KAJIAN TEORITIK KELAS KUNCI LEMAH PADA KRIPTOSISTEM IDEA BERDASARKAN FAKTOR LINEAR DAN KRIPTANALISIS DIFERENSIAL

G. TAUFIK[1], S. GURITMAN[2], B. P. SILALAHI[2]

Abstrak

Pada karya ilmiah ini dilakukan kajian teoretik yang berkaitan dengan konstruksi kelas kunci lemah pada kriptosistem IDEA dan melakukan penegasan terhadap penelitian yang terdahulu. Proses konstruksi kelas kunci lemah dilakukan berdasarkan faktor linear dan kriptanalisis diferensial. Konstruksi kelas kunci lemah berdasarkan faktor linear menghasilkan persamaan linear global yang digunakan untuk menurunkan peluang pemulihan bit-bit yang belum diketahui. Sedangkan konstruksi kelas kunci lemah berdasarkan kriptanalisis diferensial yang pada putaran ke tujuh tidak disyaratkan menghasilkan kelas kunci lemah sebanyak 2^{66}. Penegasan dilakukan dengan cara menurunkan proposisi-proposisi terhadap tabel yang dibuat oleh Daemen dkk.

Kata Kunci: IDEA (*International Data Encryption Algorithm*), kunci lemah, faktor linear, kriptanalisis diferensial.

PENDAHULUAN

Latar Belakang

Kriptografi adalah studi teknik matematik yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, autentikasi entitas, dan autentikasi asal data. Dalam [4] mendefinisikan integritas data adalah suatu layanan yang berkaitan dengan pengubahan data dari pihak-pihak yang tidak berwenang. Dalam kriptografi, cara yang umum untuk mengamankan informasi atau dokumen adalah dengan menyamarkan pesan yang ingin dikirim dengan pesan yang berbeda, kemudian pesan tersebut akan dapat dilihat oleh orang yang memiliki wewenang dengan melakukan proses pembalikan pesan yang telah disamarkan. Proses penyamaran informasi tersebut dikenal dengan kriptosistem.

Kriptosistem adalah suatu sistem yang mengamankan pesan (informasi atau dokumen) dengan menggunakan dua buah kunci yang berbeda. Kunci pertama digunakan untuk proses enkripsi dan kunci kedua untuk proses dekripsi.

[1]Mahasiswa S2, Program Studi Matematika Terapan, Sekolah Pascasarjana IPB Dramaga Bogor, 16680. E-mail: jendral_topik@yahoo.com
[2]Departemen Matematika, Fakultas Ilmu Pengetahuan Alam, Jalan Meranti Kampus IPB Dramaga Bogor, 16680.

Kriptosistem dibagi menjadi dua yaitu kriptosistem simetris dan kriptosistem asimetris. Kriptosistem simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi sedangkan kriptosistem asimetris menggunakan kunci yang berbeda untuk enkripsi dan dekripsi.

Salah satu kriptosistem simetris adalah IDEA (*International Data Encryption Algorithm*). Dalam [4] algoritme IDEA muncul pertama kali pada tahun 1990 yang dikembangkan oleh Xueijia Lai dan James L Massey. Algoritme IDEA merupakan algoritme yang beroperasi dengan blok yang berukuran 64 bit dengan menggunakan kunci yang sama berukuran 128 bit. Algoritme ini menggunakan operasi campuran yaitu operasi perkalian modulo ($2^{16} + 1$), operasi penjumlahan modulo (2^{16}) dan XOR.

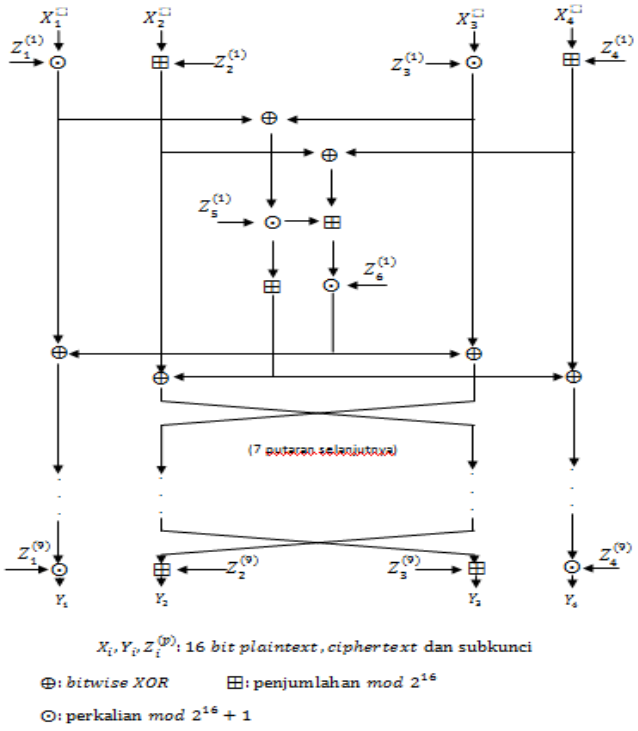
Dalam [2] telah dikaji penyerangan terhadap kriptosistem IDEA yang menghasilkan kunci lemah pada putaran ke delapan kunci 2^{51} dengan bit-bit yang bukan 0 dan masalah kunci lemah dapat dipulihkan dengan memodifikasi *schedule key* pada IDEA yang ide dasarnya adalah mengubah persamaan tak linear (yang melibatkan variabel subblok output, input dan kunci dalam aritmetik modular $\mathbb{Z}_{2^{16}+1}$) menjadi persamaan linear (yang melibatkan variabel bit (dalam $\mathbb{Z}_2$)). Penelitian yang lain melakukan penyerangan terhadap kriptosistem IDEA menghasilkan $2^{53} – 2^{64}$ kunci lemah disajikan pada [1].

