ISSN 0853-8697

KRITERIA KEAMANAN BLOK CIPHER DAN ANALISIS SANDI DIFERENSIAL

Yusuf Kurniawan[1], M. Sukrisno Mardiyanto[2], Iping Supriana Suwardi[2]
[1]*Jurusan Teknik Informatika, Universitas Pasundan*
Jl Setiabudi 193 Bandung 40153, Telp. 022-2019371, Faks. 022-2019352
E-mail: ysfk2002@yahoo.com
[2]*Departemen Teknik Informatika, Institut Teknologi Bandung*
Jl Ganesha 10 Bandung 40142, Telp 022-2508136, Faks : 022-2500940
E-mail: sukrisno@informatika.org, iping@informatika.org

ABSTRACT

Several criterions used to determine the security measure of ciphers, have been researched for tens years. Shannon recommended two concepts for designing of algorithm encryption: confusion and diffusion. These criterions have been expanded with other criterions addition like avalanche property, Strict Avalanche property, Key-dependence avalanche, sequence complexity, Binary derivatives, and Bit dependencies.

This paper will try to discuss if the criterions that have been proposed by researchers have succeeded to counter to cryptanalysis. In this paper, six-round-DES is examined. The result of the research showed that the DES reduced to six rounds has satisfied the criterions, but failed to counter to differential cryptanalysis (DC). Some researchers have proposed to strengthen DES by making all subkeys Ki independent. So, for DES reduced to six rounds with independent subkeys, the number of keys is 6x48 (288 bits). However, DC can break the cipher by analyzing only 256 cipher texts.

Keywords: Block cipher, differential cryptanalysis, DES, criterions, subkey.

1. PENDAHULUAN

Banyak orang menyangka bahwa bila sudah membuat algoritma enknripsi yang komplek, maka algoritmanya akan aman. Kenyataan membuktikan bahwa hal ini tidak selalu benar. Bukti bahwa suatu algoritma aman, kurang diperhatikan, dan ini merupakan hal yang jauh lebih sulit. Banyak algoritma yang dianggap kuat oleh pembuatnya, ternyata kemudian dapat dipecahkan oleh pihak lain. Ambil contoh, ENIGMA, yang digunakan tentara Nazi Jerman dalam perang dunia 2, dianggap Jerman sebagai algoritma yang mustahil dipecahkan. Nyatanya, Sekutu berhasil memecahkannya dan kemudian sangat mempengaruhi kemenangan Sekutu dalam PD2 tersebut.

Seorang pakar kriptografi dari Amerika Serikat, Bruce Schneier [1], menyatakan bahwa melakukan analisis sandi merupakan pekerjaan yang jauh lebih sulit dari pada membuat algoritma enkripsinya. Artinya, banyak orang yang dapat membuat algoritma enkripsinya sendiri, namun sangat diragukan bahwa orang tersebut juga dapat membuktikan bahwa algoritma enkripsinya benar-benar aman. Schneier juga menyatakan bahwa lebih dari 90% waktunya justru digunakan untuk membuktikan bahwa algoritma ciptaannya (Twofish) benar-

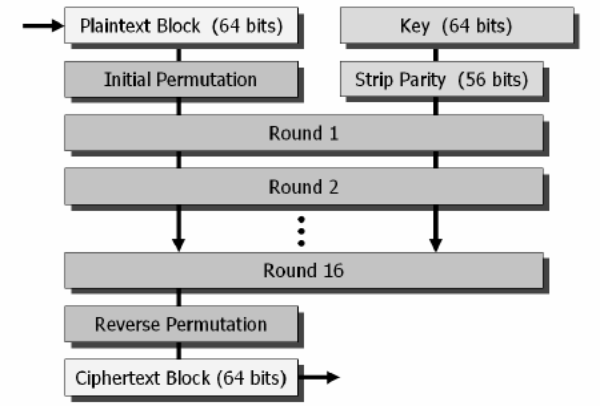
benar aman. Artinya, bila seseorang berhasil membuat sebuah algoritma enkripsi, maka dia baru melakukan 10% pekerjaan, dan sisanya yang 90% belum dilakukan sampai analisis sandinya selesai dikerjakan. Algoritma Twofish yang dibuat Schneier dan rekan-rekannya termasuk dalam 5 besar finalis dalam lomba tingkat dunia untuk menjadi algoritma *de facto* standar dunia AES (*Advanced Encryption Standard*).

