STUDI MENGENAI KRIPTANALISIS UNTUK BLOCK CIPHER DES DENGAN TEKNIK DIFFERENTIAL DAN LINEAR CRYPTANALYSIS

Luqman Abdul Mushawwir – NIM 13507029

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung
E-Mail: abdulmushawwir@gmail.com

ABSTRAK

Salah satu metode kriptografi yang pernah sangat populer saat ini adalah DES, yaitu Data Encryption Standard, yang merupakan salah satu terapan dari block cipher. Block cipher sendiri adalah satu metode kriptografi yang masih sering digunakan, bahkan dalam pengembangan DES sendiri, seperti Triple DES, DES-X, AES dan lain-lain. DES sendiri dikembangkan karena seiring perkembangan zaman, DES diketahui memiliki kelemahan-kelemahan.

Beberapa teknik yang dipakai untuk menyerang DES dan membuktikan DES sudah tidak aman lagi, di antaranya adalah *differential cryptanalyisis* dan *linear cryptanalysis*. *Differential cryptanalysis* menyerang DES dengan memanfaatkan pola perbedaan antara masukan dan keluaran. *Linear cryptanalysis* menyerang DES dengan memanfaatkan keuntungan tingginya kemunculan ekspresi linear yang melibatkan bit dari plainteks, cipherteks dan upakunci (*subkey*).

Makalah ini akan menggali dan menerapkan metode kriptanalisis *differential cryptanalysis* dan *linear cryptanalysis* pada DES. Di sini akan dijelaskan mengenai langkah-langkah yang digunakan pada pembuatan DES, masing-masing metode kriptanalisis, serta akan dipaparkan mengenai perbandingan dari kedua serangan dalam menyerang algoritma DES.

Kata Kunci: Block cipher, DES, differential cryptanalysis, linear cryptanalysis

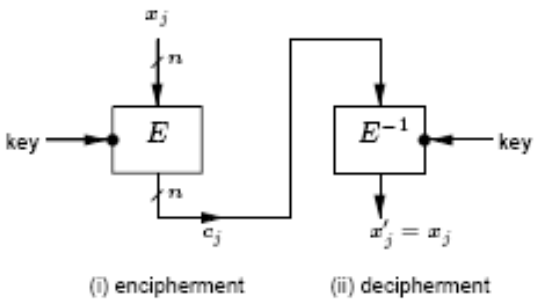
1. PENDAHULUAN

1.1 Block Cipher

Sebuah block cipher n-bit adalah sebuah cipher yang beroperasi di sebuah plainteks yang telah dibagi menjadi beberapa blok bit dengan panjang satu blok adalah n bit. Blok-blok plainteks tersebut dienkripsi dengan kunci yang mempunyai panjang sama dengan blok plainteksnya. Block cipher mempunyai beberapa skema, yaitu:

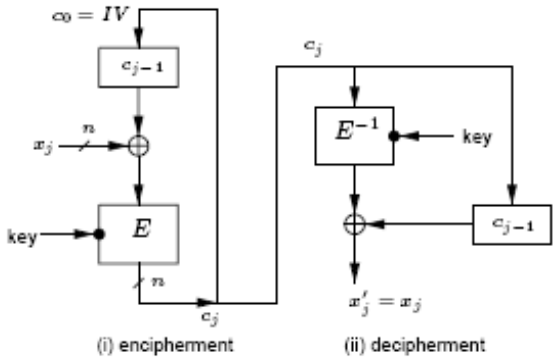
- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback (CFB)
- Output Feedback (OFB)

ECB mempunyai skema sebagai berikut:



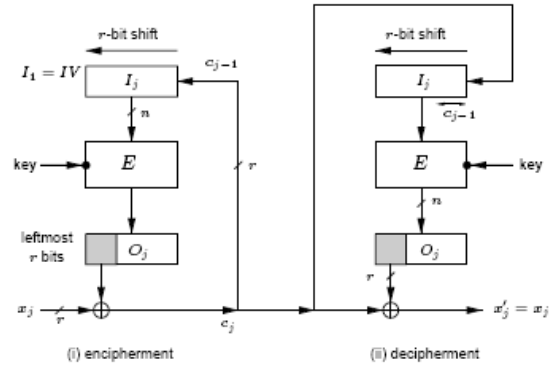
Gambar 1. Skema ECB

CBC mempunyai skema sebagai berikut:



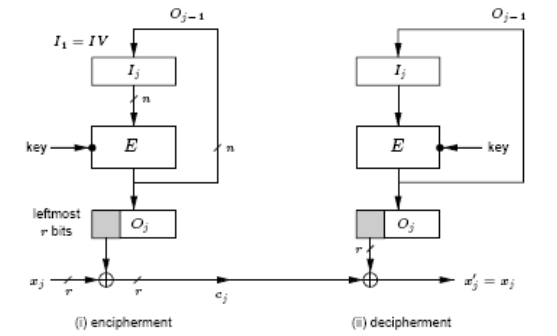
Gambar 2. Skema CBC

CFB mempunyai skema sebagai berikut:



Gambar 3. Skema CFB

OFB mempunyai skema sebagai berikut:



Gambar 4. Skema OFB

Data Encryption Standard (DES)

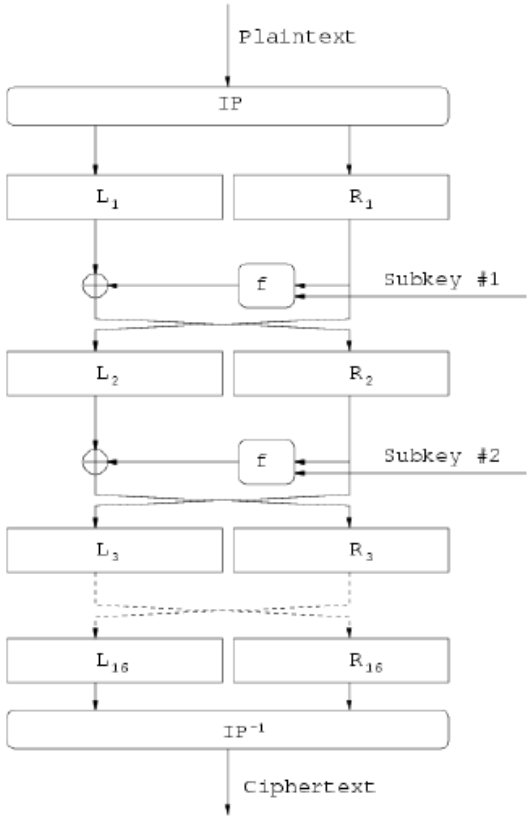
DES merupakan block cipher kunci-simetri yang paling diketahui di seluruh dunia. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan 56 bit kunci internal yang dibangkitkan oleh 64 bit kunci eksternal.

Skema umum DES adalah sebagai berikut:

1. Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).

2. Pada hasil permutasi awal kemudian dilakukan proses enkripsi sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.

3. Hasil proses enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers *initial permutation* atau IP^{-1}) menjadi blok cipherteks.



Gambar 5. Skema umum DES

1.2 Kriptanalisis

Kriptanalisis yang akan dipakai untuk mengkriptanalisis DES dan FEAL adalah kriptanalisis sebagai berikut.

1. Linear Cryptanalysis

Linear Cryptanalysis adalah sebuah *chosen-plaintext attack* yang dibuat oleh Matsui dan Yamagashi yang pertama kali dibuat untuk menyerang algoritma FEAL. Setelah sukses menyerang FEAL, metode ini digunakan oleh Matsui untuk menyerang algoritma DES.

Serangan ini memerlukan 2^{43} plainteks yang diketahui dan cipherteks yang berkoresponden dengannya.

Linear Cryptanalysis bekerja dengan memodelkan komponen non-linear pada sebuah cipher dengan aproksimasi mendekati linear. Dengan aproksimasi yang baik, sebuah fungsi mendekati linear mengaproksimasi fungsi orijinal dengan probabilitas $p = 0.5 + \varepsilon$ dengan $|\varepsilon|$ sebesar mungkin.
Jika $(a, b) \epsilon$ GF(2)^n x GF(2)^n adalah sebuah pasangan dengan $a \neq 0$ sebagai *input mask* dan *b* sebagai *output mask*. Probabilitas linear (LP) untuk (*a, b*) adalah sebagai berikut:

$$LP(a, b) = (2 \cdot \Pr_X \{(a, X) = (b, \rho(X))\} - 1)^2 \quad ...(1)$$

Vektor dari *mask* A = $(a_1, ..., a_{r+1})$ dengan $a_i \neq 0$ dan $1 \leq i \leq r$ disebut *karakterisitik linear* dari sebuah cipher.