Dalam [3] telah dikaji penyerangan terhadap kriptosistem IDEA dengan menguraikan penelitian yang telah dilakukan oleh Biryukov dan menggabungkan dengan serangan Demirci dimana serangan dilakukan seperti pada serangan faktor linear yaitu memerlukan *plaintext* (pesan asli).

Adapun yang menjadi tujuan dari penulisan karya ilmiah ini yaitu: (i) mengkaji proposisi yang terkait dengan konstruksi kelas kunci lemah pada algoritme IDEA; (ii) mengkonstruksi kelas kunci lemah berdasarkan faktor linear dan kriptanalisis diferensial; (iii) melakukan pemulihan kunci-kunci lemah pada algoritme IDEA.

Perumusan Masalah

Berdasarkan apa yang telah diuraikan di atas, maka akan dibahas mengenai bagaimana proses mengkonstruksi kelas kunci lemah algoritme IDEA yang sudah ada terhadap berbagai teknik serangan, jenis serangan yang digunakan dalam penelitian ini adalah faktor linear dan kriptanalisis diferensial serta akan melakukan penegasan yang lebih rinci terhadap penelitian yang telah dilakukan sebelumnya [2]. Proses konstruksi kelas kunci lemah dilakukan untuk para pengguna kriptosistem IDEA dalam mengamankan informasi sehingga ketika posisi kelas kunci lemah sudah diketahui maka pengguna tidak menggunakan kunci lemah. Selain itu juga, penelitian ini akan dibahas pembentukan persamaan yang dapat menurunkan peluang dalam pemulihan nilai bit-bit yang belum diketahui. Kriptosistem IDEA melakukan iterasi yang terdiri dari 8 putaran dan 1 transformasi keluaran pada putaran ke 9, dimana gambaran komputasi dan transformasi keluaran ditunjukkan oleh gambar sebagai berikut :



Gambar 1 Skema kriptosistem IDEA

KRIPTOSISTEM IDEA

Pembentukan Subkunci pada IDEA

Kriptosistem IDEA (*International Data Encryption Algorithm*) yang dikenalkan oleh Menezes dkk [4] adalah kriptosistem simetris yang beroperasi pada sebuah blok pesan terbuka dengan lebar 64 bit dan menggunakan kunci yang sama berukuran 128 bit dalam proses enkripsi dan dekripsi. Proses iterasi pada kriptosistem IDEA terdiri dari 8 putaran dan 1 transformasi output pada putaran ke-9. Kriptosistem IDEA menggunakan operasi campuran yaitu operasi perkalian modulo (2^{16} + 1), operasi penjumlahan modulo (2^{16}) dan XOR.

Dalam [2] telah dikaji proses pembentukan sub-kunci pada IDEA sebagai berikut : sebanyak 52 subblok kunci 16 bit untuk proses enkripsi diperoleh dari sebuah kunci 128 bit. Blok kunci 128 bit dibagi menjadi 8 subblok kunci 16 bit yang langsung dipakai sebagai 8 subblok kunci untuk putaran pertama. Kemudian blok kunci 128 bit dirotasi dari kiri sejauh 25 bit untuk dipartisi lagi menjadi 8 subblok kunci 16 bit berikutnya. Proses tersebut terus berulang sampai diperoleh 52 subblok kunci 16 bit.

Tabel 1
Pembentukan subkunci pada IDEA

Putaran	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6
1	0-15	16-31	32-47	48-63	64-79	80-95
2	96-111	112-127	25-40	41-56	57-72	73-88
3	89-104	105-120	121-8	9-24	50-65	66-81
4	82-97	98-113	114-1	2-17	18-33	34-49
5	75-90	91-106	107-122	123-10	11-26	27-42
6	43-58	59-72	100-115	116-3	4-19	20-35
7	36-51	52-67	68-83	84-99	125-12	13-28
8	29-44	45-60	61-76	77-92	93-108	109-124
9	22-37	38-53	54-69	70-85	-	-

Tabel Daemen dkk

Ide dasar dari penelitian yang dilakukan oleh Daemen dkk [2] adalah mengubah persamaan tak linear (melibatkan variabel subblok input X_1, X_2, X_3, X_4 subblok output Y_1, Y_2, Y_3, Y_4 dan kunci dalam aritmatik modular $\mathbb{Z}_{2^{16}+1}$) menjadi persamaan linear (melibatkan variabel bit $\mathbb{Z}_2$). Dalam [2] telah dikaji tabel-tabel yang menjadi dasar dalam hal penegasan penelitian. Dalam penelitian tersebut telah disyaratkan beberapa subblok tertentu selanjutnya dapat ditunjukkan pada Tabel 2, Tabel 3, Tabel 4 dan Tabel 5.

