Kryptanalisis pada Algoritma Simple-DES

Rio Cahya Dwiyanto 13506041
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
IF16041@students.if.itb.ac.id

Abstract—Makalah ini menjelaskan upaya untuk menyerang S-DES menggunakan pembacaan sandi diferensial dan pembacaan sandi linear. S-DES adalah versi sederhana dari Enkripsi Data Standard (DES). Ini juga mencakup diskusi tentang masalah kriptologi dan sastra yang survei paper berguna tentang kriptografi dan kryptanalisis. pembacaan sandi. Tulisan ini dimaksudkan sebagai pedoman tentang dasar-dasar diferensial dan pembacaan sandi linear kriptanalisis dari cipher Feistel.

***Index Terms* — Cipher teks, Keamanan data, Kryptanalisis, Plain teks, Serangan Cipher teks, S-DES.**

I. LATAR BELAKANG

1.1 **Keamanan di Era Informasi**

Awal Era Informasi digembar-gemborkan jenis baru ancaman kepada pemerintah, perusahaan dan individu. Cyberspace telah menjadi arena baru pertukaran informasi dan komersial. Meskipun. sangat bermanfaat, dunia maya bisa menjadi tempat untuk bentuk baru dari kejahatan lama.

Seiring dengan penggunaan utama dari dunia maya, pemerintah dan perusahaan yang menggunakan dunia maya sebagai alat untuk spionase ekonomi dan serangan infrastruktur. Kejahatan elektronik komersial di sisi lain mempengaruhi perusahaan, menjadi boom ancaman baru-baru ini yang telah memicu pemulihan ekonomi belum pernah terjadi sebelumnya Bentuk lain dari ancaman keamanan memang ada, misalnya: pencurian identitas, dan menguntit terorisme cyber. Kejahatan ini mengekspos individu untuk keuangan, psikologis, dan bahkan ancaman fisik.

Keamanan adalah perhatian utama dari organisasi yang berpartisipasi dalam revolusi informasi. Kejahatan cyber sangat nyata dan menyebabkan kerugian finansial yang serius.

Bahkan dengan miliaran dolar yang dihabiskan pada sistem keamanan, masalah pelanggaran keamanan terus meningkat sepanjang tahun, didorong oleh eksposur yang lebih besar bahkan sipil publik untuk kelemahan keamanan meluasnya alat berbahaya.

Secara historis, kriptografi memainkan peran penting dalam banyak peristiwa, terutama perang, sejak peradaban Yunani kuno. Pentingnya kriptologi bahkan lebih terasa dalam era informasi, dimana komersial, kekuatan militer dan pemerintah begitu tergantung kepada teknologi enkripsi untuk membuat lingkungan yang aman untuk pertukaran informasi dalam saluran tanpa jaminan.

1.2 Pentingnya Efisiensi Cipher

Sistem kriptografi dibutuhkan dalam berbagai aplikasi. Kriptografi menemukan jalan ke banyak aplikasi seperti e-mail verifikasi, otentikasi identitas, perlindungan hak cipta, watermark elektronik, biometrik dan lain-lain Pada tingkat yang lebih rendah, kriptografi digunakan untuk menyediakan keamanan untuk kabel paket, tertanam sistem dan banyak lagi Hari ini, sistem kriptografi digunakan dalam miliaran perangkat di seluruh dunia, baik kabel dan nirkabel.

Karena digunakan secara luas, karena itu diinginkan untuk merancang dan mengimplementasikan sistem kriptografi yang efisien yang kuat di berbagai platform. Banyak faktor yang dipertimbangkan ketika mengukur efisiensi, ini termasuk jumlah pintu gerbang untuk desain hardware, persyaratan memori dalam pelaksanaan perangkat lunak dan kinerja lintas platform.

Pentingnya efisiensi cipher adalah bukti dalam pemilihan baru-baru ini baru Rijndael sebagai AES baru. Hal ini dipilih karena memenuhi persyaratan keamanan yang ditetapkan oleh NIST dengan biaya paling kecil untuk persyaratan perangkat keras dibandingkan dengan algoritma lainnya. Pesan bisa cepat dienkripsi dan didekripsi dengan Rijndael dan pertunjukan yang sama baik di berbagai platform mulai dari kartu cerdas untuk 64 bit prosesor. Ini juga membutuhkan jumlah memori yang sederhana dan melakukan yang terbaik (dibandingkan dengan algoritma yang lain) ketika diimplementasikan dalam perangkat keras.

