Proses Dekripsi})$$

Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya.

Dengan demikian keamanan suatu pesan tergantung pada kunci ataupun kunci-kunci yang digunakan, dan tidak tergantung pada algoritma yang digunakan. Sehingga algoritma-algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis, serta produk-produk yang menggunakan algoritma tersebut dapat diproduksi massal. Tidaklah menjadi masalah apabila seseorang mengetahui algoritma yang kita gunakan.

Selama ia tidak mengetahui kunci yang dipakai, ia tetap tidak dapat membaca pesan.

2.2 Cryptographic system (cryptosystem)

Suatu cryptosystem terdiri dari sebuah algoritma, seluruh kemungkinan plaintext, ciphertext dan kunci-kunci. Secara umum cryptosystem dapat digolongkan menjadi dua buah, yaitu :

2.2.1 Symmetric Cryptosystem

Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik $K_1 = K_2 = K$, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai *secret-key ciphersystem*. Jumlah kunci yang dibutuhkan umumnya adalah :

$${}_nC_2 = \frac{n \cdot (n-1)}{2}$$

dengan n = menyatakan banyaknya pengguna (user)
 C = menyatakan banyaknya kunci.

Contoh dari sistem ini adalah :

- **IDEA** (International Data Encryption Algorithm)
- Data Encryption Standard (DES)
- Blowfish

Tingkat keamanan kriptosistem yang menggunakan algoritma ini sangat ditentukan oleh kerahasiaan kunci K yang digunakan . Jika seseorang hendak mengirimkan suatu pesan kepada orang lain , atau melakukan secure communication, orang tersebut harus terlebih dahulu memberikan kepada pihak yang dituju kunci K yang hendak digunakannya. Hal ini jelas membutuhkan saluran komunikasi yang benar-benar aman dan tidak dapat disadap (secure channel).

Secara matematis Algoritma ini dapat ditulis :

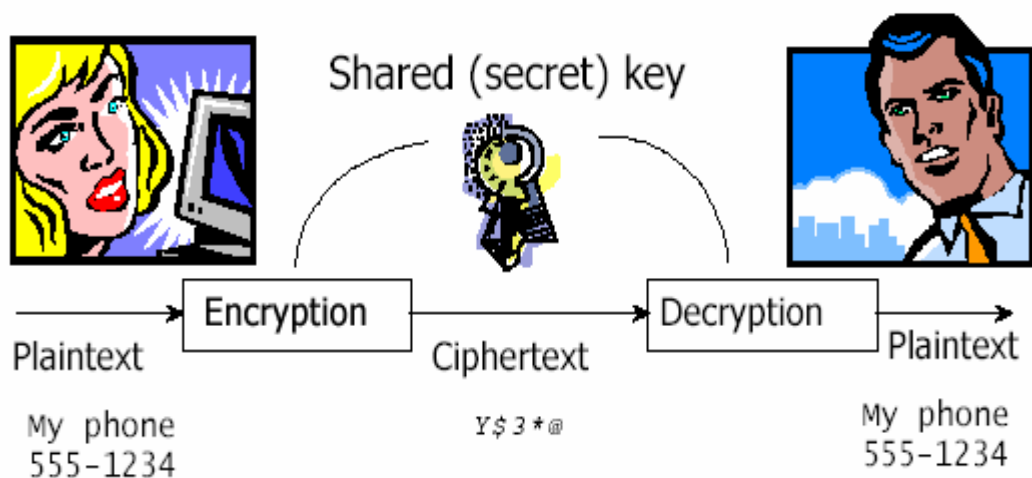
$$E_k (M) = C \Leftrightarrow d_k (C) = M$$

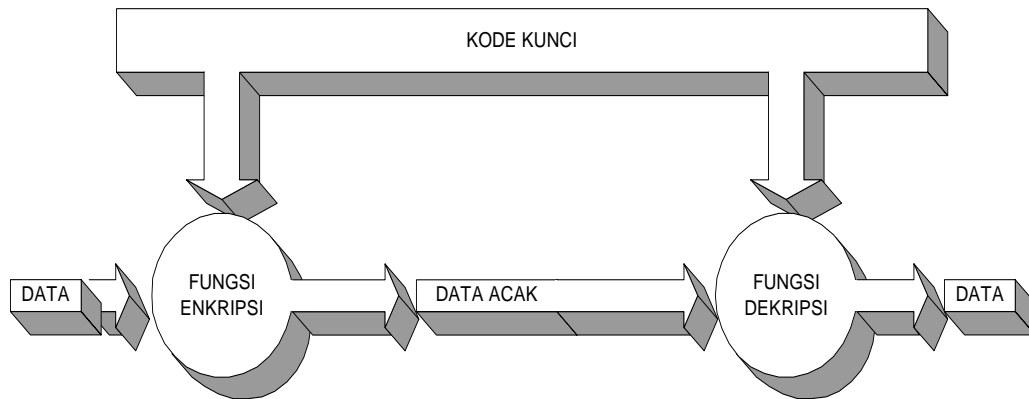
E_k adalah proses enkripsi dengan menggunakan

kunci K

M adalah pesan asli (Plaintext)