Tabel 2
Faktor linear pada fungsi putaran

Karakteristik	$\boldsymbol{Z_1}$	$\boldsymbol{Z_4}$	$\boldsymbol{Z_5}$	$\boldsymbol{Z_6}$
$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1}) \Rightarrow (\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	$-$	$(-)1$	$-$	$(-)1$
$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0}) \Rightarrow (\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$-$	$-$	$(-)1$	$(-)1$
$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1}) \Rightarrow (\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	$-$	$(-)1$	$(-)1$	$-$
$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0}) \Rightarrow (\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	$-$	$-$	$-$	$(-)1$
$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1}) \Rightarrow (\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$-$	$(-)1$	$-$	$-$
$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}) \Rightarrow (\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	$-$	$-$	$(-)1$	$-$
$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1}) \Rightarrow (\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$-$	$(-)1$	$(-)1$	$(-)1$
$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0}) \Rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(-)1$	$-$	$(-)1$	$(-)1$
$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1}) \Rightarrow (\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(-)1$	$(-)1$	$(-)1$	$-$
$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}) \Rightarrow (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(-)1$	$-$	$-$	$-$
$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1}) \Rightarrow (\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(-)1$	$(-)1$	$-$	$(-)1$
$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0}) \Rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(-)1$	$-$	$(-)1$	$-$
$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1}) \Rightarrow (\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	$(-)1$	$(-)1$	$(-)1$	$(-)1$
$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0}) \Rightarrow (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(-)1$	$-$	$-$	$(-)1$
$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1}) \Rightarrow (\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(-)1$	$(-)1$	$-$	$-$

Tabel 3
Kondisi bit kunci pada faktor linear (1,0,1,0) → (0,1,1,0)

Putaran	Input XOR	Z_4	Z_5
1	(1,0,1,0)	0 – 14	–
2	(1,1,0,0)	96 – 110	57 – 71
3	(0,1,1,0)	–	50 – 64
4	(1,0,1,0)	82 – 96	–
5	(1,1,0,0)	75 – 89	11 – 25
6	(0,1,1,0)	–	4 – 18
7	(1,0,1,0)	36 – 50	–
8	(1,1,0,0)	29 – 44	93 – 107
9	(0,1,1,0)	–	–

Tabel 4
Propagasi XOR pada fungsi putaran

Karakteristik	Z_1	Z_4	Z_5	Z_6
$(\mathbf{0},\mathbf{0},\mathbf{0},v) \Rightarrow (v,v,v,\mathbf{0})$	–	$(-)1$	–	$(-)1$
$(\mathbf{0},\mathbf{0},v,\mathbf{0}) \Rightarrow (v,\mathbf{0},\mathbf{0},\mathbf{0})$	–	–	$(-)1$	$(-)1$
$(\mathbf{0},\mathbf{0},v,v) \Rightarrow (\mathbf{0},v,v,\mathbf{0})$	–	$(-)1$	$(-)1$	–
$(\mathbf{0},v,\mathbf{0},\mathbf{0}) \Rightarrow (v,v,\mathbf{0},v)$	–	–	–	$(-)1$
$(\mathbf{0},v,\mathbf{0},v) \Rightarrow (\mathbf{0},\mathbf{0},v,v)$	–	$(-)1$	–	–
$(\mathbf{0},v,v,\mathbf{0}) \Rightarrow (\mathbf{0},v,\mathbf{0},v)$	–	–	$(-)1$	–
$(\mathbf{0},v,v,v) \Rightarrow (v,\mathbf{0},v,v)$	–	$(-)1$	$(-)1$	$(-)1$
$(v,\mathbf{0},\mathbf{0},\mathbf{0}) \Rightarrow (\mathbf{0},v,\mathbf{0},\mathbf{0})$	$(-)1$	–	$(-)1$	$(-)1$
$(v,\mathbf{0},\mathbf{0},v) \Rightarrow (v,\mathbf{0},v,\mathbf{0})$	$(-)1$	$(-)1$	$(-)1$	–
$(v,\mathbf{0},v,\mathbf{0}) \Rightarrow (v,v,\mathbf{0},\mathbf{0})$	$(-)1$	–	–	–
$(v,\mathbf{0},v,v) \Rightarrow (\mathbf{0},\mathbf{0},v,\mathbf{0})$	$(-)1$	$(-)1$	–	$(-)1$
$(v,v,\mathbf{0},\mathbf{0}) \Rightarrow (v,\mathbf{0},\mathbf{0},v)$	$(-)1$	–	$(-)1$	–
$(v,v,\mathbf{0},v) \Rightarrow (\mathbf{0},v,v,v)$	$(-)1$	$(-)1$	$(-)1$	$(-)1$
$(v,v,v,\mathbf{0}) \Rightarrow (\mathbf{0},\mathbf{0},\mathbf{0},v)$	$(-)1$	–	–	$(-)1$
$(v,v,v,v) \Rightarrow (v,v,v,v)$	$(-)1$	$(-)1$	–	–

