ISBN: 979-756-061-6

ANALISIS SANDI DIFERENSIAL PADA FEAL

Yusuf Kurniawan
Jurusan Teknik Informatika Universitas Pasundan
Jalan Setiabudi 193 Bandung
E-mail: ysfk2002@yahoo.om

Abstrak

Sejak diresmikannya penggunaan DES (Data Encryption Standard) pada pertengahan tahun 1970-an, studi algoritma enkripsi menjadi semakin banyak dilakukan di dunia akademik. Kotak Subtitusi DES yang dirahasiakan cara pembuatannya menimbulkan kecurigaan di kalangan ahli kriptografi bahwa DES telah dipasangi Backdoor. Oleh karena itulah muncul berbagai usulan agar DES diganti dengan algoritma yang keamanannya setara namun terbebas dari kecurigaan. Salah satu usul datang pada Eurocrypt 87 oleh Shimizu yang memperkenalkan FEAL. FEAL menggunakan kotak subtitusi yang berasal dari persamaan matematika yang sederhana untuk menghindari kecurigaan dipasangnya backdoor.

Kata Kunci: *DES, FEAL, Kotak Subtitusi, Backdoor.*

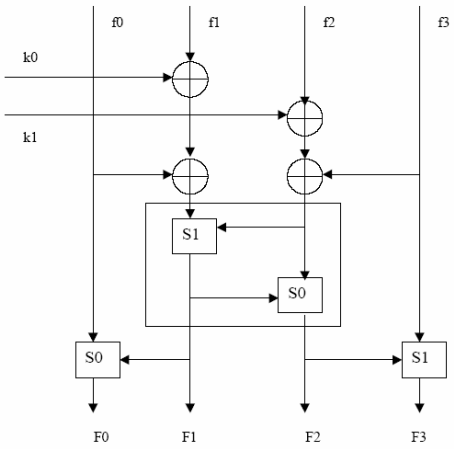
1. Pendahuluan

FEAL(*Fast Data Encipherment Algorithm*) [1] adalah cipher yang menggunakan struktur Feistel. FEAL dibuat oleh A. Shimizu dan S. Miyaguchi dan diusulkan untuk menjadi standar pengganti DES. FEAL memiliki 4 ronde dan dirancang agar memiliki kecepatan yang tinggi pada perangkat lunak. Karena itu FEAL tidak membutuhkan tabel look-up untuk kotak-S pada implementasi software. FEAL menghindari pembicaraan isi kotak S dengan membuat fungsi kotak-S yang sederhana yaitu pemetaan dari $F_2^8 * F_2^8 * F_2$ ke F_2^8

$$S(x,y,a) = Rot_2((x+y+a) \bmod 256)$$

di mana x dan y merupakan bilangan 8 bit sebagai masukan ke kotak S, sedangkan a merupakan konstanta 0 atau 1. Sedangkan Rot_2 merupakan rotasi bit ke arah kiri sebanyak 2 bit sehingga 2 bit MSB menjadi 2 bit LSB.