Matsui kemudian membuat sebuah Lemma, yang disebut Piling-Up Lemma. Asumsikan $X_1, ..., X_n$ variabel random yang merepresentasikan bit dan $\varepsilon_1, ..., \varepsilon_n$ adalah simpangannya. Kemudian, simpangan tersebut bisa kita hitung dengan berikut:

$$\varepsilon = 2^{n-1} \prod_{i=1}^{n} \varepsilon_i \quad (2)$$

Dengan menggunakan Piling-Up Lemma, kita dapat mengestimasi kemungkinan suksesnya serangan dengan linear cryptanalysis. Jika kemungkinan untuk setiap aproksimasinya diketahui.

2. Differential Cryptanalysis

Differential cryptanalysis merupakan sebuah *chosen-plaintext attack* yang pertama kali dibuat untuk menyerang block cipher FEAL. Dengan mengenkripsi sepasang plainteks yang dipilih secara hati-hati kepada cipherteks dengan kunci yang sama, penyerang dapat memprediksi apakah bit-bit dari input sampai akhir sama atau tidak. Ini didapat dengan menggunakan pola diferensiasi pada input.

Dengan persamaan *f : GF(2)^n -> GF(2)^n* yang merupakan fungsi vectorial boolean, pola diferensiasi adalah sebagai berikut:

Sebuah pola diferensiasi untuk *f* adalah sebuah tuple (Δ_I, Δ_O), yang untuk sebuah input Δ_I diferensiasi output $f(x) + f(x + \Delta_I)$ mungkin dapat mempunyai nilai Δ_O.

Biasanya, pola diferensiasi hanya didefinisikan pada lingkaran transformasi. Untuk mengikuti jalur dari pola diferensiasi, sebuah "karakteristik" didefinisikan sebagai berikut:

Sebuah karakteristik *r*-putaran adalah sebuah tuple $(r + 1)$ dari pola differensiasi $(\Lambda_1, ... ,\Lambda_{r+1})$. Untuk karakteristik satu putaran, probabilitas sebuah diferensiasi di input dari putaran menghasilkan diferensiasi output yang telah dijelaskan sebelumnya disebut probabilitas dari karakteristik, untuk sebuah fungsi *f : GF(2)^n -> GF(2)^n*.

Jika X menotasikan sebuah variabel random yang terdistribusi dalam GF(2)^n, probabilitas diferensial untuk pasangan $(\Delta_I, \Delta_O) \epsilon$ GF(2)^n x GF (2)^n dengan $\Delta_I \neq 0$, didefinisikan sebagai berikut:

$$DP(\Delta_I, \Delta_O) = \Pr_X \{\rho(X) + \rho(X + \Delta_I) = \Delta_O\} \quad ...(3)$$

Dengan asumsi nilai input untuk setiap putaran terdistribusi secara acak dan independen satu sama lain, probabilitas untuk karakteristik *r*-putaran sama dengan probabilitas untuk karakteristik satu putaran.

Diferensial didefinisikan sebagai berikut. Sebuah diferensial *r*-putaran adalah sebuah tuple (Δ_I, Δ_O) dengan Δ_I adalah perbedaan input dan Δ_O adalah perbedaan output setelah *r* putaran.

Setelah mendapatkan diferensial dari cipherteks dan plainteks yang dipilih, kita menganggap diferensial tersebut adalah perbedaan di dalam S-Box untuk mendapatkan bit-bit kunci.

2. PEMBAHASAN

2.1 DES yang Digunakan

DES yang digunakan pada pembahasan kali ini adalah DES dengan mode penerapan ECB, karena penerapan DES dengan mode ECB lebih sederhana.