1.3 Kriptologi

Kriptologi adalah ilmu yang berkembang terus-menerus, cipher yang diciptakan dan diberi waktu, hampir pasti pecah. Kriptanalisis adalah cara terbaik untuk memahami subjek kriptologi. Kriptografer terus-menerus mencari sistem keamanan yang sempurna, sistem yang cepat dan keras, sistem yang mengenkripsi cepat tetapi sulit atau tidak mungkin untuk dipecahkan. Kriptanalis selalu mencari cara untuk memecahkan keamanan yang diberikan oleh sistem kriptografi, dengan menggunakan pemahaman struktur matematika cipher.

1.4 Mengapa pembacaan sandi?

Kemajuan terbaru dalam teknik kriptoanalisis adalah hal yang luar biasa. Hal ini sekarang dianggap penting bagi setiap paper desain cipher blok baru untuk menyertakan evaluasi kuantitatif keamanan terhadap kondisi seperti pembacaan sandi kriptanalisis linear dan kriptanalisis diferensial.

Sejak 1970-an, upaya kriptanalisis adalah berpusat pada pemecahan Enkripsi Data Standard (DES), standar yang ditetapkan oleh Lembaga Nasional Standar dan Teknologi (NIST). Baru-baru ini, NIST mengadopsi standar baru, disebut Advanced Encryption Standard (AES). NIST menyerukan kepada masyarakat untuk menyerahkan cipher yang memenuhi standar yang ditetapkan untuk AES baru. Sebagian besar proposal AES disampaikan termasuk hasil kriptanalisis linear dan kriptanalisis diferensial sebagai evaluasi kekuatan cipher. Sebagian besar proposal AES menekankan pentingnya kriptanalisis. Hal ini sejalan dengan pandangan dari banyak kriptografer.

Bruce Schneier menyatakan bahwa jauh lebih sulit untuk kryptanalisis cipher daripada untuk merancang itu. Dia juga menyebutkan bahwa pembacaan sandi adalah cara terbaik menuju pemahaman konkret teknologi kriptografi. Lebih dari 90% dari usahanya dihabiskan untuk mengkryptanalisis saat bekerja pada usulan dari cipher Twofish. Kebanyakan orang memiliki konsepsi yang menciptakan sistem cipher yang baik adalah sulit.Ternyata cryptanalysing cipher adalah sebuah aktivitas yang lebih sulit daripada membuatnya. Untuk menjadi kriptografer yang baik, satu-satunya jalan adalah melalui cryptanalysing. Hanya dengan cryptanalysing dapat sebuah kriptografer benar-benar memahami cara kerja dalam-sistem kriptografi dan untuk merancang sistem yang lebih kuat terhadap serangan. Fakta ini jelas jika kita amati kriptologi buku yang dicetak, sementara ada beberapa buku bagus kriptografi, tidak ada buku, baik atau buruk, pada kriptanalisis. Ini adalah karena sifat sulit kriptoanalisis dan kenyataan bahwa satu-satunya cara untuk belajar cryptanalysis adalah melalui praktek.Sebuah cipher ditemukan oleh seseorang yang telah menunjukkan bahwa ia dapat mematahkan algoritma biasanya dianggap

jauh lebih aman. Desain itu mudah dan analisis itu sulit. Siapapun dapat membuat sebuah algoritma yang ia sendiri tidak bisa pecahkan

2.S-DES

2.1. Pengantar

S-DES adalah versi sederhana dari algoritma DES. Ia memiliki sifat yang mirip dengan DES tapi berkaitan dengan blok yang lebih kecil dan ukuran kunci (beroperasi pada blok bit pesan-8 dengan-bit kunci 10). Ia dirancang sebagai uji blok cipher untuk belajar tentang teknik kriptoanalisis modern seperti pembacaan sandi linear, pembacaan sandi differential dan kriptanalisis linear-diferensial. Ini adalah varian dari Simplified DES.