Tabel 5
Propagasi pada *plaintext* XOR (0,*v*,0,*v*) pada IDEA

Putaran	Input XOR	Z_4	Z_5
1	$(0,v,0,v)$	48 – 62	–
2	$(0,0,v,v)$	41 – 55	57 – 71
3	$(0,v,v,0)$	–	50 – 64
4	$(0,v,0,v)$	2 – 16	–
5	$(0,0,v,v)$	123 – 9	11 – 25
6	$(0,v,v,0)$	–	4 – 18
7	$(0,v,0,v)$	84 – 98	–
8	$(0,0,v,v)$	77 – 91	93 – 107
9	$(0,v,v,0)$	–	–

KONSTRUKSI KELAS KUNCI LEMAH

Pada bagian ini dilakukan kajian teoretik tentang konstruksi kelas kunci lemah pada kriptosistem IDEA berdasarkan faktor linear dan kriptanalisis diferensial. Proses konstruksi kelas kunci lemah pada kriptosistem IDEA bertujuan untuk mengetahui titik lemah kriptosistem IDEA terhadap serangan sehingga para pengguna dapat mengidentifikasi kunci lemah tersebut dengan tidak meletakkan informasi pada kunci lemah yang sudah diketahui.

Konstruksi kelas kunci lemah berdasarkan faktor linear

Pada konstruksi kelas kunci lemah berdasarkan faktor linear akan disajikan dasar-dasar linearitas sebagai acuan untuk menurunkan Tabel 2 menjadi proposisi-proposisi yang digunakan untuk menentukan kelas kunci lemah dan pembentukan persamaan linear global.

Hasil kajian teoretik terhadap konstruksi kelas kunci lemah pada kriptosistem IDEA berdasarkan faktor linear disajikan sebagai berikut.

Dasar-dasar linearitas

1. Untuk setiap $X \in \mathbb{Z}_{2^{16}}$ dengan $X \neq 0$ sebagai bitstring 16 bit dan – 1 sebagai bitstring nol 16 bit, maka
$$(-1) \odot X = [(-1) \times X] \bmod (2^{16}+1) - X = \left((2^{16} - 1 - X + 2)\right)$$
$$= (X+2) \bmod 2^{16}$$
2. Jika z adalah LSB (*Least Significant Bit*) dari Z, x adalah LSB dari X, dan y adalah LSB dari $Y = Z \boxplus X$, maka berlaku
$$y = z \oplus x \quad (1)$$
3. Misalkan $Z = (-)1$ diartikan sebagai bitstring 16 bit dengan sifat 15 bit MSB (*Most Significant Bit*) bernilai 0 sedangkan bit LSB bernilai bebas maka nilai $Z = 1$ (ketika LSB bernilai 1) atau $Z = -1$ (ketika LSB bernilai 0). Dalam hal ini, jika z adalah LSB dari Z, x adalah LSB dari X dan y adalah LSB dari $Y = Z \odot X$, maka berlaku
$$y = z \oplus x \oplus 1 \quad (2)$$
Berdasarkan Gambar 1, untuk satu putaran, dinotasikan :
$$T_1 = Z_1 \odot X_1 \; ; \; T_2 = Z_2 \boxplus X_2 \; ; \; T_3 = Z_3 \boxplus X_3 \; ; \; T_4 = Z_4 \odot X_4$$
$$S_1 = T_1 \oplus T_3 \; ; S_2 = T_2 \oplus T_4$$
$$U = Z_5 \odot S_1 \; ; V = U \boxplus S_2$$
$$W = Z_6 \odot V \; ; R = W \boxplus U$$
Akibatnya,
$$Y_1 = T_1 \oplus W \; ; Y_2 = T_3 \oplus W \; ; \; Y_3 = T_2 \oplus R \; ; Y_4 = T_4 \oplus R \quad (3)$$

Berdasarkan Gambar 1, Tabel 2 dan dasar-dasar linearitas di atas, diperoleh 15 proposisi sebagai berikut.

Proposisi 1

Misalkan x_2, x_3, x_4 secara terurut adalah LSB dari X_2, X_3, X_4 dan y_1 adalah LSB dari Y_1 dalam satu putaran. Jika diberikan $Z_4 = (-)1$, $Z_5 = (-)1$ dan $Z_6 = (-)1$ dengan LSBnya z_4, z_5 dan z_6 maka diperoleh persamaan linear

$$y_1 = x_2 \oplus x_3 \oplus x_4 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus 1 \quad (4)$$

Proposisi 2

Misalkan x_1, x_2, x_4 secara terurut adalah LSB dari X_1, X_2, X_4 dan y_2 adalah LSB dari Y_2 dalam satu putaran. Jika diberikan $Z_1 = (-)1$, $Z_4 = (-)1$, $Z_5 = (-)1$ dan $Z_6 = (-)1$ dengan LSBnya z_1, z_4, z_5 dan z_6 maka diperoleh persamaan linear

$$y_2 = x_1 \oplus x_2 \oplus x_4 \oplus z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_6 \quad (5)$$