C adalah pesan yang disandikan (Ciphertext)





b)

Gambar : a) dan b) Teknik Symmetric Cryptosystem

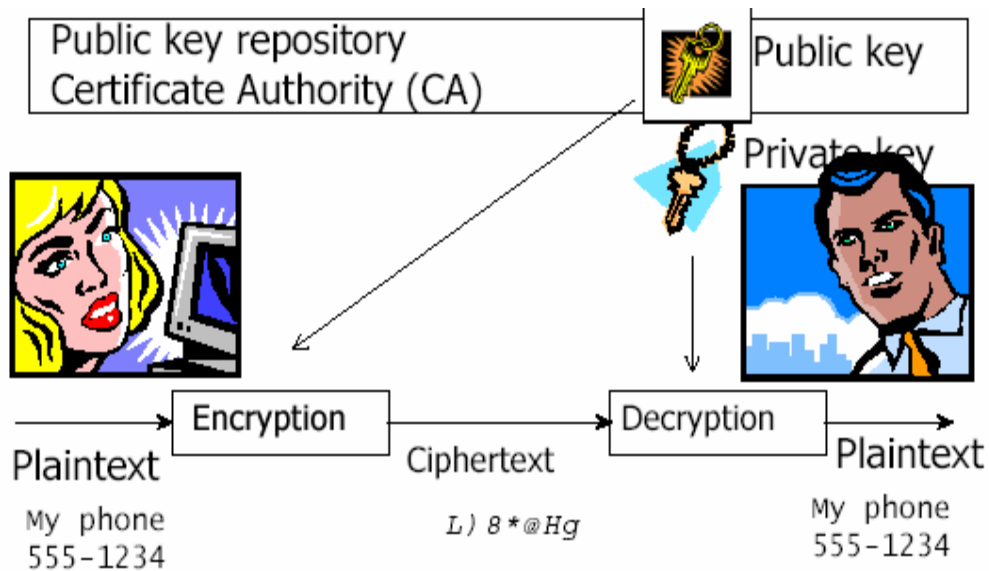
Prinsip kerja dari kriptografi kunci simetrik adalah sebagai berikut :

- Pengirim dan penerima data/Informasi sepakat menggunakan system kriptografi tertentu
- Pengirim dan penerima sepakat menggunakan satu kunci tertentu
- Dilakukan enkripsi sebelum data dikirim dan dekripsi setelah data dikirim

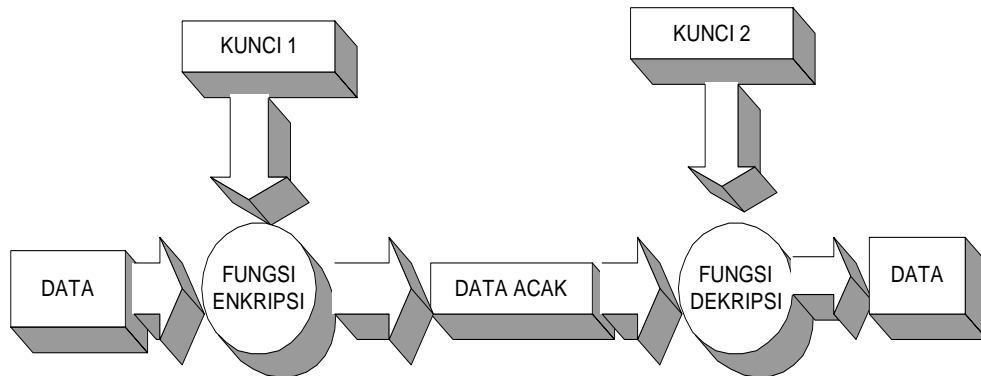
Tingkat keamanan dari kriptosistem yang menggunakan algoritma ini sangat ditentukan oleh kerahasiaan kunci K yang digunakan. Jika seseorang hendak mengirimkan suatu pesan kepada orang lain atau melakukan secure communication, orang tersebut harus terlebih dahulu memberitahu kepada pihak yang dituju kunci K yang digunakannya. Hal ini jelas membutuhkan saluran komunikasi yang benar-benar aman dan tidak dapat disadap (secure channel). Faktor inilah yang menjadi kelemahan cara ini yaitu masalah keamanan kunci dan bagaimana mendistribusikan kunci K tersebut.