Kunci yang sama digunakan untuk enkripsi dan dekripsi. Padahal, jadwal menangani kunci bit diubah sehingga dekripsi adalah kebalikan dari enkripsi. Sebuah blok input yang akan dienkripsi adalah dikenakan permutasi awal (IP). Kemudian, diterapkan untuk dua putaran tergantung pada perhitungan kunci. Akhirnya, itu diterapkan ke permutasi yang merupakan kebalikan dari permutasi awal. Sekarang kita akan melanjutkan untuk penjelasan rinci tentang komponen S-DES.

2.2 Kunci

10 bit kunci yang digunakan untuk menghasilkan 2 blok yang berbeda dari 8 subkunci bit di mana setiap blok yang digunakan dalam iterasi tertentu. Mari kita menotasikan bit kunci 10 sebagai *KUNCI,* 8 subkunci bit sebagai K_1 dan K_2. Jadwal-key digunakan untuk menghasilkan subkunci dilambangkan sebagai *KS.* Gambar dibawah mengilustrasikan perhitungan K_1 dan K_2. *KEY* tunduk pada suatu permutasi awal, Pilihan 1 permutasi yang ditentukan oleh tabel berikut:

PC-1

9 7 3 8 0

2 6 5 1 4

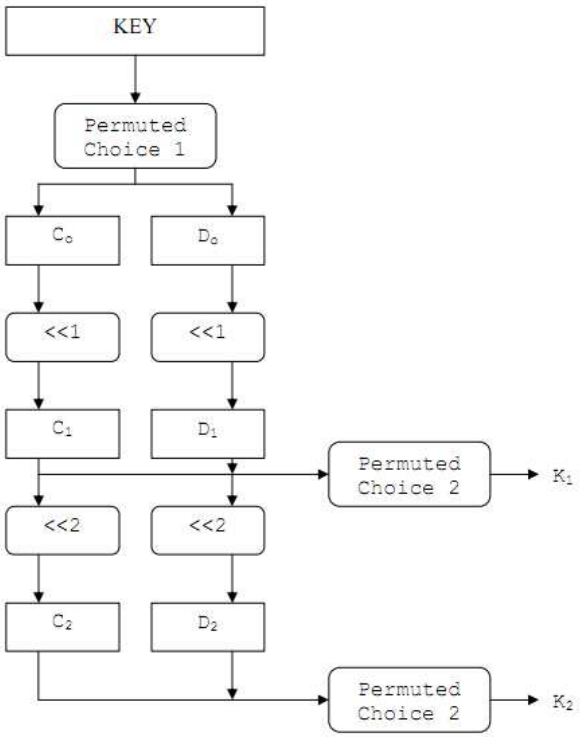
Tabel telah dibagi menjadi dua bagian. Bagian atas menentukan bit C_0 dan bagian bawah menentukan bit D_0. Bit *KUNCI* diberikan nomor dari 0 sampai 9. Dengan demikian, bit-bit C_0 adalah bit 9, 7, 3 ... dari *KUNCI* dan bit D_0 adalah bit 2, 6, 5 ... dari *KUNCI.*

Pergeseran kiri tunggal ini kemudian dilakukan pada kedua C_0 dan D_0. Hasil pergeseran kiri tunggal C_0 dan D_0 adalah C_1 dan D_1. Untuk membentuk K_1, D_1 digabungkan ke C_1 (Dengan dengan bit yang paling signifikan C_1 sebagai yang paling bit signifikan K_1 , dan bit yang paling signifikan D_1 diikuti oleh least significant bit C_1) Dan kemudian dikenai permutasi, permutasi Choice 2 yang ditentukan oleh tabel berikut:

PC-2

3 1 7 5 0 6 4 2

Dengan demikian, bit pertama dari K_1 adalah bit ketiga C_1D_1. Perhatikan bahwa bit K_1 hanya 8 bit.



Gambar 2.1

To form *K* Untuk membentuk K_2, C_1 dan D_1 dikenakan untuk dua shift kiri menghasilkan C_2 dan D_2. Kemudian, D_1 digabungkan ke C_1 menghasilkan C_1D_1. C_1D_1 kemudian dikenai permutasi, permutasi Choice 2 seperti dijelaskan di atas, menghasilkan K_2.

