International Data Encryption Algorithm

Brian Al Bahr - 13506093
Jurusan Teknik Informatika, Sekolah Teknik Elektro dan Informatika,
Institut Teknologi Bandung, email : if16093@if.itb.ac.id

Abstract *– Makalah ini membahas tentang pengenalan kriptografi, sejarah singkat kriptografi, dan klasifikasi kriptografi yang lebih dikhususkan lagi pada salah satu bentuk klasifikasinya dalam bentuk algoritma simetris yaitu kriptografi* ***IDEA*** *(International Data Encryption Algorithm) sebagai pokok bahasan dari makalah ini. Pokok bahasan dalam makalah ini memuat antara lain Definisi IDEA, proses enkripsi dan dekripsi IDEA, dan contoh komputansi menggunakan IDEA. Pada bagian lampiran, penulis juga menyertakan program IDEA itu sendiri yang dibuat oleh Fauzan Mirza dari University of London.*

IDEA merupakan sebuah algoritma kriptografi simetrik yang diciptakan pada awalnya sebagai pengganti Data Encryption Standard (DES). IDEA adalalah sebuah revisi kecil dari cipher yang lebih awal, yakni PES (Proposed Encryption Standard). Pada awalnya, IDEA disebut IPES (Improved PES).

Algoritma IDEA terbilang sederhana karena hanya melibatkan 3 proses utama dan 9 putaran, lebih sedikit jika dibandingkan dengan blowfish yang mencapai 16 putaran.

Kata Kunci*: International Data Encryption Algorithm, Xuejia Lai, James Massey, Kriptografi, Enkripsi, Dekripsi*

1. PENDAHULUAN

Sebelum era modern bergulir, kriptografi dianggap semata-mata sebagai mengubah pesan dari bentuk yang dapat dipahami menjadi bentuk yang tidak dapat dipahami dan sebaliknya, membuat pesan tersebut menjadi tidak dapat dipahami oleh pengganggu yang tidak mengetahui rahasianya (kunci yang diperlukan untuk mendekripsi pesan tersebut). Dewasa ini, bidang ini telah berkembang dari sekedar masalah kerahasiaan menjadi sebuah teknik yang bertujuan untuk :

1) Authentication
   Memberikan dua layanan, yakni mengidentifikasikan keaslian suatu pesan dan memberikan jaminan keotentikannya, serta untuk menguji identitas seseorang apabila ia akan memasuki sebuah sistem.

2) Convidentiality
   memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan informasi lewat teknik-teknik enripsi.

3) Message Integrity
   Yaitu memberikan jaminan untuk tiap bagian bahwa esan tidak akan mengalami perubahan dari saat data dibuat/dikirim sampai dengan saat data tersebut dibuka.

4) Non-repudiation
   Yaitu memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apbila ia mencoba menyangkal memiliki dokumen tersebut.

1.1 Sejarah Singkat Kriptografi

Bentuk paling awal kriptografi ada 2 jenis,yakni *transposition ciphers* dan *substitution ciphers* . Bentuk *transposition ciphers* digunakan oleh tentara Sparta pada Zaman Yunani Kuno pada 400 SM. Mereka menggunakan alat yang disebut *Scytale*. Alat ini terdiri dari sebuah pita panjang yang dililitkan pada sebatang slinder. Pesan yang akan dikirimkan ditulis horizontal . Bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun membentuk pesan rahasia.

Gambar 1.1 Scytale

Bentuk *substitution ciphers* (yang mengganti grup huruf dengan grup huruf lain) digunakan oleh Julius Caesar, dikenal dengan nama Caesar cipher dimana tiap huruf didistribusikan dengan huruf ketiga berikutnya. Contoh : '*Fly at once*' menjadi '*Gmz bu podf*'

Seiring berjalannya waktu, kriptografi telah banyak digunakan dalam berbagai bidang, misalnya di bidang religious, digunakan dalam "*The Number of The Beast*", dalam bidang mata-mata, kerahasiaan komunikasi, bahkan kriptografi juga dianjurkan dalam buku "*Kama Sutra*" . Kriptografi juga berperan besar ketika Sekutu memenangkan Perang Dunia II. Ketika itu, *Enigma Machine,* sebuah mesin enkripsi/dekripsi,

digunakan oleh Jerman dalam PD II pada tahun 1920-an sampai akhir perang. Alat itu digunakan untuk menjaga komunikasi sensitif. Memecahkan cipher Enigma ketika itu adalah sebuah faktor yang sangat penting yang berkontribusi dalam kemenangan Sekutu.