2.2.2 Assymmetric Cryptosystem

Dalam assymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (*public key*) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (*private key*) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.



a)



b)

Gambar : a) dan b) Teknik Assymmetric Cryptosystem

Setiap cryptosytem yang baik harus memiliki karakteristik sebagai berikut :

- Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
- Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
- Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
- Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya

Namun demikian perlu diperhatikan bahwa bila suatu cryptosystem berhasil memenuhi seluruh karateristik di atas belum tentu ia merupakan sistem yang baik. Banyak cryptosystem lemah yang terlihat baik pada awalnya. Kadang kala untuk menunjukkan bahwa suatu cryptosystem

kuat atau baik dapat dilakukan dengan menggunakan pembuktian matematika.

Hingga saat ini masih banyak orang yang menggunakan cryptosystem yang relatif mudah dibuka, alasannya adalah mereka tidak mengetahui sistem lain yang lebih baik serta kadang kala terdapat motivasi yang kurang untuk menginvestasikan seluruh usaha yang diperlukan untuk membuka suatu sistem.

Berikut ini akan diperlihatkan perbedaan beerbagai aspek penting dari Symmetric Cryptosystem dengan Assymmetric Cryptosys

Symmetric Cryptosysem	Asymmetric Cryptosystem
<p>Yang dibutuhkan untuk bekerja :</p> <ol style="list-style-type: none"> 1. Algoritma yang sama dengan kunci yang sama dapat digunakan untuk proes enkripsi maupun dekripsi 2. Pengirim dan penerima hars membagialgoritma dan kunci yang sama 	<p>Yang dibutuhkan untuk bekerja :</p> <ol style="list-style-type: none"> 1. Algoritma yang digunakan untuk enkripsidan dekripsi dengan sepasang kunci , satu untuk ekripsi satu untuk dekripsi 2. Penirim dan penerima harus mempunyai sepasan kunci yang cocok
<p>Yang dibutuhkan untuk keamanan</p> <ol style="list-style-type: none"> 1. Kunci harus dirahasiakan. 2. Adalah tidak mungkin atau sangat tidak praktis untuk 	<p>Yang dibutuhkan untuk keamanan</p> <ol style="list-style-type: none"> 1. Salah satu kunci harus dirahasiakan . 2. Adalah tidak mungki aau snat tidak praktis untuk

menterjemahkan Informasi yang telah dienkripsi 3. Pengetahuan tentang algoritma dan sampel dari kata yang terenkripsi tidak menukupi untuk menentukan kunci	menterjemahkan Informasi yang telah dienkripsi. 3. Pengetahuan tentang algoritma dan sampel dari kata yang terenkripsi tidak mencukupi untuk menentukan kunci
---	---

Bab III

KRIPTOGRAFI IDEA

3.1 Diskripsi umum Algoritma IDEA

Algoritma penyandian IDEA (International Data Encryption Algorithm) muncul pertama kali pada tahun 1990 yang dikembangkan oleh ilmuwan Xueijia Lai dan James L Massey. Algoritma utama dari sistem kriptografi IDEA adalah sebagai berikut :

1. Proses enkripsi : $e_k(M) = C$
2. Proses dekripsi : $d_k(C) = M$

Dimana :