Untuk menghadapi analisis sandi, beberapa kriteria telah diteliti para pakar kriptografi. Di antaranya adalah avalanche property, Strict Avalanche property, Key-dependence avalanche, sequence complexity, Binary derivatives, and Bit dependencies. Dalam penelitian ini, kriteria ini akan dihadapkan pada ASD (Analisis Sandi Diferensial). Memang tidak setiap kriteria yang disebutkan disini berhubungan langsung dengan ASD. Namun, kriteria ini merupakan kriteria yang umum, yang diharapkan dapat menghadapi segala macam analisis sandi, sehingga terdapat juga peneliti yang secara tidak langsung menghubungkan kriteria ini dengan ASD [4]. Hubungan kriteria ini dengan ASD akan dijelaskan pada bagian kriteria.

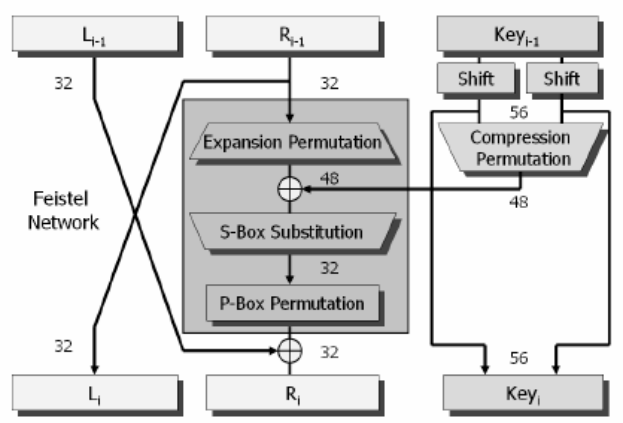
DES (*Data Encryption Standard*) merupakan standar *de facto* algoritma enkripsi dunia yang terdiri dari 16 ronde seperti terlihat pada gambar 1. Pada penelitian ini hanya dianalisis 6 ronde mengingat kompleknya algoritma 16 ronde [2], dan karena seperti pada [4] telah diperlihatkan bahwa DES 6 ronde telah memenuhi kriteria-kriteria yang telah disebutkan. Sehingga, penekanan dalam makalah ini adalah detil cara ASD terhadap DES 6 ronde.

2. DATA ENCRYPTION STANDARD (DES)

Pada bagian ini akan dijelaskan tentang struktur detil DES. Gambar 1 memperlihatkan DES lengkap 16 ronde, yang setiap rondenya berisi komponen seperti yang diperlihatkan pada gambar 2. Untuk Rincian DES yang lengkap, lihatlah [5].



Gambar 1. Diagram blok DES lengkap



Gambar 2. Satu ronde DES

Satu-satunya komponen yang linear dalam DES adalah kotak subtitusi (kotak-S). Sehingga boleh dikatakan komponen inilah yang menjadi penentu keamanan DES. Meskipun demikian, komponen lain juga membantu kotak-S memberi tambahan keamanan. Misalkan komponen *Expansion Permutation*, memberi tambahan keamanan dengan peningkatan jumlah kotak-S yang aktif.

3. KRITERIA KEAMANAN BLOK *CIPHER*

Para ahli kriptografi berusaha mendefinisikan kriteria agar sebuah algoritma dapat dianggap aman menghadapi berbagai analisis sandi.

a. Sifat *Avalanche*

Pada *cipher* yang baik, membalik satu bit masukan (*plaintext*), akan mengubah keluaran (*ciphertext*) menjadi tidak terprediksi. Bila sifat *avalanche* dipenuhi, maka rata-rata setengah bit-bit *ciphertext* akan berubah bila satu bit plaintext diubah. Hubungannya dengan ASD adalah bahwa apabila pengubahan bit-bit tertentu dari plaintext akan mengubah bit-bit ciphertext tertentu dengan peluang yang besar, maka beda (XOR) bit-bit tertentu plaintext juga akan mengubah beda (XOR) bit-bit tertentu keluaran.

b. Sifat *Strict Avalanche*

Strict Avalanche Criterion (SAC) merupakan generalisasi sifat *avalanche*. Blok cipher dikatakan memenuhi SAC bila pengubahan satu bit plaintext, akan membalik setiap bit *ciphertext* dengan peluang 0,5. Hubungan dengan ASD serupa dengan kriteria sebelumnya.