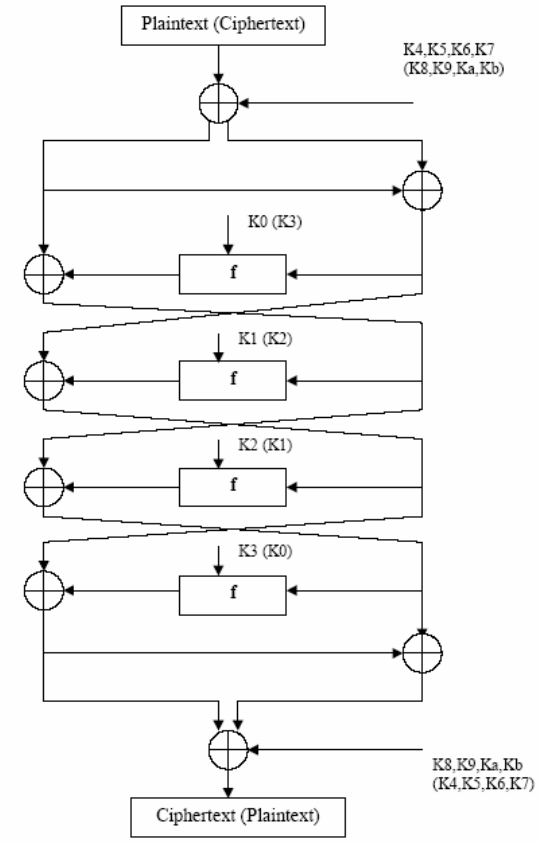
FEAL[3] memiliki kunci total 64 bit yang diperpanjang menjadi 12x 16 bit subkey. FEAL memiliki masukan plaintext 64 bit yang setelah di-XORkan dengan subkey K4,K5,K6,K7 dibagi 2 menjadi masing-masing 4 byte. Fungsi subkey ini adalah untuk *whitening* seperti yang dilakukan terhadap DES-X yang merupakan varian DES. Sebelum memasuki fungsi F, bagian kanan (32 bit) diXORkan dengan bagian kiri seperti terlihat pada gambar 2. Fungsi F nya sendiri dapat lihat pada gambar 1[5].



Gambar 1. Fungsi F FEAL

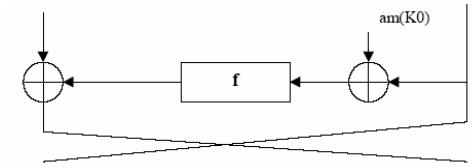
Ketika memasuki fungsi F, data 32 bit dipecah menjadi 4 byte (f0 f1 f2 f3). Sedangkan subkey K0 (16 bit) dibagi menjadi 2 (yaitu k0 dan k1). f0 ⊕ f1 ⊕ k menjadi masukan bagi kotak-S0 sebelah dalam sedangkan f2⊕f3⊕k1 menjadi masukan bagi kotak-S0 sebelah dalam. Sementara itu, f0 menjadi masukan bagi kotak S0 sebelah luar dan f3 menjadi masukan bagi kotak S1 sebelah luar seperti terlihat pada gambar 1. Setelah melalui perulangan sebanyak 4 kali dan diXOR dengan subkey K8,K9,Ka,Kb, diperoleh ciphertext. Untuk kotak S0, maka a pada S(x,y,a) bernilai 0 dan untuk kotak S1, nilai a adalah 1.

ISBN: 979-756-061-6



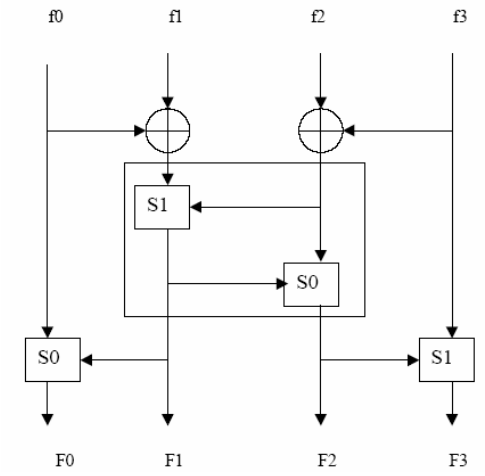
Gambar 2. Struktur FEAL lengkap

Untuk mempermudah analisis sandi pada FEAL, terlebih dahulu kita sederhanakan struktur FEAL. Dengan mengubah kunci Ki 16 bit menjadi am(Ki) di mana am(Ki) adalah suatu nilai sebesar 32 bit yang terdiri dari {0,k0,k1,0}, maka fungsi F pada FEAL dapat ditulis menjadi:

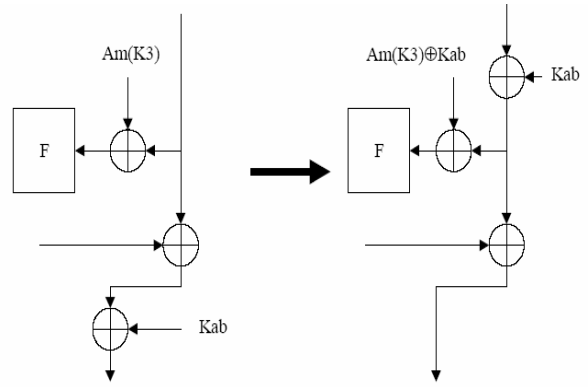


Gambar 3. Perubahan struktur ekivalen

Dan fungsi F pada FEAL dapat disederhanakan menjadi gambar 4. Untuk lebih mempermudah analisis sandi, kita hilangkan „whitening“ akhir (K8,K9,Ka,Kb) dengan struktur yang diusahakan tetap ekivalen.