E = adalah fungsi enkripsi

D = adalah fungsi dekripsi

M = adalah pesan terbuka

C = adalah pesan rahasia

K = adalah kunci enkripsi atau dekripsi

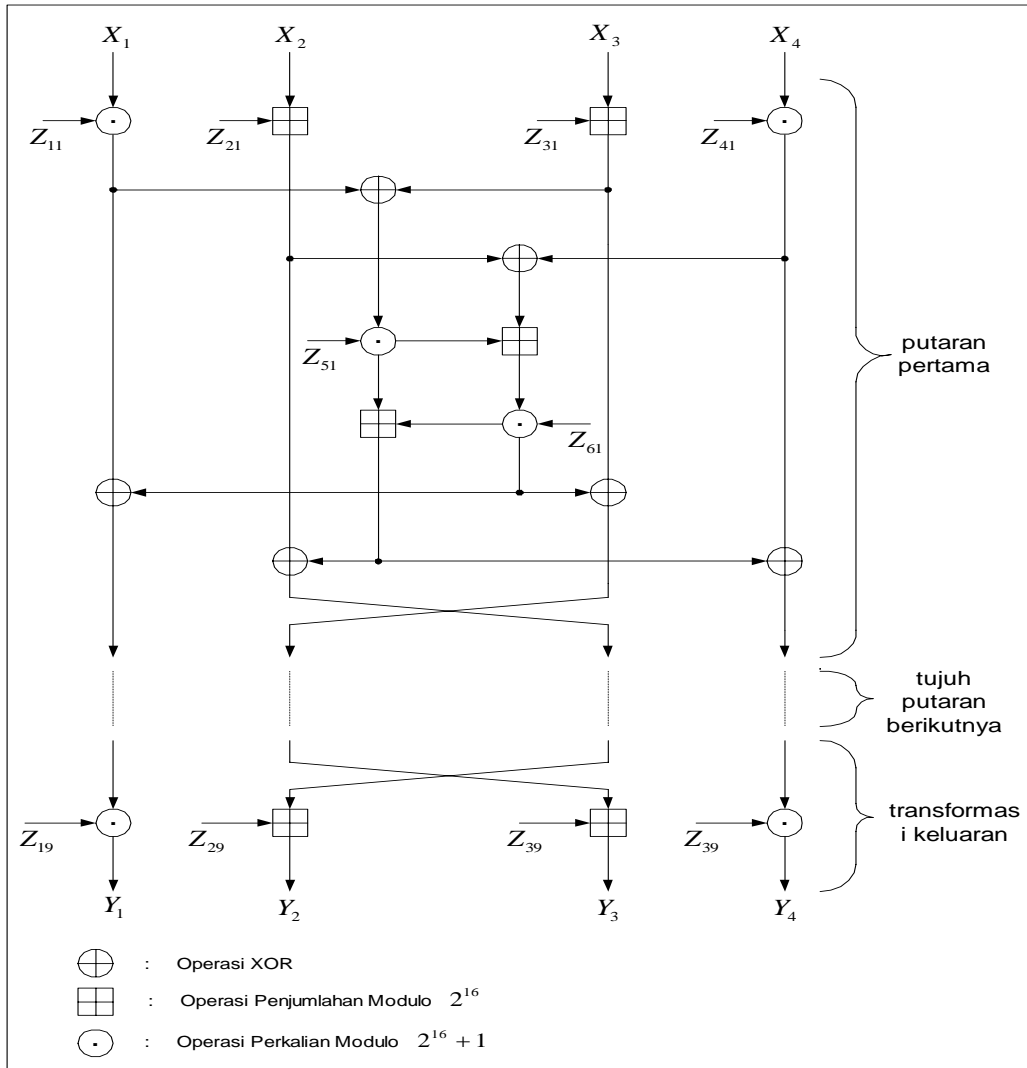
IDEA (International Data Encryption Algorithm) merupakan algoritma simetris yang beroperasi pada sebuah blok pesan terbuka dengan lebar 64-bit. Dan menggunakan kunci yang sama , berukuran 128-bit, untuk

proses enkripsi dan dekripsi. Pesan rahasia yang dihasilkan oleh algoritma ini berupa blok pesan rahasia dengan lebar atau ukuran 64-bit

Pesan dekripsi menggunakan blok penyandi yang sama dengan blok proses enkripsi dimana kunci dekripsinya diturunkan dari kunci enkripsi.

Algoritma ini menggunakan operasi campuran dari tiga operasi aljabar yang berbeda, yaitu XOR, operasi penjumlahan modulo 2^{16} dan operasi perkalian modulo $(2^{16} + 1)$. Semua operasi ini digunakan dalam pengoperasian sub-blok 16-bit.

Algoritma ini melakukan iterasi yang terdiri dari atas 8 putaran dan I transformasi keluaran pada putaran ke 9, dimana gambaran komputasi dan transformasi keluaran ditunjukkan oleh gambar sebagai berikut :



Gambar Algoritma IDEA

3.2 Proses Enkripsi IDEA

Pada proses enkripsi, algoritma IDEA ini ditunjukkan oleh gambar di atas, terdapat tiga operasi yang berbeda untuk pasangan sub-blok 16-bit yang digunakan, sebagai berikut :

- XOR dua sub-blok 16-bit bir per bit, yang disimbolkan dengan tanda \oplus
- Penjumlahan integer modulo $(2^{16} + 1)$ dua sub-blok 16-bit , dimana edua sub-blok itu dianggap sebagai representasi biner dari integer biasa, yang disimbolkan