c. *Key-dependence avalanche*

Kriteria ini merupakan perluasan dari dari kriteria *avalanche* di atas. Pada cipher yang baik, membalik satu bit kunci, akan mengubah rata-rata setengah bit-bit ciphertext. Hubungan dengan ASD di sini tidak secara langsung, yaitu bila perubahan bit-bit kunci tertentu akan mengakibatkan perubahan bit-bit tertentu

ciphertext dengan peluang yang cukup besar, maka XOR bit-bit ciphertext juga akan mengakibatkan XOR bit-bit tertentu kuncinya. Dengan mengetahui bit-bit ciphertext, maka peluang diketahuinya bagian bit-bit kunci juga akan meningkat.

d. Kompleksitas urutan

Tes statistik yang lebih baik dapat digunakan untuk mengukur apakah $E_K(P) \oplus E_K(P \oplus e_i)$ terlihat terdistribusi acak. $E_K(P \oplus e_i)$ adalah Enkripsi dengan kunci K terhadap masukan $(P \oplus e_i)$. Kompleksitas urutan merupakan salah satu ukuran keacakan deretan bit yang diukur dengan menghitung jumlah pola baru yang nampak Misalkan 0010111011001001 = 0/01/011/10110/0100/1 memiliki kompleksitas 6. Hubungan dengan ASD adalah bahwa pada ASD, dicari XOR keluaran yang dihasilkan dari XOR masukan dengan peluang yang sebesar mungkin, maka terlihat di sini bahwa bila kriteria ini lemah, maka XOR masukan akan cenderung membuat XOR bit-bit tertentu dari keluaran akan tertentu dengan peluang yang lebih besar.

e. *Binary Derivative (BD)*

Tes acak dapat dilakukan dengan menghitung bobot Hamming dari BD. BD didefinisikan dengan persamaan $s_i' = si \oplus s_{i+1}$. Di sini tidak ada hubungan langsung dengan ASD, kecuali bahwa bila tes BD ini dipenuhi, maka keacakan *cipher* lebih terjamin. Sedangkan ASD mengeksploitasi cipher yang kurang acak, yaitu yang memiliki keteraturan beda keluaran yang dihasilkan dari beda masukan dengan peluang yang besar.

f. Ketergantungan Bit

Keluaran *cipher* dapat dinyatakan sebagai fungsi boolean plaintext dan kuncinya. Pada *cipher* yang baik, setiap bit keluaran akan tergantung pada seluruh bit masukan. Secara langsung tidak ada hubungan antara kriteria ini dengan ASD.

4. ANALISIS SANDI DIFERENSIAL

Pada bagian ini akan dijelaskan tentang ASD [3].

Definisi 1 *(Operasi difference) Difference antara dua deretan bit X dan X* didefinisikan sebagai*

$$\Delta X = X \Theta (X^*)^{-1}$$

di mana Θ merupakan operasi grup yang digunakan untuk mengkombinasikan kunci dengan data internal X dalam cipher. $(X^*)^{-1}$ merupakan inversi X dari operator Θ.*

Jika digunakan kunci K yang sama untuk X dan X*, maka $(X \Theta K) \Theta (X^* \Theta K)^{-1} = X\Theta K\Theta K^{-1}\Theta(X^*)^{-1} = X \Theta (X^*)^{-1} = \Delta X$. Dengan demikian, *difference* Θ merupakan operasi yang invarian terhadap kunci K.

Definisi 2. *(Markov Cipher) Jika terdapat operasi grup Θ untuk mendefinisikan difference sedemikian sehingga untuk semua pilihan dari α $(\alpha \neq 0)$ dan β $(\beta \neq 0)$, $Pr(\Delta Y = \beta \mid \Delta X = \alpha, X = \gamma)$ adalah tidak bergantung pada γ ketika subkey dipilih mengikuti*

distribusi uniform, maka iterated cipher dengan fungsi ronde $Y = F_K(X)$ adalah cipher Markov.