Gambar 4. Fungsi F ekivalen



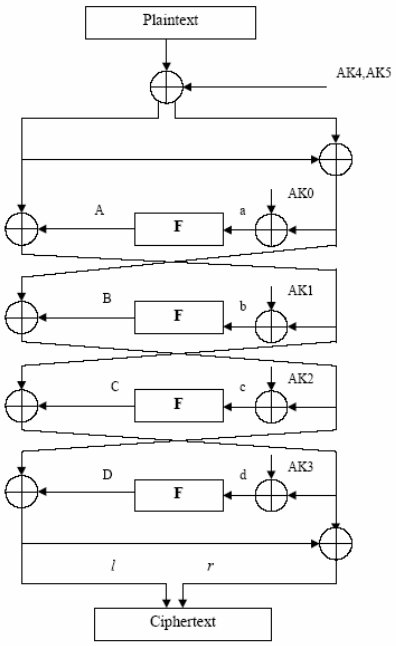
Gambar 5. Konversi masukan F

di mana untuk i=0,1,2,3
AKi = am(Ki) ⊕ K89 jika i genap
AKi = am(Ki) ⊕ K89 ⊕ Kab jika i ganjil

Whitening awal dapat dilakukan dengan dua nilai 32 bit yaitu AK4 dan AK5 di mana
AK4 = K45⊕K89⊕Kab
AK5 = K67⊕Kab

Sehingga struktur lengkap FEAL sekarang menjadi seperti gambar 6. Perhatikan bahwa struktur FEAL yang baru memiliki nilai-nilai 32 bit (AK0-AK5).

ISBN: 979-756-061-6



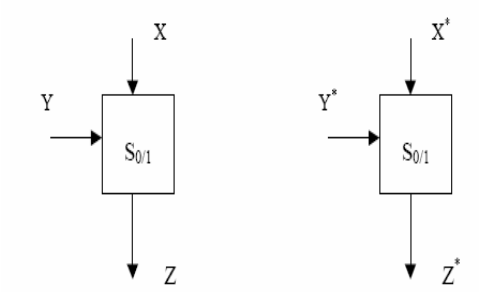
Gambar 6. Struktur FEAL ekivalen

2. Analisis Sandi Diferensial Pada FEAL

Setahun setelah dipublikasikannya FEAL, Boer menyatakan telah dapat memecahkan FEAL dengan hanya membutuhkan maksimal 10 ribu plaintext[2]. Di sini kita akan menggunakan ASD yang hanya membutuhkan 4 pasangan plaintext yang dipilih.

Analisis Sandi Diferensial (ASD) adalah usaha untuk mendapatkan kunci *cipher* dengan mencari beda masukan yang menghasilkan beda keluaran dengan peluang yang cukup besar[4]. Karena hanya kotak subtitusi FEAL satu-satu komponen yang tidak linear, maka pertama–tama kita periksa kotak-S FEAL.