Pengenkripsian plainteks dengan DES dengan langkah-langkah sebagai berikut:

- Kunci ditentukan oleh pengguna
- Pembangkitan matriks *initial permutation* (IP) dan invers *initial permutation* (IP^{-1})
- Melakukan permutasi kepada plainteks dengan menggunakan IP
- *Enciphering* plainteks dengan 16 putaran jaringan feistel dengan fungsi: $L_i = R_{-1}$ dan $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ dengan pembangkitan kunci internal di setiap putarannya dengan matriks-matriks permutasi kompresi
- Melakukan permutasi lagi pada hasil *enciphering* dengan menggunakan IP^{-1} menghasilkan cipherteks yang diinginkan

Sedangkan fungsi *f* pada jaringan feistel adalah sebagai berikut:

- R_{i-1} diekspansi menjadi 48 bit dengan matriks permutasi ekspansi.
- Hasil ekspansi di-XOR-kan dengan kunci internal yang dibangkitkan pada putaran itu, menghasilkan vektor *A*.
- Vektor *A* dibagi menjadi 8 bagian, masing-masing 6 bit, dan menjadi masukan untuk matriks substitusi menjadi vektor *B*.
- Hasil substitusi tersebut dipermutasi oleh sebuah matriks *P* menjadi vektor *P*(*B*).
- *P*(*B*) di-*XOR*-kan dengan L_{i-1} menghasilkan R_i: $R_i = L_{i-1} \oplus P(B)$

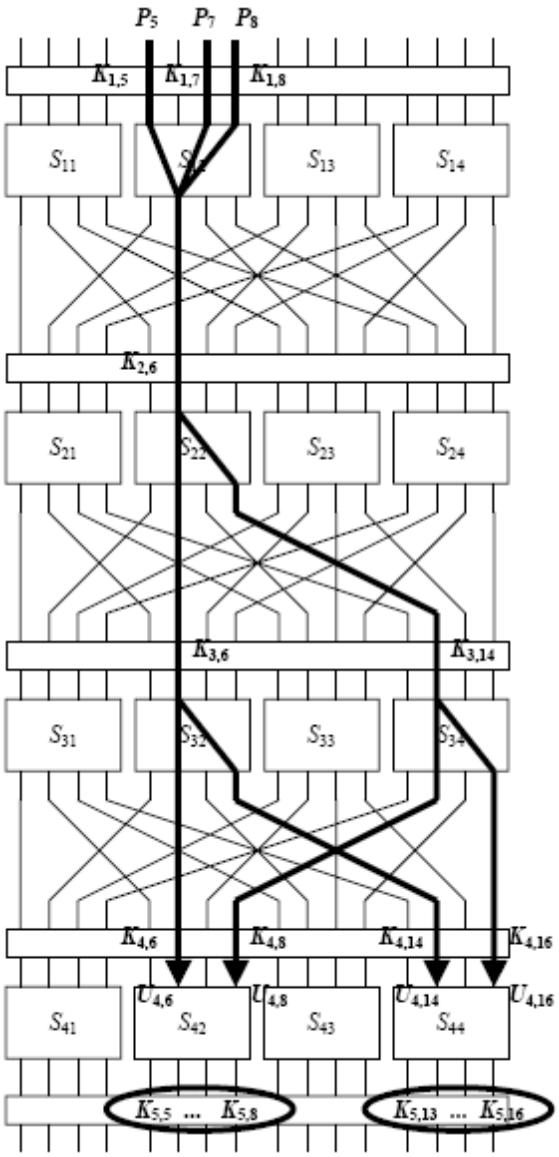
Setelah semua proses di atas, didapatkan cipherteks yang diinginkan.

2.2 Penerapan *Linear Cryptanalysis* pada Algoritma DES

Penerapan *Linear Cryptanalysis*

Linear Cryptanalysis yang dilakukan pada DES yang telah dibuat dilakukan dengan langkah-langkah sebagai berikut:

1. Melakukan aproksimasi linear sebanyak *r*-1 putaran pada *r* putaran cipher dengan bagan sebagai berikut:



Gambar 6. Satu putaran aproksimasi linear dari S-Box

Dari aproksimasi linear di atas didapat:

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_K = 0. \quad (4)$$

dimana

$$\Sigma_K = K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} \oplus K_{4,6} \oplus K_{4,8} \oplus K_{4,14} \oplus K_{4,16} \quad (5)$$

Σ_K adalah 0 atau 1, tergantung dari kunci pada tiap-tiap putarannya. Dengan menggunakan Piling-Up Lemma, didapat probabilitas untuk ekspresi di atas adalah $\frac{1}{2} + 2^3(3/4 - 1/2)(1/4\text{-}1/2)^3 = 15/32$

Ketika Σ_K sudah diketahui, kita mengetahui bahwa

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0 \quad (6)$$

harus mempunyai probabilitas sebesar 15/32 atau (1-15/32) = 17/32, tergantung dari nilai Σ_K adalah 0 atau 1.