Dengan tanda \boxplus

- Perkalian modulo $(2^{16} + 1)$ dua sub-blok 16-bit, dimana kedua sub-blok 16-bit itu dianggap sebagai representasi biner dari integer biasa kecuali sub-blok nol dianggap mewakili integer 2^{16} , yang disimbolkan dengan tanda \odot

Blok pesan terbuka dengan lebar 64-bit, X , dibagi menjadi 4 sub-blok 16-bit, X_1, X_2, X_3, X_4 , sehingga $X = (X_1, X_2, X_3, X_4)$. Keempat sub-blok 16-bit itu ditransformasikan menjadi sub-blok 16-bit, Y_1, Y_2, Y_3, Y_4 , sebagai pesan rahasia 64-bit $Y = (Y_1, Y_2, Y_3, Y_4)$ yang berada dibawah kendali 52 sub_blok kunci 16-bit yang dibentuk dari dari blok kunci 128 bit.

Keempat sub-blok 16-bit, X_1, X_2, X_3, X_4 , digunakan sebagai masukan untuk putaran pertama dari algoritma IDEA. Dalam setiap putaran dilakukan operasi XOR, penjumlahan, perkalian antara dua sub-blok 16-bit dan diikuti pertukaran antara sub-blok 16-bit putaran kedua dan ketiga. Keluaran putaran sebelumnya menjadi masukan putaran berikutnya. Setelah putaran kedelapan dilakukan transformasi keluaran yang dikendalikan oleh 4 sub-blok unci 16-bit.

Pada setiap putaran dilakukan operasi-operasi sebagai berikut :

- 1) Perkalian X_1 dengan sub-kunci pertama
- 2) Penjumlahan X_2 dengan sub-kunci kedua
- 3) Pejumlahan X_3 dengan sub kunci ketiga
- 4) Perkalian X_4 dengan sub kunci keempat
- 5) Operasi XOR hasil langkah 1) dan 3)
- 6) Operasi XOR hasil angka 2) dan 4)
- 7) Perkalian hasil langkah 5) dengan sub-kunci kelima
- 8) Penjumlahan hasil langkah 6) dengan langkah 7)

- 9) Perkalian hasil langkah 8) dengan sub-kunci keenam
- 10) Penjumlahan hasil langkah 7) dengan 9)
- 11) Operasi XOR hasil langkah 1) dan 9)
- 12) Operasi XOR hasil langkah 3) dan 9)
- 13) Operasi XOR hasil langkah 2) dan 10)
- 14) Operasi XOR hasil langkah 4) dan 10)

Keluaran setiap putaran adalah 4 sub-blok yang dihasilkan pada langkah 11), 12), 13), dan 14) dan menjadi masukan putaran berikutnya.

Setelah putaran kedelapan terdapat transformasi keluaran, yaitu :

- 1) Perkalian X_1 dengan sub-kunci pertama
- 2) Penjumlahan X_2 dengan sub-kunci ketiga
- 3) Penjumlahan X_3 dengan sub-kunci kedua
- 4) Perkalian X_4 dengan sub-kunci keempat

Terakhir, keempat sub-blok 16-bit yang merupakan hasil operasi 1), 2), 3), dan 4) ini digabung kembali menjadi blok pesan rahasia 64-bit.

3.3 Proses Dekripsi IDEA

Proses dekripsi menggunakan algoritma yang sama dengan proses enkripsi tetapi 52 buah sub-blok kunci yang digunakan masing-masing merupakan hasil turunan 52 buah sub-blok kunci enkripsi. Tabel sub-blok kunci dekripsi yang diturunkan dari sub-blok kunci enkripsi dapat dilihat pada tabel berikut :

Sub-blok Kunci Enkripsi

Putaran Ke-1	$Z_{11} \ Z_{21} \ Z_{31} \ Z_{41} \ Z_{51} \ Z_{61}$
Putaran Ke-2	$Z_{12} \ Z_{22} \ Z_{32} \ Z_{42} \ Z_{52} \ Z_{62}$
Putaran Ke-3	$Z_{13} \ Z_{23} \ Z_{33} \ Z_{43} \ Z_{53} \ Z_{63}$
Putaran Ke-4	$Z_{14} \ Z_{24} \ Z_{34} \ Z_{44} \ Z_{54} \ Z_{64}$
Putaran Ke-5	$Z_{15} \ Z_{25} \ Z_{35} \ Z_{45} \ Z_{55} \ Z_{65}$
Putaran Ke-6	$Z_{16} \ Z_{26} \ Z_{36} \ Z_{46} \ Z_{56} \ Z_{66}$
Putaran Ke-7	$Z_{17} \ Z_{27} \ Z_{37} \ Z_{47} \ Z_{57} \ Z_{67}$
Putaran Ke-8	$Z_{18} \ Z_{28} \ Z_{38} \ Z_{48} \ Z_{58} \ Z_{68}$
Trnsformasi output	$Z_{19} \ Z_{29} \ Z_{39} \ Z_{49}$