Gambar 1.2 Enigma Machine

Perkembangan komputer digital dan elektronika yang begitu pesat memungkinkan pembuatan cipher yang jauh lebih kompleks daripada sebelumnya. Lebih jauh lagi, komputer memungkinkan enkripsi data apa pun yang direpresentasikan oleh komputer sebagai format biner, tidak seperti cipher kuno yang terbatas pada meng-enkripsi teks-teks tertulis. Banyak komputer cipher yang bisa dikarakterisasi oleh operasi bit biner, tidak seperti cipher kuno yang secara umum memanipulasi karakter tradisional secara langsung.

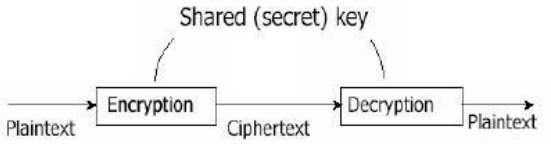
1.2 Klasifikasi Kriptografi

Tingkat keamanan algoritma yang diperoleh dengan menyembunyikan secara rahasia bagaimana algoritma itu bekerja disebut dengan algoritma rahasia(restricted algorithm). Pada awalnya, algoritma jenis ini yang berkembang, namun ternyata algoritma ini memiliki banyak kelemahan, sebagai contohnya adalah seseorang harus menggunakan algoritmanya sendiri, dan jika algoritma ini diketahui orang lain, maka algoritma ini harus diganti dengan yang baru. Kelemahan lainnya adalah tidak memungkinkannya standardisasi sebagai kendala mutu, karena setiap kelompok pengguna harus mempunyai algoritmanya sendiri-sendiri.

Sebagai pemecah masalah tersebut, maka ditemukanlah algoritma kunci, berbeda dengan algoritma rahasia, algoritma ini menggunakan sebuah kunci yang dapat berupa sebarang nilai dari sejumlah angka. Oleh karena itu, algoritma ini dapat dipublikasikan dan dapat diproduksi masal karena tingkat keamanan algoritma ini adalah berdasarkan kerahasiaan kuncinya, bukan algoritmanya. Algoritma ini dibagi menjadi 2 bagian utama, yakni Algoritma Simetris/Privat Key Criptography dan Algoritma Asimaetris/Public Key Criptography.

1.2.1 Privat Key Criptography

Privat Key Criptography ini prinpsip utamanya adalah kunci yang digunakan untuk proses enkripsi sama dengan kunci untuk proses dekripsi K = K1 = K2. Kunci ini harus dirahasiakan. Hanya jenis inilah yang diketahui di depan umum sampai dengan tahun 1976.



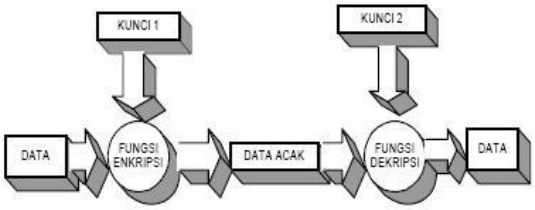
Gambar 1.2.1.1 Privat Key Criptography

Contoh dari kriptografi ini adalah A5, KPD, DES, **IDEA**, LOKI

Prinsip kerja privat key criptography ini adalah pengirim dan penerima sepakat menggunakan sistem kriptografi tertentu dan kunci tertentu. Tingkat keamanan jenis kriptografi ini sangat ditentukan oleh kerahasiaan kunci yang digunakan.

1.2.2 Public Key Criptography

Public Key Criptography ini menggunakan 2 buah kunci, yaitu kunci publik dan kunci rahasia. Untuk mengirim pesan, pengirim meng-enkripsi data dengan menggunakan kunci publik sedangkan penerima menggunakan kunci privat untuk men-dekripsi ciphertext tersebut agar menjadi plaintext yang dapat dipahami isinya.



Gambar 1.2.2.1 Public Key Criptography

Contoh dari kriptografi ini adalah RSA, ACC, dan LUC.