2. Mengekstrak bit-bit kunci dari cipherteks dan plainteks yang sudah diketahui sebelumnya, yaitu dengan mengetahui bit-bit subkunci terakhir. Ekspresi linear (6) mempengaruhi masukan dari S_{42} dan S_{44} di putaran terakhir.

Untuk setiap sampel plainteks dan cipherteks, kita mencoba semua dari 256 nilai dari subkey parsial [$K_{5,5}$...$K_{5,8}$, $K_{5,13}$...$K_{5,16}$]. Untuk setiap nilai subkunci, kita akan menginkremen hitungan setiap persamaan (6) bernilai *true*, dimana kita menentukan nilai dari [$U_{4,5}$...$U_{4,8}$, $U_{4,13}$...$U_{4,16}$] dengan menjalankan data mundur melalui subkunci parsial target dan kotak-S S_{42} dan S_{44}.

Setelah menyimulasikan penyerangan dengan membangkitkan 10000 nilai plainteks/cipherteks yang diketahui, dan dari proses kriptanalisis sebelumnya, didapat nilai subkunci parsial [$K_{5,5}$...$K_{5,8}$] adalah [0010] dan [$K_{5,13}$...$K_{5,16}$] adalah [0100], dengan perhitungan simpangan sebagai berikut:

$$| \text{bias} | = | \text{count} - 5000 | / 10000 \quad (7)$$

Nilai subkunci tadi didapat dengan membandingkan setiap nilai simpangan (bias) dengan simpangan yang sebenarnya, yaitu 1/32 (didapat dari ½ - 15/32). Dari hasil kriptanalisis, didapat tabel nilai bias sebagai berikut:

partial subkey [$K_{5,5}$...$K_{5,8}$, $K_{5,13}$...$K_{5,16}$]	| bias |
1 C	0.0031
1 D	0.0078
1 E	0.0071
1 F	0.0170
2 0	0.0025
2 1	0.0220
2 2	0.0211
2 3	0.0064
2 4	**0.0336**
2 5	0.0106
2 6	0.0096
2 7	0.0074
2 8	0.0224
2 9	0.0054
2 A	0.0044
2 B	0.0186
2 C	0.0094
2 D	0.0053
2 E	0.0062
2 F	0.0133
3 0	0.0027
3 1	0.0050
3 2	0.0075
3 3	0.0162
3 4	0.0218
3 5	0.0052
3 6	0.0056
3 7	0.0048

Tabel 1. Nilai simpangan pada masing-masing subkunci yang dihitung

Nilai simpangan dari [2,4], yaitu 0.0336 sangat dekat dengan nilai simpangan sesungguhnya yaitu 1/32 atau 0.03125, oleh karena itu disimpulkan bahwa nilai subkunci parsial di atas adalah [2,4]

Kemudian hal ini dilakukan untuk setiap putaran, sehingga akan didapat 26 bit subkunci, sedangkan untuk 30 bit sisanya, harus dilakukan *exhaustive search*.

2.3 Penerapan *Differential Cryptanalysis* pada Algoritma DES

Penerapan *Differential Cryptanalysis*

Dengan cipher yang sama dengan penerapan *linear cryptanalysis*, pertama-tama kita menganalisis komponen dari cipher dengan cara sebagai berikut:

Anggap sebuah S-box dengan input $X = [X_1, X_2, X_3, X_4]$ dan output $Y = [Y_1, Y_2, Y_3, Y_4]$. Semua pasangan perbedaan dari sebuah S-box, (ΔX, ΔY), dapat diketahui dan probabilitas dari ΔY didapat dari ΔX dengan $\Delta X = X' \oplus X''$. Setelah dihitung semua ΔX dan ΔY, bisa didapat tabel distribusi perbedaan dan pasangan perbedaan dari S-box.