**Tabel sub-blok kunci Dekripsi yang diturunkan
Dari sub-blok kunci enkripsi**

Sub-blok kunci dekripsi

Putaran Ke-1	$(Z_{19})^{-1} \begin{matrix} -Z_{29} & -Z_{39} \\ Z_{58} & Z_{68} \end{matrix} (Z_{49})^{-1}$
Putaran Ke-2	$(Z_{18})^{-1} \begin{matrix} -Z_{38} & -Z_{28} \\ Z_{57} & Z_{67} \end{matrix} (Z_{48})^{-1}$
Putaran Ke-3	$(Z_{17})^{-1} \begin{matrix} -Z_{37} & -Z_{27} \\ Z_{56} & Z_{66} \end{matrix} (Z_{47})^{-1}$
Putaran Ke-4	$(Z_{16})^{-1} \begin{matrix} -Z_{36} & -Z_{26} \\ Z_{55} & Z_{65} \end{matrix} (Z_{46})^{-1}$
Putaran Ke-5	$(Z_{15})^{-1} \begin{matrix} -Z_{35} & -Z_{25} \\ Z_{54} & Z_{64} \end{matrix} (Z_{45})^{-1}$
Putaran Ke-6	$(Z_{14})^{-1} \begin{matrix} -Z_{34} & -Z_{24} \\ Z_{53} & Z_{63} \end{matrix} (Z_{44})^{-1}$
Putaran Ke-7	$(Z_{13})^{-1} \begin{matrix} -Z_{33} & -Z_{23} \\ Z_{52} & Z_{62} \end{matrix} (Z_{43})^{-1}$
Putaran Ke-8	$(Z_{12})^{-1} \begin{matrix} -Z_{32} & -Z_{22} \\ Z_{51} & Z_{61} \end{matrix} (Z_{42})^{-1}$
Trnsformasi output	$(Z_{11})^{-1} \begin{matrix} -Z_{21} & -Z_{31} \\ & (Z_{41})^{-1} \end{matrix}$

Keterangan :

- Z^{-1} merupakan invers perkalian modulo $2^{16}+1$ dari Z ,
dimana $Z Z^{-1} = 1$
- $-Z$ merupakan invers penjumlahan modulo 2^{16} dri Z ,
dimana $Z Z^{-1} = 0$