2. KRIPTOGRAFI IDEA

2.1 Deskripsi Algoritma IDEA

Kriptografi IDEA (International Data Encryption Algorithm) diperkenalkan pertama kali tahun 1991 oleh Xuejia Lai dan James L Massey. Algoritma ini dimaksudkan sebagai pengganti DES(Data Encryption Standard). IDEA adalah revisi minor cipher yang lebih awal, yakni PES, dan pada awalnya disebut IPES (Improved PES).

IDEA didesain di bawah kontrak Hasler Foundation. Sandi rahasia ini dipatenkan di banyak negara tapi dapat digunakan secara gratis untuk penggunaan yang tidak komersial. Nama "IDEA" juga dipatenkan dan hak patennya berakhir tahun 2011. Lisensi dari IDEA dipegang oleh MediaCrypt. IDEA digunakan di Pretty Good Privacy (PGP) v2.0 dan sebagai algoritma opsional dalam OpenPGP, Netscape's Secure Socket Layer (SSL), dan Secure Hypertext transfer Protocol (S-HTTP).

Algoritma utama dari sistem kriptografi IDEA adalah sebagai berikut :

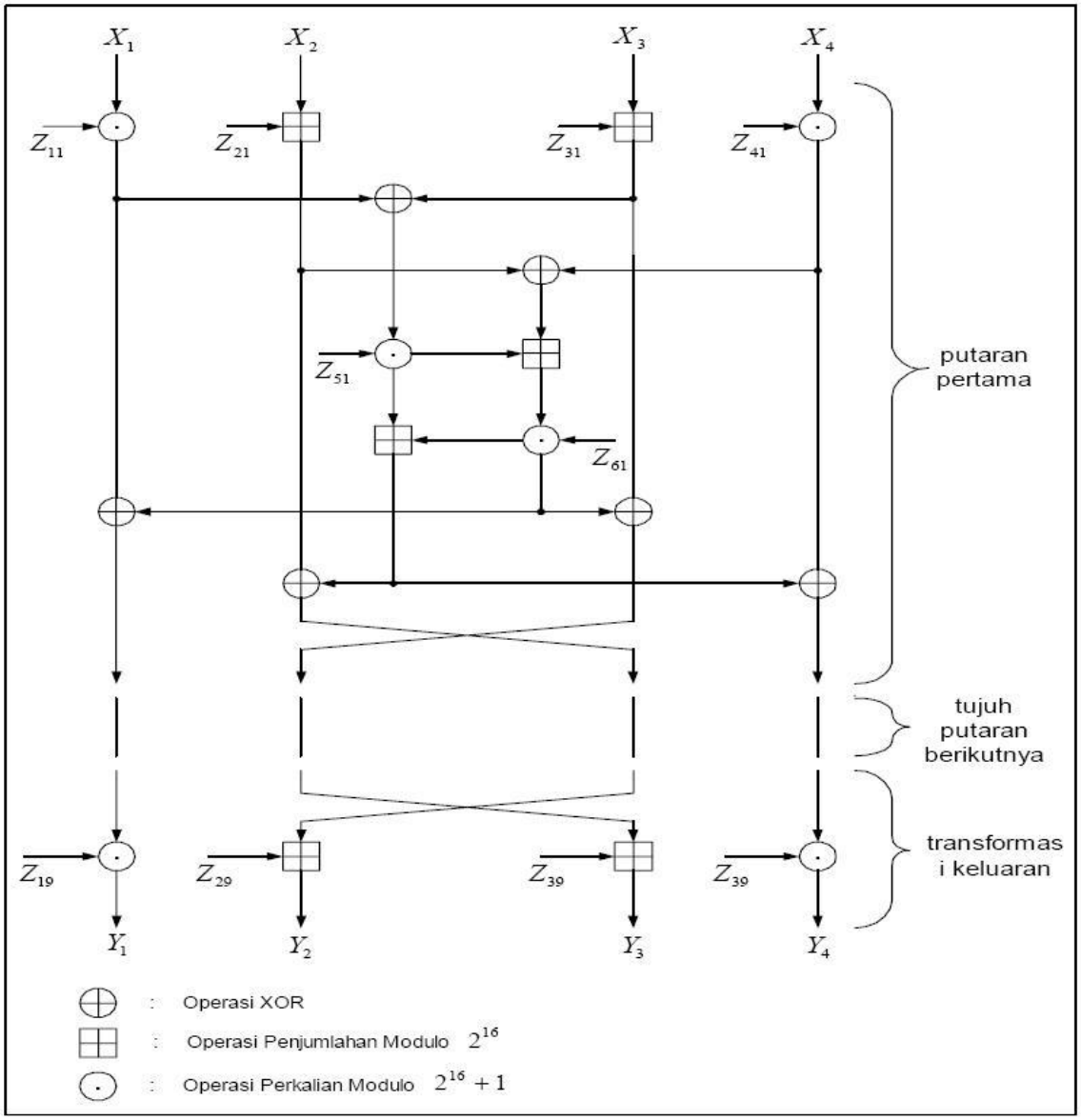
1. Proses Enkripsi : $e_k\ (M) = C$ (1)
2. Proses Dekripsi : $d_k\ (C) = M$ (2)