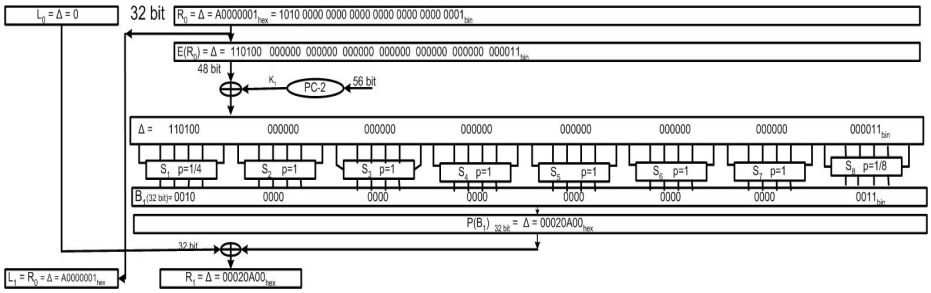
Definisi 3.*(Pasangan benar) Pasangan benar yang berhubungan dengan karakteristik r ronde (δ_0,.... δr)adalah pasangan plaintext (P, P*) di mana untuk $P \Theta P^* = \delta_0$, dan untuk setiap ronde i, $1 \leq i \leq r$, enkripsi pasangan menggunakan subkey ki yang tidak diketahui dan independen, memiliki difference masukan ronde δ_{i-1} dan difference keluaran ronde δ_i. Pasangan yang bukan „pasangan benar" yang berkenaan dengan karakteristik dan subkey ronde yang independen, disebut „pasangan salah".*

Definisi 4.*(Differensials) Diferensial r ronde adalah pasangan teks difference(δ_0, δr) di mana difference masukan adalah $\Delta P=\delta_0$ dan difference keluaran adalah $\Delta C = \delta r$. Peluang differensial (ΔP, ΔC) adalah :*

$$\Pr(\Delta C=\delta r \mid \Delta P=\delta_0) = \sum_{\delta_1}\cdots\sum_{\delta_{r-1}}\cdots \prod_{i=1}^{r} \Pr(\Delta Ci=\delta i \mid \Delta C_{i-1} = \delta_{i-1})$$

di mana $\Delta C_0 = \Delta P$

Untuk DES, kita harus menyusun karakteristiknya.



Gambar 3. Analisis Sandi Diferensial pada DES

Dari Gambar 3 kita lihat, bahwa Analisis Sandi Diferensial dimulai dari kotak-S. Untuk mendapatkan peluang karakteristik sebesar mungkin, harus diusahakan agar sesedikit mungkin kotak-S yang aktif. Sebab, dengan asumsi bahwa peluang setiap kotak-S adalah independen, maka peluang total merupakan hasil kali peluang dari semua kotak-S. Oleh karena itu, dimulai dari kotak-kotak Subtitusi di ronde 1, kita cari peluang diferensial terbesar. Dari tabel distribusi difference kotak-S, peluang terbesarnya adalah 16/64. Misalkan pada kotak-S1, terlihat bahwa peluang ini dipenuhi oleh pasangan $\Delta X = 34_{16}$ dan $\Delta Y= 2$, kemudian pada untuk kotak-S2 terlihat bahwa ($\Delta X=8$; $\Delta Y= A_{16}$) ($\Delta X = 1D_{16}$; $\Delta Y=7$) ($\Delta X=36_{16}$; $\Delta Y= D_{16}$) memiliki peluang karakteristik terbesar yaitu 16/64. Dari sini terlihat bahwa banyak sekali kemungkinan yang dapat terjadi bila kita mengambil peluang karakteristik terbesar.

Tabel 1 merupakan bagian dari tabel distribusi difference kotak subtitusi 1 DES yang penulis buat dengan bahasa C. Tabel seperti ini berjumlah 8 buah. Satu tabel untuk setiap kotak S. Tabel seperti ini juga dapat dilihat pada [2]

Tabel 1. Contoh distribusi difference kotak S1

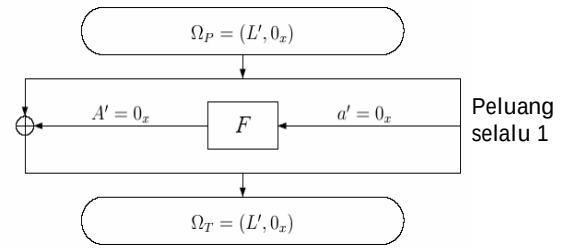
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	**0**	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	**1**	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2	**2**	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3	**3**	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4	**4**	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5	**5**	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6	**6**	0	4	2	4	8	2	6	2	8	4	**4**	2	4	2	0	12
7	**7**	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8	**8**	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9	**9**	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A	**10**	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
B	**11**	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C	**12**	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
D	**13**	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
E	**14**	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
F	**15**	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
10	**16**	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6