Proposisi 3

Misalkan x_4 adalah LSB dari X_4 dan y_3 adalah LSB dari Y_3 dalam satu putaran. Jika diberikan $Z_4 = (-)1$ dan $Z_6 = (-)1$ dan dengan LSBnya z_4, z_6 maka diperoleh persamaan linear

$$y_3 = x_4 \oplus z_4 \oplus z_6 \quad (6)$$

Proposisi 4

Misalkan x_2 adalah LSB dari X_2 dan y_4 adalah LSB dari Y_4 dalam satu putaran. Jika diberikan $Z_6 = (-)1$ dengan LSB z_6 maka diperoleh persamaan linear

$$y_4 = x_2 \oplus z_2 \oplus z_6 \oplus 1 \quad (7)$$

Proposisi 5

Misalkan x_1, x_3 adalah LSB dari X_1, X_3 dan y_1, y_2 adalah LSB dari Y_1, Y_2 dalam satu putaran. Jika diberikan $Z_1 = (-)1$ dengan LSB z_1 maka diperoleh persamaan linear

$$y_1 \oplus y_2 = x_1 \oplus x_3 \oplus z_1 \oplus z_3 \oplus 1 \quad (8)$$

Proposisi 6

Misalkan x_2, x_3 adalah LSB dari X_2 , X_3 dan y_1, y_3 adalah LSB dari Y_1, Y_3 dalam satu putaran. Jika diberikan $Z_5 = (-)1$ dengan LSB z_5 maka diperoleh persamaan linear

$$y_1 \oplus y_3 = x_2 \oplus z_2 \oplus x_3 \oplus z_3 \oplus z_5 \oplus 1 \quad (9)$$

Proposisi 7

Misalkan x_3, x_4 adalah LSB dari X_3, X_4 dan y_1, y_4 adalah LSB dari Y_1, Y_4 dalam satu putaran. Jika diberikan $Z_5 = (-)1$ dengan LSB z_5 dan $Z_4 = (-)1$ dengan LSB z_4, maka diperoleh persamaan linear

$$y_1 \oplus y_4 = x_3 \oplus x_4 \oplus z_3 \oplus z_4 \oplus z_5 \quad (10)$$

Proposisi 8

Misalkan x_1 x_2 adalah LSB dari X_1, X_2 dan y_2, y_3 adalah LSB dari Y_2, Y_3 dalam satu putaran. Jika diberikan $Z_1 = (-)1$ dan $Z_5 = (-)1$ dengan LSB masing-masing $z_1$dan z_5, maka diperoleh persamaan linear

$$y_2 \oplus y_3 = x_1 \oplus x_2 \oplus z_1 \oplus z_2 \oplus z_5 \quad (11)$$

Proposisi 9

Misalkan x_1 x_4 adalah LSB dari X_1, X_4 dan y_2, y_4 adalah LSB dari Y_2, Y_4 dalam satu putaran. Jika diberikan $Z_1 = (-)1$, $Z_4 = (-)1$ dan $Z_5 = (-)1$ dengan LSB z_1, z_4 dan z_5, maka diperoleh persamaan linear

$$y_2 \oplus y_4 = x_1 \oplus x_4 \oplus z_1 \oplus z_4 \oplus z_5 \oplus 1 \quad (12)$$

Proposisi 10

Misalkan x_2 x_4 adalah LSB dari X_2, X_4 dan y_3, y_4 adalah LSB dari Y_3, Y_4 dalam satu putaran. Jika diberikan $Z_4 = (-)1$ dengan LSB z_4 , maka diperoleh persamaan linear

$$y_3 \oplus y_4 = x_2 \oplus x_4 \oplus z_3 \oplus z_4 \oplus z_5 \quad (13)$$

Proposisi 11

Misalkan x_1 x_3, x_4 adalah LSB dari X_1, X_3 , X_4 dan y_1, y_2, y_3 adalah LSB dari Y_1, Y_2, Y_3 dalam satu putaran. Jika diberikan $Z_1 = (-)1$, $Z_4 = (-)1$ dan $Z_6 = (-)1$ dengan LSB z_1, z_4, z_6, maka diperoleh persamaan linear

$$y_1 \oplus y_2 \oplus y_3 = x_1 \oplus x_3 \oplus x_4 \oplus z_1 \oplus z_3 \oplus z_4 \oplus z_6 \oplus 1 \quad (14)$$

Proposisi 12

Misalkan $x_1\ x_2, x_3$ adalah LSB dari X_1, X_2, X_3 dan y_1, y_2, y_4 adalah LSB dari Y_1, Y_2, Y_4 dalam satu putaran. Jika diberikan $Z_1 = (-)1$ dan $Z_6 = (-)1$ dengan LSB $z_1$dan z_6, maka diperoleh persamaan linear

$$y_1 \oplus y_2 \oplus y_4 = x_1 \oplus x_2 \oplus x_3 \oplus z_1 \oplus z_2 \oplus z_3 \oplus z_6 \quad (15)$$