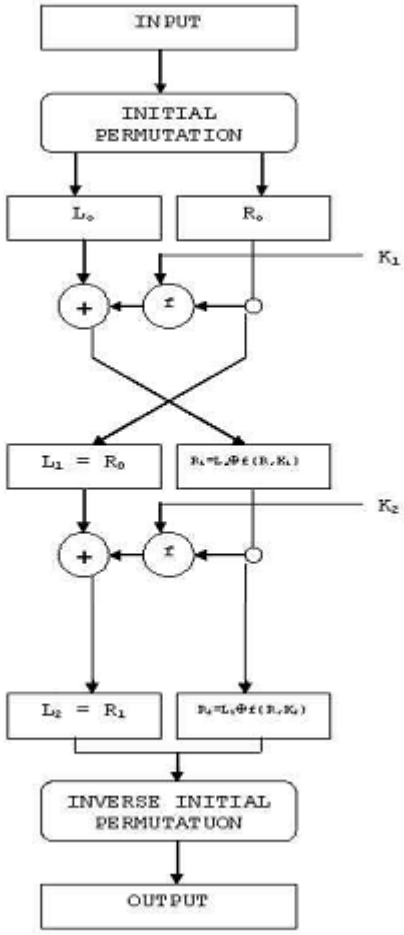
2.3 Cipher

Enciphering

Gambar 2.2 menggambarkan perhitungan yang diperlukan untuk enciphering. Prosedur enkripsi dapat diringkas sebagai:

$$C = E(P, K) = IP^{-1}(\rho_2(\rho_1(IP(P))))$$

Sekarang kita mulai melihat setiap tahap dari algoritma secara rinci.



Gambar 2.2

Blok 8 bit dikenakan ke permutasi awal, *IP 1,* yaitu sebagai berikut:

IP 1
7 6 4 0
2 5 1 3

Tabel telah dibagi menjadi dua bagian. Bagian atas menentukan bit L_0 dan bagian bawah menentukan bit R_0. Bit INPUT diberi nomor 0 sampai dengan 7. Dengan demikian, bit L_0 adalah bit 7, 6, 4… dari INPUT dan bit R_0 adalah bit 2, 5, 1 ... dari INPUT.

Setelah permutasi awal, L_0 dan R_0.kemudian mengalami putaran 1. Output dari putaran 1 adalah L_1 dan R_1. Perhitungan adalah sebagai berikut:

$L_1 = R_0$

$R_1 = L_0 \oplus f(R, K_1)$

Fungsi ini tergantung key cipher *f,* akan dijelaskan kemudian.

L_1 dan R_1 kemudian diterapkan pada putaran 2, menghasilkan L_2 dan R_2 seperti berikut ini:

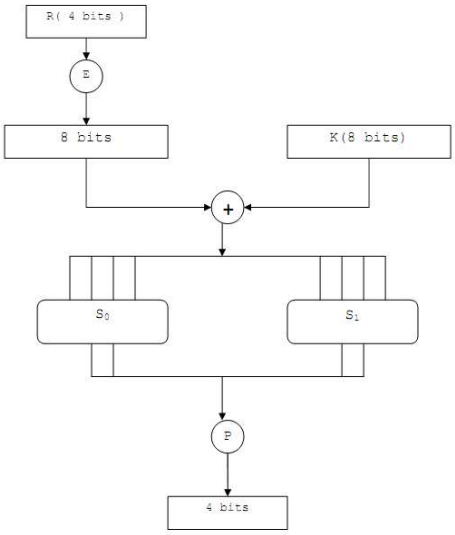
$L_2 = R_1$

$R_2 = L_1 \oplus f(R, K_2)$

Langkah terakhir memerlukan Rangkaian R_2 ke L_2 yang menghasilkan R_2 L_2. Hal ini kemudian dimasukkan ke permutasi yang merupakan kebalikan dari permutasi awal. Setelah permutasi ini, OUTPUT dihasilkan.