Misalkan kita ambil bahwa hanya kotak-S1 yang aktif, dan kotak-S lainnya tidak aktif seperti terlihat pada gambar 3. Maka Δmasukan S1 (ΔX) menjadi 34_{16} = 110100_2 dan Δkeluaran (ΔY) S-1 adalah 0010. Kemudian, karena operasi XOR yang terletak sebelum memasuki kotak-S tidak berpengaruh pada Analisis Sandi Diferensial, maka kita menuliskan bahwa Δkeluaran E juga sama dengan Δmasukan kotak-S. Jadi kita dapat menuliskan bahwa Δkeluaran E = 110100 000000 000000 000000 000000 000000 000000 000000. Namun kita harus ingat pada keluaran Ekspansi E, bit pertama = bit ke-31 dan bit ke-2=bit ke-32. Artinya, karena bit pertama dan kedua Δkeluaran E = 11, maka bit-31 dan bit ke32 juga harus =1. Sehingga, ΔE_{out} (Δkeluaran E) dan sekaligus juga Δmasukan S menjadi = 110100 000000 000000 000000 000000 000000 000000 000011 seperti yang terlihat pada gambar 3. Sekarang, kotak-S yang aktif bukan hanya satu (kotak-S1 saja) seperti yang kita harapkan melainkan menjadi dua yaitu kotak S1 dan kotak S8. Dan karena peluang karakteristik kotak-S1 = 1/4 dan kotak S8 = 1/8, maka peluang karakteristik ronde 1 menjadi ¼ x 1/8 = 1/32. Padahal bila kita hanya menggunakan satu kotak-S yang aktif, peluang ronde 1 hanya =1/4 (peluang differensial kotak-S1 saja).

Artinya pemilihan karakteristik pada kotak S1 di mana $\Delta X=34_{16}$ dan $\Delta Y=2$ dianggap salah, sebab bila masih di ronde-1 saja sudah sedemikian kecil peluangnya, bisa dibayangkan apabila dihitung 16 ronde, yang tentu akan menjadi sangat kecil sekali. Misalkan saja bila setiap ronde memiliki p=1/32, maka dalam 16 ronde, peluangnya menjadi $(1/32)^{16} = 2^{-80}$. Sedangkan jumlah kemungkinan masukan DES hanya 2^{64}. Artinya, mustahil DES dapat di-*attack*

dengan cara ini. Apalagi dengan adanya permutasi di akhir fungsi F di setiap ronde, kemungkinan kotak-S yang aktif di ronde-ronde berikutnya akan bertambah banyak. Dan peluang differensial DES lengkap 16 ronde sangat mungkin akan menjadi jauh lebih kecil dari 2^{-80}, dan semakin tidak mungkin dilakukan analisis sandi diferensialnya.

Oleh karena itu diperlukan cara lain untuk mendapatkan karakteristik yang tepat. Biham [2] memberikan contoh karakteristik yang bermanfaat. Jadi kita set ΔL_0 = a dan ΔR_0 = 0 agar menghasilkan ΔL_1 = 0 dan ΔR_1 = a. Kuncinya adalah Δmasukan fungsi F = 0 agar menghasilkan Δkeluaran fungsi F = 0 supaya diperoleh p = 1. Sebab dari tabel distribusi kotak S1-S8 diketahui bahwa setiap ΔX=0 akan menghasilkan ΔY=0 sehingga p = 1.



Gambar 4. Karakteristik 1R

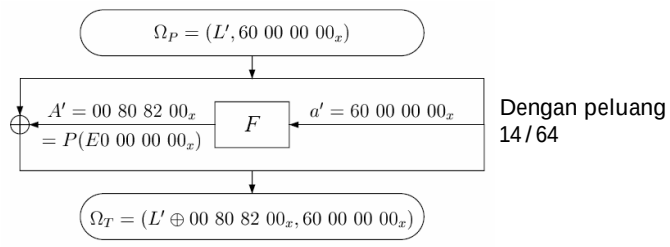
Ωp adalah XOR masukan suatu ronde di mana ruas kiri adalah L' dan ruas kanan adalah a' adalah XOR masukan F, dan A' adalah keluaran XOR F. Ω_T adalah XOR keluaran ronde. Namun karakteristik ini belum dapat digunakan untuk mendapatkan kunci DES 6 Ronde.