Proposisi 13

Misalkan x_1 adalah LSB dari X_1 dan y_2, y_3, y_4 adalah LSB dari Y_2, Y_3, Y_4 dalam satu putaran. Jika diberikan $Z_1 = (-)1$, $Z_5 = (-)1$ dan $Z_6 = (-)1$ dengan LSB z_1, z_5 dan z_6, maka diperoleh persamaan linear

$$y_2 \oplus y_3 \oplus y_4 = x_1 \oplus z_1 \oplus z_5 \oplus z_6 \quad (16)$$

Proposisi 14

Misalkan x_3 adalah LSB dari X_3 dan y_1, y_3, y_4 adalah LSB dari Y_1, Y_3, Y_4 dalam satu putaran. Jika diberikan $Z_5 = (-)1$ dan $Z_6 = (-)1$ dengan LSB masing-masing z_5 dan z_6, maka diperoleh persamaan linear

$$y_1 \oplus y_3 \oplus y_4 = x_3 \oplus z_3 \oplus z_5 \oplus z_6 \quad (17)$$

Proposisi 15

Misalkan x_1, x_2, x_3, x_4 adalah LSB dari X_1, X_2, X_3, X_4 dan y_1, y_2, y_3, y_4 adalah LSB dari Y_1, Y_2, Y_3, Y_4 dalam satu putaran. Jika diberikan $Z_1 = (-)1$ dan $Z_4 = (-)1$ dengan LSB masing-masing $z_1$dan z_4, maka diperoleh persamaan linear

$$y_1 \oplus y_2 \oplus y_3 \oplus y_4 = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus z_1 \oplus z_2 \oplus z_3 \oplus z_4 \quad (18)$$

Persamaan Linear Global

Tabel 3 merupakan contoh untuk faktor linear global (1,0,1,0) → (0,1,1,0) dan sebagai dasar menentukan himpunan kelas kunci global yang beranggotakan 2^{23} bitstring 128 bit dengan posisi bit yang disyaratkan : $b_{0-25} = b_{29-71} = b_{75-110} = 0$ (posisi bit bebas 26-28, 72-74, 111-127). Kelas yang demikian disebut kelas kunci lemah karena setiap anggotanya terkait dengan faktor linear global. Misalkan *plaintext* (X_1, X_2, X_3, X_4) dienkripsi menjadi *ciphertext* (C_1, C_2, C_3, C_4) menggunakan kunci global yang disyaratkan berdasarkan Tabel 3.

Berikut ini ditentukan persamaan linear global antara c_2, c_3, x_1, x_3 (variabel LSB dari C_2, C_3, X_1, X_3) dan beberapa posisi bit dari subkunci. Berdasarkan

Gambar 1, Tabel 2 dan beberapa proposisi dapat disusun persamaan linear global sebagai berikut

$$c_2 \oplus c_3 = x_1 \oplus x_3 \oplus b_{111} \oplus b_{127} \oplus b_{72} \oplus b_{120} \oplus b_{26} \oplus b_{74} \oplus b_{115} \oplus 1 \quad (19)$$

Konstruksi kelas kunci lemah berdasarkan kriptanalisis diferensial

Dalam [2] telah membuat tabel propagasi XOR pada setiap fungsi putaran dimana digunakan untuk menentukan kelas kunci lemah berdasarkan kriptanalisis diferensial. Pada bagian ini akan disajikan proposisi-proposisi yang berkaitan dengan propagasi XOR pada putaran dengan syarat tertentu untuk menentukan kelas kunci lemah.

Berdasarkan Gambar 1, dalam suatu putaran, misalkan pasangan input $X = (X_1, X_2, X_3, X_4)$ dan $X^* = ({X_1}^*, {X_2}^*, {X_3}^*, {X_4}^*)$ dinotasikan sebagai berikut

$$X' = X \oplus X^* \Leftrightarrow$$
$${X_1}^*, {X_2}^*, {X_3}^*, {X_4}^* = (X_1 \oplus {X_1}^*, X_2 \oplus {X_2}^*, X_3 \oplus {X_3}^*, X_4 \oplus {X_4}^*)$$

Jika pasangan input $Y = (Y_1, Y_2, Y_3, Y_4)$ dan $Y^* = ({Y_1}^*, {Y_2}^*, {Y_3}^*, {Y_4}^*)$ dinotasikan sebagai berikut

$$Y' = Y \oplus Y^* \Leftrightarrow$$
$${Y_1}^*, {Y_2}^*, {Y_3}^*, {Y_4}^* = (Y_1 \oplus {Y_1}^*, Y_2 \oplus {Y_2}^*, Y_3 \oplus {Y_3}^*, Y_4 \oplus {Y_4}^*)$$

Untuk pasangan $X, X^* \in \mathbb{Z}_{2^{16}}$ dinotasikan $X' = X \oplus X^*$ dan $v = 2^{15} \in \mathbb{Z}_{2^{16}}$ maka berlaku :