Fungsi Cipher f

Sebuah sketsa perhitungan *f (R, K)* diberikan pada **Gambar 2.3**



GAMBAR 2.3

E menunjukkan fungsi yang mengambil di blok input bit 4 dan menghasilkan blok 8 bit sebagai output. Output 8-bit blok *E* diperoleh sesuai dengan tabel berikut:

E-BIT SELECTION TABLE

3 0 1 2 1 2 3 0

Dengan demikian, tiga bit pertama dari *E (R)* adalah bit 3, 0, 1 *R*. 8 bit *E (R)* kemudian XOR dengan 8 bit subkey *K*. Subkunci K_1 digunakan untuk putaran 1 dan K_2 digunakan untuk putaran 2.

Hasil operasi XOR ini kemudian dibagi menjadi dua blok, empat bit pertama dari yang paling signifikan bit yang B_1 dan sisanya merupakan bit B_2 . B_1 dan B_2 kemudian diterapkan pada S_0 dan S_1 masing.

S_0 dan S_1 adalah S-box yang mengambil dalam input bit 4 dan menghasilkan output 2 bit.

	S_0 Column Number			
Row No.	0	1	2	3
0	1	0	2	3
1	3	1	0	2
2	2	0	3	1
3	1	3	2	0

	S_1 Column Number			
Row No.	0	1	2	3
0	0	3	1	2
1	3	2	0	1
2	1	0	3	2
3	2	1	3	0

Kita ambil S_0 sebagai contoh untuk menggambarkan bagaimana blok output ditentukan. S_0 mengambil bit pertama dan terakhir dari bit-bit blok 4 dan menggunakannya untuk mewakili dalam basis 2 nomor dalam kisaran 0 sampai 3. Misalnya, untuk blok 1101 bit, 11 diperoleh dan kemudian dikonversi ke 3. Ini digunakan untuk menentukan baris, dalam hal ini, baris 3.

Bit tengah 2 digunakan untuk mewakili dalam basis 2 nomor dalam kisaran 0 sampai 3. Ini digunakan untuk menentukan kolom. Dalam kasus blok contoh kita, dua bit di tengah merupakan kolom 2.

Dari S_0 di atas, nomor dari baris 3 kolom 2 dipilih, sehingga menghasilkan nomor 2, yang dalam biner ditulis sebagai 10.

Hasil S_0 dan S_1 di rubah untuk membentuk sedikit blok empat yang kemudian diterapkan pada permutasi, *P*.

Fungsi ini didefinisikan oleh tabel berikut:

P

1 0 3 2

Hasil *P* akan menjadi 4 bit dikembalikan oleh fungsi *f*.

Deciphering

Untuk menguraikan, algoritma yang sama digunakan, tetapi subkunci diterapkan dalam urutan terbalik. Artinya, bukan menerapkan K_1 untuk putaran 1, K_2 digunakan sebagai gantinya. Untuk putaran 2, K_1 digunakan sebagai gantinya.

3. BRUTE FORCE ATTACK

Kriptanalisis Brute force, seperti namanya adalah serangan kriptanalisis yang paling mudah. Meskipun menjadi salah satu metode yang paling primitif menyerang cipher adalah mendapatkan peningkatan penerapan sebagai akibat dari meningkatnya daya komputasi.

Walaupun sederhana, kekerasan hanya praktis untuk kriptografi kunci dengan ukuran maksimum 56 bit (Lebih dari 2^{56} = 72 milion lipat empat kali coba). Kriptografi lain dengan ukuran kunci lebih besar dari 56-bit bisamembutuhkan waktu yang lama untuk memecahkan dengan brute dan bahkan mungkin tidak layak. Sebagai contoh, saat ini AES dengan ukuran blok-128 bit hampir mustahil untuk di-crack oleh brute dengan komputer umum hari ini. Jumlah kombinasi untuk mencoba lebih dari butir pasir di bumi, kali lebih banyak dari satu miliar untuk setiap meter persegi di bumi.

Hal ini layak untuk menyerang S-DES dengan brute karena hanya memiliki ukuran kunci 10 bit. Untuk melakukan serangan brute, kita harus memiliki pasangan plaintext-ciphertext di mana kita mencari ruang kunci sampai code plaintext yang sesuai, terenkripsi dengan kunci yang ditargetkan menghasilkan ciphertext.