E : fungsi enkripsi
D : fungsi dekripsi
M : pesan terbuka
C : pesan rahasia
K : kunci enkripsi atau dekripsi

IDEA merupakan algoritma simetris yang beroperasi pada sebuah blok pesan terbuka 64-bit, menggunakan kunci yang sama 128-bit untuk proses enkripsi dan dekripsi. Keluaran dari algoritma ini adalah blok pesan ter-enkripsi 64-bit.

Proses dekripsi menggunakan blok penyandi (algoritma) yang sama dengan proses enkripsi dimana kunci dekripsinya diturunkan dari kunci enkripsi.

IDEA menggunakan proses iterasi yang terdiri dari 8 putaran dan 1 transformasi keluaran pada putaran ke-8,5



Gambar 2.1.1 Algoritma IDEA

Algoritma IDEA ini menggunakan 3 operasi aljabar utama, yakni : Xor, operasi penjmlahan modulo 2^{16} dan operasi perkalian modulo (2^{16} + 1). Operasi ini semuanya dilakukan pada sub-blok 16-bit. IDEA mendapatkan keamanannya dari operasi dari grup yang berbeda – penambahan dan penjumlahan modular serta *exclusive or* dari bit—yang secara aljabar tidak *cocok* dalam beberapa pengertian.

2.2 Proses Enkripsi IDEA

Pada proses enkripsi algoritma ini, terdapat 3 operasi berbeda yang digunakan :

- Xor dari 2 sub blok 16-bit ;bit per bit
- Penjumlahan modulo 2^{16} 2 sub blok 16 bit
- Perkalian modulo (2^{16} + 1) 2 sub blok 16 bit

Blok masukan pesan 64-bit mula-mula dibagi menjadi 4 sub-sub blok 16-bit : X1, X2, X3, X4. Keempat sub-blok 16 bit tadi kemudian ditransformasikan menjadi sub-blok 16 bit, Y1, Y2, Y3, Y4. Semua proses ini berada di bawah kendali 52 sub-blok kunci 16-bit yang dibentuk dari blok kunci 128-bit.

Keempat sub-blok 16-bit X1, X2, X3, X4 digunkan sebagai masukan putaran pertama dari algoritma IDEA. Dapat dilihat dari gambar bahwa dalam setiap putaran dilakukan operasi Xor, penjumlahan modulo dan perkalian modulo. Dari gambar juga terlihat bahwa keluaran dari putaran sebelumnya merupakan masukan dari putaran berikutnya. Hal ini terus berlangsung sampai 8 putaran. Pada putaran terakhir (putaran 8,5) dilakukan transformasi keluaran yang dikendalikan oleh 4 sub-blok kunci 16-bit. Sub kunci diberi simbol Z.

Operasi yang dilakukan pada setiap putaran dapat dirangkum sebagai berikut :

1) Perkalian X1 dengan Z_{11}
2) Penjumlahan X2 dengan Z_{21}
3) Pejumlahan X3 dengan Z_{31}
4) Perkalian X4 dengan Z_{41}
5) Operasi XOR hasil langkah 1) dan 3)
6) Operasi XOR hasil angkah 2) dan 4)
7) Perkalian hasil langkah 5) dengan Z_{51}
8) Penjumlahan hasil langkah 6) dengan langkah 7)
9) Perkalian hasil langkah 8) dengan Z_{61}
10) Penjumlahan hasil langah 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 dari setiap putaran (11), 12) ,13), 14)) menjadi masukan bagi operasi selanjutnya. Pada putaran ke 8,5 dilakukan transformasi keluaran :

1) Perkalian X1 dengan $Z_{1\,8,5}$
2) Penjumlahan X2 dengan $Z_{3\,8,5}$
3) Penjumlahan X3 dengan $Z_{2\,8,5}$
4) Perkalian X4 dengan $Z_{4\,8,5}$

Setelah semua selesai, keempat sub-blok 16-bit yang merupakan keluaran dari 8,5 putaran operasi tadi digabung kembali menjadi blok pesan rahasia 64-bit.