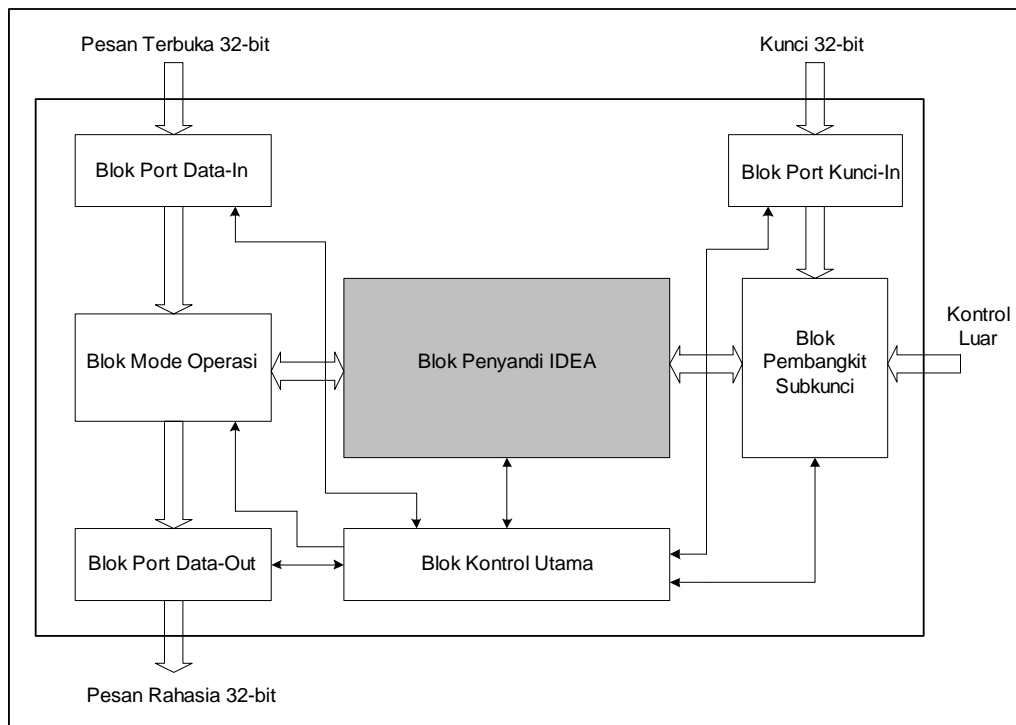
3.4 Pembentukan sub-kunci

Sebanak 52 sub-blok kunci 16-bit untuk proses enkripsi diperoleh dari sebuah kunci 128-bit ilihan pemakai. Blok kunci 128-bit dipartisi menjadi 8 sub-blok kunci 16-bit yang langsung dipakai sebagai 8 sub-blok kunci pertama. Kemudian blok kunci 128-bit dirotasi dari kiri 25 posisi untuk dipartisi lagi menjadi 8 sub-blok kunci 16-bit berikutnya. Proses rotasi dan partisi itu diulangi lagi sampai diperoleh 52 sub-blok kunci 16-bit, dengan urutan sebagai berikut :

$Z_{11} Z_{21} Z_{31} Z_{41} Z_{51} Z_{61}$
 $Z_{12} Z_{22} Z_{32} Z_{42} Z_{52} Z_{62}$
 $Z_{13} Z_{23} Z_{33} Z_{43} Z_{53} Z_{63}$
 $Z_{14} Z_{24} Z_{34} Z_{44} Z_{54} Z_{64}$
 $Z_{15} Z_{25} Z_{35} Z_{45} Z_{55} Z_{65}$
 $Z_{16} Z_{26} Z_{36} Z_{46} Z_{56} Z_{66}$
 $Z_{17} Z_{27} Z_{37} Z_{47} Z_{57} Z_{67}$
 $Z_{18} Z_{28} Z_{38} Z_{48} Z_{58} Z_{68}$
 $Z_{19} Z_{29} Z_{39} Z_{49}$

3.5 Arsitektur umum Processor Kriptografi IDEA

Pada gambar berikut diperlihatkan arsitektur atau penggambaran umum sebuah processor yang mengolah sistem keamanan data dengan menggunakan algoritma IDEA :



Gambar Arsitektur umum Processor IDEA

Keterangan :

1. Blok penyandi IDEA

Blok ini berfungsi untuk melakukan proses penyandian data. Jika sub-kunci yang diproses oleh blok ini berupa sub-kunci enkripsi maka pesan yang dihasilkan adalah pesan rahasia (Chiper teks) dan jika yang diproses berupa sub-kunci dekripsi maka pesan yang dihasilkan adalah pesan sebenarnya (Plain teks).

2. Blok pembangkit sub-kunci

Blok ini berfungsi untuk membentuk 52 buah sub-kunci enkripsi 16 bit dari kunci enkripsi 128 bit membentuk 52 buah sub-kunci dekripsi 16 bit dari kunci dekripsi 128 bit.

3. Blok port data-in

Blok ini berfungsi untuk membaca 2 buah blok data masukan 32 bit dan menyimpannya sebagai blok data

masukan 64 bit yang akan dienkripsi atau didekripsi.

4. Blok poert data-out

Blok ini berfungsi untuk mengeluarkan blok data keluaran 64 bit yang merupakan hasil enkripsi atau dekripsi engan cara membagi menjadi 2 buah ok data keluaran 32 bit.

5. Blok poert kunci-n

Blok ini berfungsi untuk membaca 4 buah blok kunci 32 bit dan menyimpannya sebagai blok kunci 128 bit.

6. Blok mode operasi

Blok ini berfungsi untuk menentukan mode operasi yang digunakan paa prses ekripsi dan dekripsi.

7. Blok kontrol

Blok ini berfungsi untuk mengontrol operasi antara blok fungsional yang menyusun sebuah blok besar seperti sinkronisasi transfer data antar blok.