1. Jika $X' = 0$ (berarti $X = X^*$) dan untuk setiap $Z \in \mathbb{Z}_{2^{16}}$, didefinisikan $Y = X \boxplus Z$ dan $Y^* = X^* \boxplus Z$ maka $Y' = Y \oplus Y^* = 0 \Leftrightarrow Y = Y^*$
2. Jika $X' = 0$ (berarti $X = X^*$) dan untuk setiap $Z \in \mathbb{Z}_{2^{16}}$, didefinisikan $Y = X \odot Z$ dan $Y^* = X^* \odot Z$ maka $Y' = Y \oplus Y^* = 0 \Leftrightarrow Y = Y^*$
3. Jika $X' = v$ dan untuk setiap $Z \in \mathbb{Z}_{2^{16}}$, didefinisikan $Y = X \boxplus Z$ dan $Y^* = X^* \boxplus Z$ maka $Y' = Y \oplus Y^* = v$
4. Jika $X' = v$ dan untuk setiap $Z \in \mathbb{Z}_{2^{16}}$, didefinisikan $Y = X \odot Z$ dan $Y^* = X^* \odot Z$ maka $Y' = Y \oplus Y^* \neq v$
5. Jika $X' = v$ dan untuk $Z = (-)1$, didefinisikan $Y = X \odot Z$ dan $Y^* = X^* \odot Z$ maka $Y' = Y \oplus Y^* = v$

Berdasarkan penotasian di atas, Gambar 1 dan Tabel 4, maka didapatkan 15 proposisi yang terkait dengan sifat beda input dan output suatu putaran sebagai berikut.

Proposisi 16

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (0,0,0,v)$ dan disyaratkan $Z_4 = Z_6 = (-)1$ maka $Y' = (v, v, v, 0)$.

Proposisi 17

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (0,0,v,0)$ dan disyaratkan $Z_5 = Z_6 = (-)1$ maka $Y' = (v,0,0,0)$.

Proposisi 18

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (0,0,v,v)$ dan disyaratkan $Z_4 = Z_5 = (-)1$ maka $Y' = (0,v,v,0)$.

Proposisi 19

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (0,v,0,0)$ dan disyaratkan $Z_6 = (-)1$ maka $Y' = (v,v,0,0)$.

Proposisi 20

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (0,v,0,v)$ dan disyaratkan $Z_4 = (-)1$ maka $Y' = (0,0,v,v)$.

Proposisi 21

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (0,v,v,0)$ dan disyaratkan $Z_5 = (-)1$ maka $Y' = (0,v,0,v)$.

Proposisi 22

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (0,v,v,v)$ dan disyaratkan $Z_4 = Z_5 = Z_6 = (-)1$ maka $Y' = (v,0,v,v)$.

Proposisi 23

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (v,0,0,0)$ dan disyaratkan $Z_1 = Z_5 = Z_6 = (-)1$ maka $Y' = (0,v,0,0)$.

Proposisi 24

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (v,0,0,v)$ dan disyaratkan $Z_1 = Z_4 = Z_5 = (-)1$ maka $Y' = (v,0,v,0)$.

Proposisi 25

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (v,0,v,0)$ dan disyaratkan $Z_1 = (-)1$ maka $Y' = (v,v,0,0)$.

Proposisi 26

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (v, 0, v, v)$ dan disyaratkan $Z_1 = Z_4 = Z_6 = (-)1$ maka $Y' = (0,0, v, 0)$.

Proposisi 27

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (v, v, 0,0)$ dan disyaratkan $Z_1 = Z_5 = (-)1$ maka $Y' = (v, 0,0, v)$.

Proposisi 28

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (v, v, 0, v)$ dan disyaratkan $Z_1 = Z_4 = Z_5 = Z_6 = (-)1$ maka $Y' = (0, v, v, v)$.

Proposisi 29

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (v, v, v, 0)$ dan disyaratkan $Z_1 = Z_6 = (-)1$ maka $Y' = (0,0,0, v)$.

Proposisi 30

Berdasarkan Gambar 1, dalam satu putaran, jika $X' = (v, v, v, v)$ dan disyaratkan $Z_1 = Z_4 = (-)1$ maka $Y' = (v, v, v, v)$.

PEMULIHAN BIT-BIT KUNCI LEMAH

Pada bagian ini akan disajikan hasil penelitian yang berkaitan dengan pemulihan bit-bit kelas kunci lemah sehingga para pengguna dapat memilih bit-bit yang tidak termasuk dalam kelas kunci lemah. Berdasarkan Tabel 5 bahwa bit-bit kunci yang sudah ditetapkan bernilai "0" adalah posisi 0 – 25, 41 – 71, 77 – 107, dan 123 – 127 sedangkan bit-bit yang belum diketahui ada sebanyak 35 bit yaitu pada posisi 26 – 40, 72 – 76, dan 108 – 122. Masalah selanjutnya adalah menentukan bit-bit yang belum diketahui tersebut, kemudian akan dipulihkan menggunakan metode *brute force*. Bit-bit yang dipulihkan dari percobaan yang dilakukan disajikan pada tabel.