2.3 Proses Dekripsi IDEA

Pada proses dekripsi, IDEA menggunakan algoritma yang sama dengan proses enkripsi namun 52 buah sub-blok kunci yang digunakan merupakan turunan dari 52 buah sub-blok kunci untuk enkripsi. Penurunan kunci dekripsi sebagai 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	$Z_{18}\ Z_{28}\ Z_{38}\ Z_{48}\ Z_{58}\ Z_{68}$
Transformasi output	$Z_{1\,8,5}\ Z_{2\,8,5}\ Z_{3\,8,5}\ Z_{4\,8,5}$

Sub-blok Kunci Dekripsi

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

Pada sub-blok kunci dekripsi, Z^{-1} adalah invers perkalian modulo (2^{16} + 1) dari Z dimana $Z\ Z^{-1} = 1$.

Pada sub-blok kunci dekripsi, -Z adalah invers penjumlahan modulo 2^{16} dari Z dimana $Z\ Z^{-1} = 0$.

2.4 Proses Pembentukan Sub-Kunci

Pada proses enkripsi, 52 sub-blok kunci 16-bit diperoleh dari sebuah kunci 128-bit pilihan pengguna. Blok kunci 128-bit tadi kemudian dipartisi menjadi 8 sub-blok kunci 16-bit yang langsung digunakan sebagai 8 sub-blok kunci pertama. Dari situ kemudian blok kunci 128-bit dirotasi 25 posisi dari kiri untuk kemudian dipartisi lagi menjadi 8 sub-blok kunci 16-bit berikutnya. Proses tersebut terus diulangi sampai diperoleh 52 sub-blok kunci 16-bit. Urutan pembentukan sub-kunci 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}
$Z_{1\,8,5}$ $Z_{2\,8,5}$ $Z_{3\,8,5}$ $Z_{4\,8,5}$

2.5 Contoh Komputasi 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= 11, X_2= 12, X_3 = 13,dan X_4 = 14 , dan kunci telah d ibagi-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 :

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

Gambar 2.4.1 Tabel Komputasi Algoritma IDEA-Enkripsi

Setelah memperhatikan tabel dengan seksama, maka dapat terlihat bahwa hasil enkripsi bilangan integer 11, 12, 13, 14 masing-masing adalah 25112, 3347, 31031, dan 35414. Sekarang mari kita dekripsi hasil yang sudah kita dapat tadi dengan algoritma yang sama tetapi dengan kunci dekripsi yang merupakan kunci enkripsi yang diturunkan.

Setelah meninjau Gambar 2.4.2, maka dapat dilihat bahwa hasil dekripsi dari hasil enkripsi sesuai dengan pesan asli, yakni 11, 12, 13, 14 ; $\mathbf{Y_1\ Y_2\ Y_3\ Y_4 = X_1\ X_2\ X_3\ X_4}$ **= 11121314**

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**

Gambar 2.4.2 Tabel Komputasi Algoritma IDEA-Dekripsi

3. HASIL DAN PEMBAHASAN

Cryptanalys bertujuan menemukan kelemahan atau ketidak-amanan dalam sebuah skema kriptografi, jadi dapat diperbaiki atau menghindari kelemahan tersebut. Cryptanalys mungkin dilakukan oleh penyerang yang berusaha untuk menumbangkan sebuah sistem atau dilakukan oleh desainer sistem untuk mengevalusi apakah sistem yang digunakan tersebut mudah diserang atau tidak.

Para desainer telah melakukan riset dan menganalisis IDEA untuk mengukur kekuatannya terhadap *differential crypanalysis*. Setelah melakukan penelitian panjang, mereka menyimpulkan bahwa algoritma IDEA ini kebal dalam asumsi tertentu.