S0 = ROL2(x+y) mod 256
S1 = ROL2(x+y+1) mod 256



Gambar 7. Masukan keluaran kotak-S FEAL

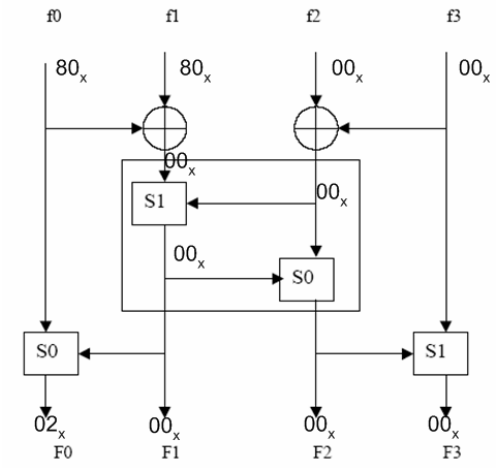
Kita cari ΔX dan ΔY sedemikian sehingga menghasilkan ΔZ dengan peluang yang sebesar mungkin. Untuk itu dibuatlah program untuk mendapatkan hasil seperti pada tabel 1. Dari tabel 1 terlihat bahwa bila kotak-$S_{0/1}$ diberi masukan $(\Delta x,\Delta y)=(0,0)$, maka akan dihasilkan $\Delta z=0$ dengan peluang p=1, demikian pula bila $(\Delta x,\Delta y,\Delta z)=(80_{hex},0,2)$ atau $(0,80_{hex},2)$ atau $(80_{hex},80_{hex},0)$

Tabel 1. Diferensial kotak S0/1

ΔX	*ΔY*	*ΔZ*	*p*
0	0	0	1
80	0	2	1
0	80	2	1
80	80	0	1
1	0	4	0.5
2	0	8	0.5
4	0	10	0.5
8	0	20	0.5

ΔX	*ΔY*	*ΔZ*	*p*
10	0	40	0.5
40	0	1	0.5
40	0	1	0.5
81	0	6	0.5
82	0	A	0.5
84	0	12	0.5
88	0	22	0.5
90	0	42	0.5

Kita gunakan tabel 1 untuk mendapatkan XOR masukan-keluaran dari fungsi F seperti pada gambar 8.

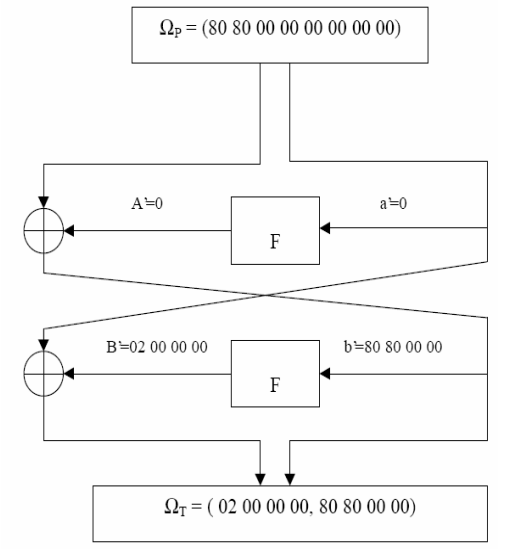


Gambar 8. Diferensial pada fungsi F

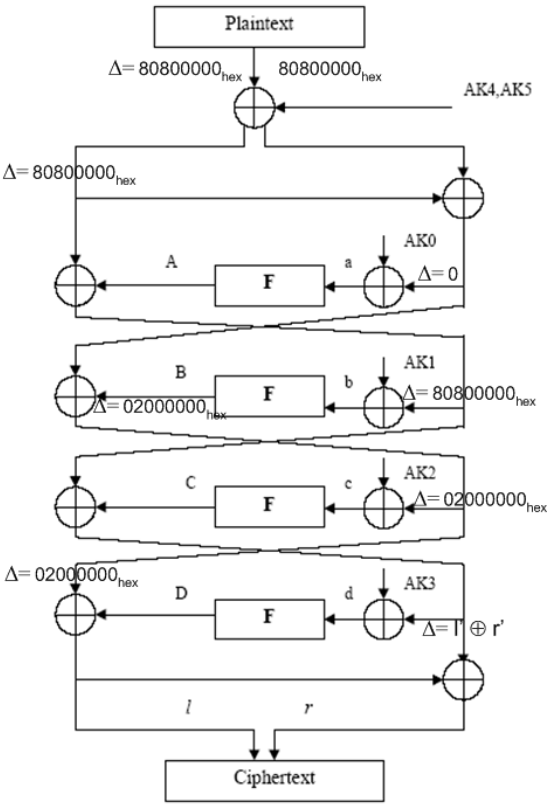
Bila XOR masukan-keluaran fungsi F diperluas, maka akan diperoleh karakteristik 2 ronde seperti pada gambar 10 yang berguna untuk *attack* FEAL.