Berikut adalah contoh karakteristik satu ronde dengan peluang 14/64. Pada ronde ini, semua karakteristik semua masukan kotak-S adalah 0 kecuali S1. Satu kotak-S dipilih agar peluangnya menjadi maksimal. Dari percobaan sebelumnya, ternyata kotak-S1 tidak bisa dipasang p=16/64, karena adanya pengaruh E. Agar E tidak berpengaruh, maka harus diusahakan agar bit-bit "1 " tidak terletak di pinggir masukan E. Misalkan jangan sampai masukan kotak-S1 berupa 1001 atau 1000 atau 0001, sebab ini mempengaruhi kotak-S lainnya, yang pada akhirnya akan memperkecil peluang karakteristik.

Karena itu kita ambil peluang terbesar berikutnya yaitu 14/64. Terdapat 12 macam pasangan (ΔX,ΔY) yang memenuhi p=14/64 yaitu (3,0) ($1E_{16}$,4) (10_{16},7) ($3E_{16}$,7) (24_{16},8) (35_{16},8) (24_{16},9) (29_{16},9) ($2A_{16}$,9) (C_{16},E_{16}) ($1D_{16}$,E_{16}) (35_{16},E_{16}) atau dalam biner Δmasukannya (ΔX) adalah 0110000, 011110, 010000, 111110, 100100, 110101, 100100, 101001, 101010, 001100, 011101, 110101.

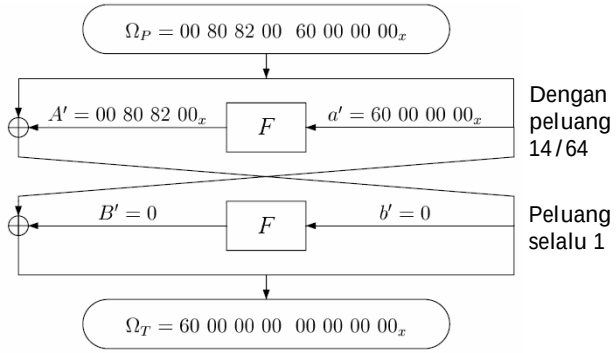
Perhatikan nilai biner yang merupakan XOR masukan kotak-S1. Pada warna abu-abu tidak boleh berisi bit "1" karena akan menyebabkan peningkatan kotak-S yang aktif. Hanya satu ΔX yang memenuhi syarat tersebut yaitu pada $\Delta X = C_{16}$ atau pasangan $(\Delta X,\Delta Y) = (C_{16},E_{16})$. Oleh karena itu, kita pilih pasangan (C_{16},E_{16}) dengan p = 14/16 untuk kotak-S1, sedangkan untuk kotak S2..S8 kita gunakan $\Delta X = 0 \rightarrow Y=0$ dengan peluang p=1

Dengan menelusuri $\Delta X = C_{16}$ pada S1 dan $\Delta X=0$ untuk S lainnya ke arah masukan F, maka kita peroleh a' = 60 00 00 00_x (di mana subskrib x merujuk pada he**x**adesimal) dan dengan menelusuri ke arah keluaran F, maka kita peroleh A' = 00 80 82 00_x atau A' merupakan keluaran permutasi P(E0 00 00 00_x) di mana E adalah XOR keluaran kotak-S1.



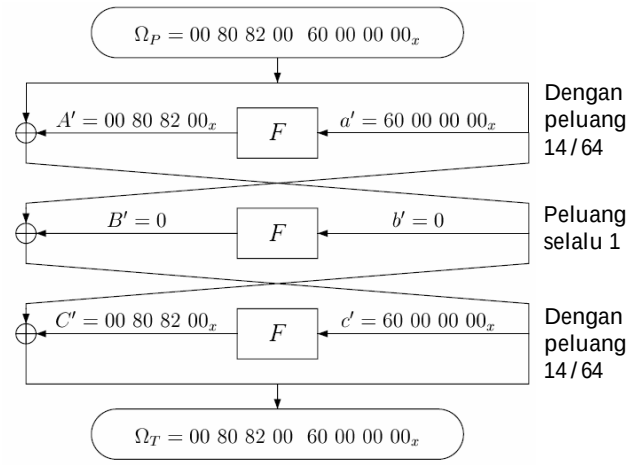
Gambar 5. Karakteristik 1R dari kotak S1