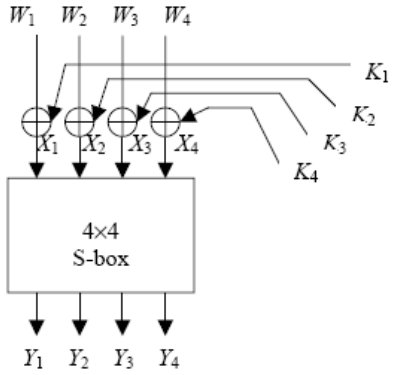
X	Y	ΔY		
		ΔX = 1011	ΔX = 1000	ΔX = 0100
0000	1110	0010	1101	1100
0001	0100	0010	1110	1011
0010	1101	0111	0101	0110
0011	0001	0010	1011	1001
0100	0010	0101	0111	1100
0101	1111	1111	0110	1011
0110	1011	0010	1011	0110
0111	1000	1101	1111	1001
1000	0011	0010	1101	0110
1001	1010	0111	1110	0011
1010	0110	0010	0101	0110
1011	1100	0010	1011	1011
1100	0101	1101	0111	0110
1101	1001	0010	0110	0011
1110	0000	1111	1011	0110
1111	0111	0101	1111	1011

Tabel 2. Pasangan Perbedaan pada S-box

		Output Difference															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Difference	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
	2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
	3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
	4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
	5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
	6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
	7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
	8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
	9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
	A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
	B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
	C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
	D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
	E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
	F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Tabel 3. Distribusi perbedaan

Perhitungan di atas adalah perhitungan pada S-box yang belum diberi kunci. Pada S-box yang sudah diberi kunci, anggap semua masukan adalah $W = [W_1, W_2, W_3, W_4]$. Skema masukan-keluarannya adalah sebagai berikut:



Gambar 7. Skema masukan-keluaran pada S-box yang telah diberi kunci

Cara mencari W_i adalah sebagai berikut:

$$\Delta W_i = W_i' \oplus W_i'' = (X_i' \oplus K_i) \oplus (X_i'' \oplus K_i) = X_i' \oplus X_i'' = \Delta X_i \quad (8)$$

Dapat disimpulkan, S-box yang berkunci mempunyai distribusi perbedaan yang sama dengan S-box yang tidak berkunci.

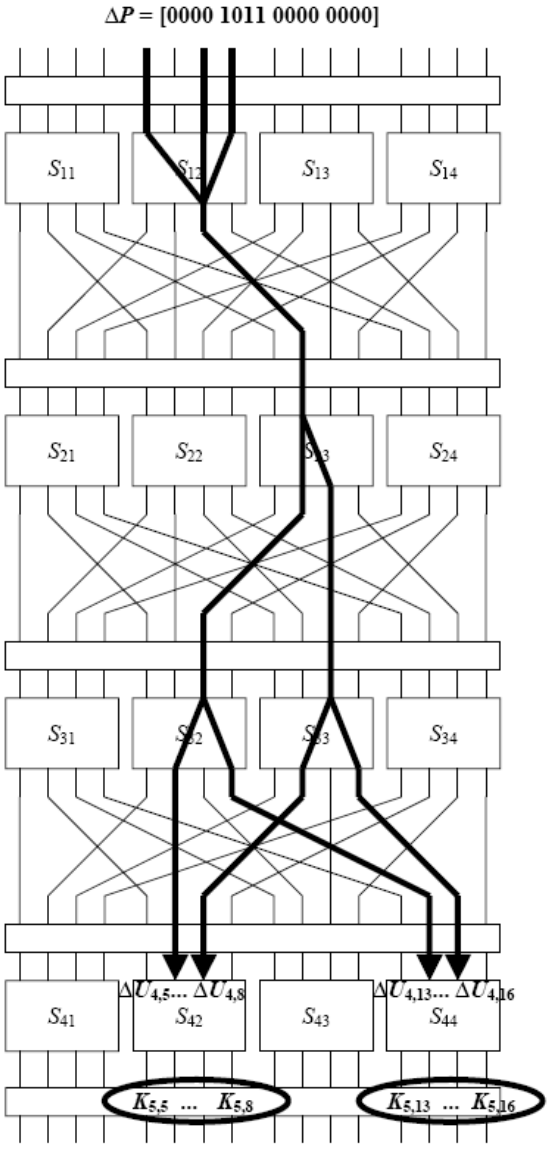
Anggap sebuah karakteristik diferensial melibatkan S_{12}, S_{23}, S_{32}, S_{33}. Kita menggunakan pasangan ini pada S-box:

S_{12}: $\Delta X = \mathrm{B} \rightarrow \Delta Y = 2$ with probability 8/16
S_{23}: $\Delta X = 4 \rightarrow \Delta Y = 6$ with probability 6/16
S_{32}: $\Delta X = 2 \rightarrow \Delta Y = 5$ with probability 6/16
S_{33}: $\Delta X = 2 \rightarrow \Delta Y = 5$ with probability 6/16

Perbedaan input dalam cipher sama dengan perbedaan input pada putaran pertama:

$$\Delta P = \Delta U_1 = [0000\,1011\,0000\,0000] \quad (9)$$

Maka, karakteristik diferensial pada S-box dapat dimodelkan sebagai berikut:



Gambar 8. Sampel karakteristik diferensial

Pada ekstraksi kunci, hampir sama dengan penyerangan linear, namun di sini digunakan

probabilitas dari perbedaan yang muncul. Probabilitas tersebut dihitung dengan persamaan sebagai berikut:

$$\text{prob} = \text{count} / 5000. \quad (10)$$

Dengan 5000 didapat dari jumlah pembangkitan *known ciphertext.* Count akan bertambah jika perbedaan dari input sampai ke putaran terakhir sama dengan nilai yang diharapkan pada karakteristik diferensial.

Pada S-box ini, didapat P_D = 27/1024 atau kira-kira 0.0264, dan pada tabel berikut ini didapat [2,4] mempunyai nilai probabilitas 0.0244, atau mendekati nilai P_D.

partial subkey $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	prob
1 C	0.0000
1 D	0.0000
1 E	0.0000
1 F	0.0000
2 0	0.0000
2 1	0.0136
2 2	0.0068
2 3	0.0068
2 4	**0.0244**
2 5	0.0000
2 6	0.0068
2 7	0.0068
2 8	0.0030
2 9	0.0024
2 A	0.0032
2 B	0.0022
2 C	0.0000
2 D	0.0000
2 E	0.0000
2 F	0.0000
3 0	0.0004
3 1	0.0000
3 2	0.0004
3 3	0.0004
3 4	0.0000
3 5	0.0004
3 6	0.0000
3 7	0.0008

Tabel 4. Hasil untuk serangan diferensial

Untuk selanjutnya, dilakukan hal yang sama sampai semua S-box dieksplor. Untuk subkunci yang belum ditemukan, dilakukan cara *exhaustive search.*

3. KESIMPULAN

Algoritma DES dapat diserang dengan cara-cara selain cara *brute force*, di antaranya adalah dengan cara Linear Cryptanalysis dan Differential Cryptanalysis.

Jika dibandingkan antara kedua metode kriptanalisis tersebut, keduanya memiliki persamaan yaitu merupakan sebuah *known-plaintext attack.* Namun, keduanya memiliki pendekatan yang berbeda, dimana pada linear cryptanalysis menggunakan pendekatan linear, sedangkan pada differential cryptanalysis menggunakan pendekatan perbedaan antara input dan outputnya.

DAFTAR PUSTAKA

[1] Bruce Schneier, "Applied Cryptography - Second Edition". John Wiley & Sons, Inc, 1996

[2] Menezes, P. Van Oorschot, S. Vanstone, "Handbook of Applied Cryptography". CRC Press, Inc, 1997

[3] Pascal Junod, "Linear Cryptanalysis of DES, Diploma Thesis". Technische Hochschule Zurich.

[4] Bruce Schneier, "A Self-Study Course in Block-Cipher Cryptanalysis".

[5] Ralf Philipp Weinmann, "Algebraic Methods in Block Cipher Cryptanalysis". Department of Computer Science, Technischen Universität Darmstadt

[6] Howard M. Heys, "A Tutorial on Linear and Differential Cryptanalysis". Electrical and Computer Engineering, Faculty of Engineering and Applied Science, Memorial University of Foundland.

[7] "Basic Cryptanalisis". FIELD MANUAL NO 34-40-2, HEADQUARTERS DEPARTMENT OF THE ARMY. Washington, DC, 13 September 1990