Tabel 6
Pemulihan bit-bit kelas kunci lemah pada putaran ke-9

Posisi bit dari kunci global	Bit yang bernilai "0"	Bit yang akan dipulihkan	Bit yang belum dipulihkan
$\boldsymbol{Z_1^{(9)}}$ = 22 – 37	22 – 25	26 – 37	38 – 40; 72 – 76; 108 – 122

$\boldsymbol{Z_2^{(9)}}$ = 38 – 53	41 – 53	38 – 40	72 – 76; 108 – 122
$\boldsymbol{Z_3^{(9)}}$ = 54 – 69	54 – 69	–	–
$\boldsymbol{Z_4^{(9)}}$ = 70 – 85	70 – 71; 77 – 85	72 – 76	108 – 122
$\boldsymbol{Z_6^{(8)}}$ = 109 – 124	123 – 124	109 – 122	108

Tabel 7
Pemulihan bit-bit kelas kunci lemah ketika putaran ke-8 tidak disyaratkan

Posisi bit dari kunci global	Bit yang bernilai "0"	Bit yang akan dipulihkan	Bit yang belum dipulihkan
$\boldsymbol{Z_1^{(9)}}$ = 22 – 37	22 – 25	26 – 37	38 – 40; 72 – 83; 99 – 122
$\boldsymbol{Z_2^{(9)}}$ = 38 – 53	41 – 53	38 – 40	72 – 83; 99 – 122
$\boldsymbol{Z_3^{(9)}}$ = 54 – 69	54 – 69	–	–
$\boldsymbol{Z_4^{(9)}}$ = 70 – 85	70 – 71; 84 – 85	72 – 83	99 – 122

Tabel 8
Pemulihan bit-bit kelas kunci lemah ketika putaran ke-7 tidak disyaratkan

Posisi bit dari kunci global	Bit yang bernilai "0"	Bit yang akan dipulihkan	Bit yang belum dipulihkan
$\boldsymbol{Z_1^{(9)}}$ = 22 – 37	22 – 25	26 – 37	38 – 40; 72 – 122
$\boldsymbol{Z_2^{(9)}}$ = 38 – 53	41 – 53	38 – 40	72 – 122
$\boldsymbol{Z_3^{(9)}}$ = 54 – 69	54 – 69	–	–
$\boldsymbol{Z_4^{(9)}}$ = 70 – 85	70 – 71	72 – 85	86 – 122

Berdasarkan pada Tabel 5 dan Tabel 7 dapat dilihat bit-bit kunci yang sudah ditetapkan bernilai "0" adalah posisi 0 – 25, 41 – 71, 84 – 98 dan 123 – 127, sedangkan bit-bit yang belum diketahui ada sebanyak 51 bit yaitu 26 – 40, 72 – 83 dan 99 – 122. Artinya ketika putaran ke delapan pada Tabel 5 tidak disyaratkan dengan menggunakan metode *brute force* maka mampu menurunkan peluang menebak kunci pada kriptosistem IDEA sebesar 2^{-51}. Selanjutnya pada Tabel 5 dan Tabel 8 dapat dilihat bit-bit kunci yang sudah ditetapkan bernilai "0" adalah posisi 0 – 25, 41 – 71 dan 123 – 127, sedangkan bit-bit yang belum diketahui ada sebanyak 66 bit yaitu 26 – 40 dan 72 – 122. Artinya ketika putaran ke tujuh pada Tabel 5 tidak disyaratkan dengan menggunakan metode *brute force* maka mampu menurunkan peluang menebak kunci pada kriptosistem IDEA sebesar 2^{-66}.

SIMPULAN

Berdasarkan hasil kajian teoretik terhadap kriptosistem IDEA dihasilkan proposisi-proposisi yang berkaitan dengan kelas kunci lemah pada kriptosistem IDEA dimana proposisi merupakan penurunan dari tabel yang dibuat oleh Daemen.

Berdasarkan hasil konstruksi kelas kunci lemah pada kriptosistem IDEA dengan menggunakan faktor linear, diperoleh persamaan linear global yaitu :
$c_2 \oplus c_3 = {y_1}^{(1)} \oplus {y_3}^{(1)} \oplus b_{111} \oplus b_{127} \oplus b_{72} \oplus b_{120} \oplus b_{26} \oplus b_{74} \oplus b_{115} \oplus 1$
Variabel cipherteks c_2 dan c_3 merupakan variabel LSB dari cipherteks C_2 dan C_3. Sedangkan hasil konstruksi kunci lemah pada kriptosistem IDEA dengan menggunakan kriptanalisis diferensial yang pada putaran ke tujuh pada Tabel 5 tidak disyaratkan dengan menggunakan metode *brute force* diperoleh kelas kunci lemah sebanyak 66 sehingga mampu menurunkan peluang menebak kunci sebesar 2^{-66}.

DAFTAR PUSTAKA

[1] Biryukov A, Govaerts R, Vanderwalle J. 2002. New Weak-Key Classes of IDEA. *Appread in Information and Communications Security, 4th International Conference. Springer – Verlag*, 315 – 326.

[2] Daemen J, Govaerts R, Vanderwalle J. 1993. Weak Key for IDEA. *Appread in Advances in Cryptology, Springer - Verlag*. 224 – 231.

[3] Nakahara JJ, Preneel B, Vanderwalle J. 2006. The Biryukov-Demirci Attack on IDEA and MESH Ciphers. *ACIP, Springer – Verlag*, 98 – 109.

[4] Menezes A, Oorschot PC, Vanstone SA. 1996. *Handbook of Applied Cryptography*. Florida, CRC Press.