Bila kita inginkan Ω_T = 00 00 00 00 , 00 00 00 00 maka kita set L' = 00 80 82 00_x dan Ω_T menjadi b' (XOR masukan F ronde 2) sehingga kita peroleh karakteristik 2 ronde DES sebagai berikut:



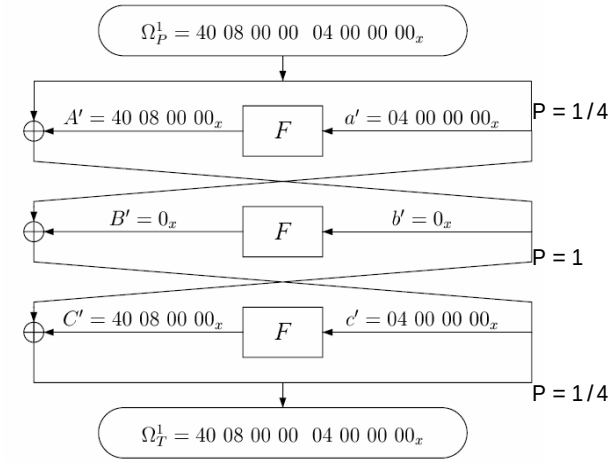
Gambar 6. Karakteristik 2R dari kotak S1

Bila kita gunakan lagi karakteristik a' → A' (60 00 00 00 → 00 80 82 00) untuk ronde ketiga maka akan diperoleh:



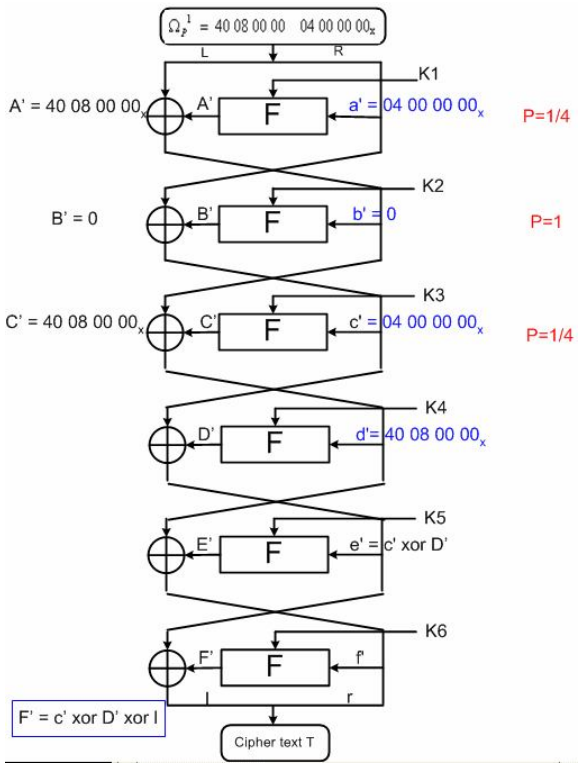
Gambar 7. Karakteristik 3R dari kotak S1

Sehingga karakteristik 3 ronde memiliki peluang $(14/64)^2$ = 0,04785. Dengan demikian, untuk tiga ronde kita memiliki peluang yang cukup besar dibandingkan sebelumnya. Dengan cara yang sama kita dapat memperoleh karakteristik lainnya, misalkan dari kotak S2 diperoleh :