Pasangan *plaintext* yang memenuhi karakteristik ini disebut pasangan benar. Namun karena karakteristik memiliki peluang 1, maka semua pasangan plaintext yang memenuhinya adalah pasangan benar.

ISBN: 979-756-061-6



Gambar 10. Karakteristik 2 ronde



Gambar 11. Karakteristik FEAL-4 lengkap

Untuk memecahkan FEAL-4, dibuatlah karakteristik lengkap seperti pada gambar 11. Kemudian siapkan pasangan *plaintext* dengan beda masukan $\Delta P = 80\ 80\ 00\ 00\ \ 80\ 80\ 00\ 00_{hex}$.

- Gunakan attack karakteristik 2 ronde dengan p = 1
- Dari arah *ciphertext*, d' = l' ⊕ r'
- C' = d' ⊕ b' = l' ⊕ r' ⊕ b' = l' ⊕ r' ⊕ 80800000_{hex}
- D' = l' ⊕ c' = l' ⊕ 02000000_{hex}
- Sekarang *attack* AK3, dengan mencoba 2^{32} kemungkinan nilai
- Nilai l' dan r' diketahui, sehingga D' dapat diketahui. Sedangkan l⊕r⊕AK3 → fungsi F → D, sehingga AK3 dapat dihitung karena l,r, dan D' telah diketahui
- Sebagai catatan, P⊕P* = P', di mana P dan P* adalah dua plaintext dengan karakteristik yang diinginkan.
- Dapatkan nilai kunci AK3 di mana D'=D⊕D* selalu sama nilainya untuk 4 pasangan *plaintext* yang dipilih.

Dalam waktu singkat, AK3 akan diperoleh. Jumlah pasangan *plaintext* yang diperlukan hanya sedikit karena digunakan karakteristik dengan peluang 1. Setelah AK3 diperoleh, maka ronde terakhir dapat dilepas untuk mendapatkan AK2, kemudian AK1, AK0 dan akhirnya AK4 dan AK5.

3. Kesimpulan

FEAL didesain dengan desain yang sangat sederhana dengan tujuan agar diperoleh kecepatan yang jauh lebih tinggi dibanding DES, khususnya pada perangkat lunak. Kotak-S FEAL menggunakan aritmatika modulo 256 untuk menghindari kecurigaan ditanamnya *backdoor*.

Ternyata FEAL-4 dengan mudah dapat ditaklukkan oleh ASD dengan hanya membutuhkan 4 pasang plaintext yang diketahui, karena kelemahan kotak-S nya yang ternyata rentan terhadap ASD.

Pendesain FEAL menjawab masalah ini dengan meningkatkan jumlah rondenya menjadi 8 ronde, namun tetap saja mudah ditaklukkan ASD. Penelitian selanjutnya menunjukkan bahwa FEAL baru berhasil menahan ASD setelah 32 ronde[6]. Dan tentunya, FEAL 32 ronde menjadi jauh lebih lambat dibanding FEAL aslinya yang hanya 4 ronde.

Daftar Pustaka

[1] A. Shimizu et.al, *Fast Data Encipherment Algorithm FEAL*, Advances in Cryptology-Eurocrypt '87, Lecture Notes in Computer Science 304.

[2] B. D. Boer, *Cryptanalysis of FEAL,* Advances in Cryptology-Eurocrypt '88 Proceedings, Springer Verlag, 1988

[3] Bruce Schneier, "Applied Cryptography", 2nd edition, John Wiley & Sons, Inc., 1996

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

[5] FEAL-4, http://www.computing.dcu.ie

[6] K. Aoki et. all, *The Best Differential Characteristics search of FEAL.* IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences Japan, Vol. E81-A, No 1 pp 98-104. 1998.