Tidak ada kelemahan aljabar atau kelemahan linier yang terjadi yang dilaporkan. Beberapa kelas kunci yang lemah memang telah ditemukan, tapi hal ini dalam praktiknya merupakan hal kecil untuk diperhatikan karena sangat jarang sehingga tidak perlu dihindari secara eksplisit. Sampai 2004, serangan terbaik yang menggunakan semua kunci dapat memecahkan IDEA dan menguranginya sampai 5 putaran (yang dalam IDEA aslinya sampai 8,5 putaran).

Bruce Schneier, Seorang kriptografer Amerika, spesialis keamanan komputer, dan penulis , mempunyai gagasan terhadap IDEA dan menulis "*In my opinion, it is the best and most secure block algorithm available to the public at this time*." (*Applied Cryptography*, 2nd ed.)—"*Menurut pendapat saya, IDEA merupakan blok algoritma yang paling baik dan paling aman yang ada saat ini*". Sayangnya, pada tahun 1996, beliau tidak lagi merekomendasikan algoritma ini karena ketersediaan algoritma yang lebih cepat, kemajuan dalam cryptanalys-nya, dan masalah paten IDEA.

4. KESIMPULAN

Kesimpulan yang dapat diambil dari studi dan implementasi International Data Encryption Algorithm antara lain:

1. Banyak fakor yang harus diperhatikan ketika

ingin mengimplementasikan sutu metode enkripsi pada produk software berbasis keamanan. Kecepatan enkripsi , kesederhanaan, kekompakan, keamanan, dan kekuatan kode, kemudahan dalam pengimplementasian, dan lain sebagainya. Salah satu metode atau algoritma yang dapat diandalkan untuk memenuhi segala persyaratan tersebut antara lain adalah IDEA.

2. Round(putaran) enkripsi memegang peranan penting dalam keamanan algoritma IDEA. Jumlah putaran dalam algoritma ini tidak sedikit (8,5 putaran). Sampai saat ini algoritma IDEA ini baru dapat dipecahkan dan dikurangi putarannya sampai dengan 5 putaran.
3. Algoritma ini menyediakan keamanan yang cukup tinggi yang tidak didasarkan atas kerahasiaan algoritmanya akan tetapi lebih ditekankan pada keamanan/kerahasian kunci yang digunakan.
4. Algoritma ini dapat digunakan dan dimengerti oleh semua orang karena operasinya yang sederhana yang hanya menggunakan 3 operasi dasar, yakni Xor, penjumlahan modulo, dan perkalian modulo.

DAFTAR PUSTAKA

[1]. **Munir, Rinaldi.** *Diktat Kuliah Matematika Diskrit*. Bandung : Departemen Teknik Informatika, Institut Teknologi Bandung, 2004.

[2]. Schneier, Bruce. Applied Cryptography 2nd Edition. John Wiley & Sons, Inc. 1999.

[3]. ***http://cypherspace.org/adam/rsa/idea.html***. Tanggal akses : 2 Januari 2008.

[4]. http://dret.net/glossary/idea. Tanggal akses : 27 Desember 2007.

[4]. ***http://en.wikipedia.org/wiki/IDEA***. Tanggal akses : 27 Desembar 2007 .

[5]. ***http://www.answers.com/topic/cryptography-1?cat=biz-fin*****.** Tanggal akses : 27 Desember 2007.

[6]. ***http://www.cert.or.id/~budi/courses/ec7010/dikmenjur/taufik-report.pdf.*** Tanggal akses 23 Desember 2007.

[7]. ***http://www.efymagonline.com/pdf/software.pdf.*** Tanggal akses : 27 Desember 2007.

LAMPIRAN

Pada bagian lampiran ini, penulis menyertakan sebuah software untuk melakukan enkripsi dan deskripsi dari IDEA ini.Program IDEA ini dibuat oleh Fauzan Mirza *dari University of London*. Program ini di-*download* dari situs **http://cypherspace.org/adam/rsa/idea.htm**

Folder program ini terlampir bersama makalah ini dengan nama folder idea3a.zip. Untuk menjalankan program ini mula-mula *un-zip* dulu folder idea3a.zip kemudian ikuti langkah-langkah yang ditulis pembuatnya di file *"readme.txt"*.