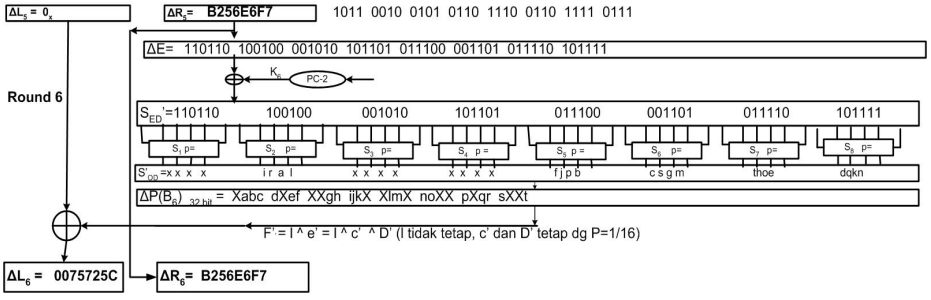


Gambar 8. Karakteristik 3R dari kotak S2

Karakteristik ini memiliki peluang yang lebih baik daripada sebelumnya yaitu $(¼)^2$ = 1/16. Sehingga karakteristik inilah yang digunakan untuk ASD DES 6 ronde. Karena menggunakan 3 Ronde untuk analisis sandi 6 ronde, maka metode ini disebut sebagai serangan 3 Ronde (3R-attack) [2].



Gambar 9. Attack DES 6R



Gambar 10. Contoh ASD pada ronde-6

Dengan memberi Δmasukan = 40 08 00 00 04 00 00 00$_x$ maka dapat diperoleh Δkeluaran = 00 75 72 5C B2 56 E6 F7x seperti terlihat pada gambar 4. ΔL5 dianggap = 0 untuk mempermudah analisis. Meskipun yang sebenarnya adalah ΔL5 = ΔR4= X000 0X00 XX00 000X X00X 00XX 0X00 0XX0$_2$ di mana X menyatakan bit yang tidak diketahui (bit ”0” atau ”1”). ΔR4 ini diperoleh dengan masukan ΔR3 = 40 08 00 00$_x$ mengikuti karateristik yang digunakan. Dengan

mengikuti alur komponen fungsi F, kita dapat melihat Δmasukan dan Δkeluaran kotak-S menjadi seperti pada gambar 4 dengan peluang tetap = 1/16. Karena untuk ronde 6, Δmasukan kotak S2, S5, S6, S7, dan S8 diketahui, maka kita dapat menerka subkey yang memasuki kotak-kotak S tersebut. Caranya adalah dengan menggunakan 256 pasangan (ΔP,ΔC) seperti contoh pada gambar 4 dan menggunakan penghitung subkey yang memasuki kotak-S di atas. Anggap subkey masukan ke kotak-kotak S tersebut adalah bilangan 30 bit. Bilangan ini dinaikkan satu-satu, dan dilihat pasangan ΔP,ΔC mana yang paling banyak memenuhi karakteristik. Subkey itulah yang merupakan subkey yang benar. Dengan demikian, Analisis Sandi Diferensial ini berhasil mendapatkan 30 bit subkey di ronde 6. Dengan karakteristik yang lain yaitu Ω^2_P = 00 20 00 08 00 00 04 00_x 12 subkey (yang masuk ke S2,S4) lainnya dapat ditemukan. Ω^2_P ini dapat ditemukan menggunakan metode yang telah dijelaskan di atas terhadap kotak S6. Sisa kunci DES 14 bit (56 – 42 bit) dapat ditemukan dengan brute force attack.

5. SIMPULAN

Dari penelitian di atas dapat diketahui bahwa:

a. Terpenuhinya kriteria keamanan cipher tidak menjamin bahwa cipher tersebut juga aman menghadapi analisis sandi.
b. Analisis sandi merupakan usaha yang sangat rumit dan sangat komplek, sehingga Schneier menyatakan bahwa 90% waktunya digunakan untuk melakukan analisis sandi Twofish, dan hanya sekitar 10% waktu yang digunakan untuk mendesain algoritmanya.
c. Banyak orang dapat membuat algoritma enkripsinya sendiri tanpa bisa membuktikan apakah algoritmanya benar-benar aman atau tidak.

PUSTAKA

[1] Schneier, B. (2000). *A Self-Study Course in Block-Cipher Cryptanalysis*. Counter-pane Internet Security.

[2] Biham, E., dan Shamir, A. (1991). Differential Crypanalysis of DES-like Cryptosystems. In *Advances in Cryptology: CRYPTO '90*, Springer Verlag, 2-21.

[3] Nakahara, J. (2003). *Cryptanalysis and Design of Block Ciphers.* KU Leuven.

[4] Wagner, D.A. (1995). The Security of MacGuffin. *Bachelor of Arts Thesis*, Princeton University.

[5] Rhee, M. Y. (1994). *Cryptography and Secure Communications*. New York: McGraw-Hill.