3.6 Contoh Komputansi Penggunaan Algoritma IDEA

Pada tabel berikut dapat dilihat data hasil enkripsi tiap putaran yang diproses dengan sebuah program yang mengimplementasikan algoritma IDEA utuk sebuah pesan terbuka dalam bentuk bilangan integer **11121314** yng telah dibagi-bagi menjadi empat yaitu $X_1 = Z_{11}$ 11, $X_2 = 12$, $X_3 = 13$, dan $X_4 = 14$, dan kunci telah d Z_{11} dibagi-bagi menjadi $Z_{11} = 2$, $Z_{21} = 4$, $Z_{31} = 6$, $Z_{41} = 8$, $Z_{51} = 10$, $Z_{61} = 12$, $Z_{12} = 14$, $Z_{22} = 16$:

Data hasil enkripsi

Putaran	$X_1=11$	$X_2=12$	$X_3=13$	$X_4=14$
1	1742	1739	1818	1914
2	7747	19997	6873	43941
3	17904	14848	38199	28280
4	19495	50387	56036	37729
5	50786	38066	65017	61306
6	8314	58477	18894	58477
7	33229	58903	41037	5557
8	59491	30519	33083	30571
9	25112	33467	31031	35414

Dari tabel diatas dapat dilihat data hasil enkripsi tiap putaran untuk pesan rahasia, yaitu :

$$Y_1 = 25112, Y_2 = 33467, Y_3 = 3103, Y_4 = 35414$$

Yang dihasilkan oleh proses enkripsi, dengan menggunakan kunci yang diturunkan dari kunci enkripsi dan dengan menggunakan blok dekripsi yang sama dengan proses enkripsi. Terlihat bahwa pesan rahasia telah didekripsi menjadi pesan terbuka sebenarnya seperti tabel berikut:

Putaran	$Y_1=25112$	$Y_2=33467$	$Y_3=31031$	$Y_4=35414$
1	16154	41038	42520	20552
2	11700	19054	58605	20757
3	15054	19054	54450	30993
4	6196	19172	9427	13904
5	7555	38263	14904	29629
6	17706	15065	27165	37202
7	23488	3866	1755	47015
8	22	19	16	112
9	11	12	13	14

Hasil dekripsi akan sesuai dengan pesan asli seperti terlihat pada tabel putaran kesembilan yaitu bilangan integer $Y_1 Y_2 Y_3 Y_4 = X_1 X_2 X_3 X_4 = 11121314$

Bab IV

PENUTUP

Dari uraian diatas secara umum untuk menjaga Keamanan dan kerahasiaan data dalam suatu jaringan komputer, maka diperlukan beberapa jenis enkripsi guna membuat data agar tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali untuk penerima yang berhak. Enkrpsi merupakan salah satu metoda untuk menjamin agar omonikasi menggunakan jaringan komputer menjadi lebih aman.

Bahwa didalam melakukan langkah-langkah enkripsi banyak cara atau algoritma yang tersedia, algoritma IDEA yang dibahas pada makalah ini hanyalah salah satu dari sekian banyak algoritma yang berkembang saat ini. Dan algoritma IDEA ini sampai sekarang masih cukup handal untk diterapkan sebagai metoda pengamanan data.

Pengamanan data tersebut selain bertujuan meningklatkan keamanan data, juga berfungsi untuk :

- Melindungi data agar tidak dapat dibaca oleh orang-orang yan tidak berhak
- Mencegah agar orang-orang yang tidak berhak, menyisipkan atau menghapus data

Dari uraian diatas tentang algoritma IDEA dapat diambil kesimpulan bahwa algoritma tersebut mempunyai keuntungan diantaranya sebagai berikut :

- Algoritma ini menyediakan keamanan yang cukup tinggi yang tidak didasarka atas kerahasiaan algoritmanya akan etapi lebih ditekankan pada keamanan/kerahasiaan kunci yang digunakan
- Dapat dengan mudah untuk dipahami secara penuh

- Algoritma ini dapat digunakan dan dimengerti oleh semua orang
- Algoritma ini sangat layak untuk digunakan sebagai keamanan dalam bidang aplikasi
- Dapat diterapkan dalam bentuk komponen elektronik(Chip) secara ekonomis/relatif murah
- Dapat digunakan secara efisien
- Algoritma ini memungkinkan untuk disebarluaskan keseluruh dunia.

Referensi :

1. P Pflieger, Charles, Security in Computing, Prentice Hall PTR,1996
2. Mark S, Mercow & James Bhreithaupt, Internet the Complete Guide to Security, AMACOM,2000
3. Stalling,William, Ph.D, Network and Internetwork Security Prentice Hall, 1995
4. Kristanto, Andri, Keamanan Data Pada Jaringan Komputer, Gaya Media, 2003
5. <http://WWW.cryptography.com>
6. <http://WWW.bogor.net>