4. DIFFERENTIAL CRYPTANALYSIS

Kriptanalisis diferensial plaintext dipilih / serangan ciphertext dipilih yang awalnya dikembangkan untuk menyerang-seperti cipher DES. Sebuah serangan plaintext yang dipilih adalah salah satu dimana penyerang dapat memilih input untuk cipher dan memeriksa output. Menjadi salah satu serangan sebelumnya pada DES, diferensial kriptanalisis telah dipelajari secara ekstensif Banyak cipher ini dirancang dengan pertimbangan untuk

kekebalan terhadap kriptanalisis diferensial. Namun demikian, pembacaan sandi diferensial memberikan pemahaman yang baik tentang kemungkinan kelemahan cipher dan teknik untuk mengatasinya.

Diferensial kriptanalisis melibatkan analisis pengaruh perbedaan pasangan plaintext pada selisih yang ciphertext. Perbedaan yang paling yang umum digunakan adalah nilai XOR tetap dari pasangan plaintext. Dengan memanfaatkan perbedaan ini, subkey parsial yang digunakan dalam algoritma cipher dapat dinebak. Hal ini dilakukan secara statistik dengan menggunakan prosedur penghitungan (Sect. 5.5) untuk setiap kunci yang dengan jumlah tertinggi diasumsikan menjadi parsial subkunci kemungkinan paling tinggi.

4.1 Konsep Dasar

Pertimbangkan fungsi linier cipher dasar sebagai berikut:

$$C = P \oplus K$$

Dengan mengambil perbedaan sepasang ciphertext, kita telah membatalkan keluar kunci yang terlibat, meninggalkan kita dengan tidak ada informasi tentang kunci:

$$C \oplus C' = P \oplus K \oplus P' \oplus K$$
$$C \oplus C' = P \oplus P'$$

Hal ini karena linearitas fungsi. Persamaan di atas hanya memberitahu kita bahwa perbedaan antara plaintext adalah sama dengan perbedaan antara ciphertext.

S-DES bukan merupakan cipher linear. Dengan demikian, perbedaan antara ciphertext tidak sama dengan perbedaan antara plainteks. Dalam S-DES, perbedaan dalam pasangan ciphertext untuk perbedaan tertentu pasangan plaintext dipengaruhi oleh kunci. Thus, by utilising this fact, and the knowledge that certain Jadi, dengan memanfaatkan kenyataan ini, dan pengetahuan yang tertentu. Perbedaan plaintext terjadi dengan probabilitas yang lebih tinggi daripada perbedaan lain, kita dapat mengungkapkan informasi tentang kunci. Seperti kriptanalisis linear, kita mulai dengan menganalisis komponen non-linear dari cipher, S-Box. Kemudian, kita memperpanjang nilai-nilai yang diperoleh untuk membentuk karakteristik diferensial lengkap cukup untuk melakukan serangan.

4.2 Difference Pairs of an S-Box

Pertimbangkan-Box S_0 dan S_1 S-DES. Kita menunjukkan input untuk S-Box sebagai X dan output sebagai y. Perbedaan pasang sebuah S-Box ini kemudian dinotasikan sebagai $(\Delta X, \Delta Y)$, di mana $\Delta X = X' \oplus X''$. Hal ini lebih yaman jika kita mempertimbangkan semua 16 nilai dari X 'dengan ΔX sebagai kendala untuk nilai X'', sehingga $X'' = X' \oplus \Delta X$. Dengan X 'dan X'', nilai ΔY kemudian dapat diperoleh.

4.3 Differential Characteristics

Contoh di atas hanya merupakan pengantar untuk kemungkinan yang tersedia bagi kita saat kita menganalisis perbedaan antara pasangan plaintext dan ciphertext pasang. Kami memperluas pengetahuan ini untuk membuat diferensial karakteristik untuk 1 putaran S-DES. Dengan karakteristik diferensial, kita dapat memperoleh subkey, K_2 digunakan dalam putaran terakhir. Pertama, kita membangun sebuah karakteristik diferensial yang melibatkan S_1 di kedua putaran S-DES menggunakan pasangan perbedaan berikut S_0 dan S_1:

S_0: $\Delta X_0 = 2 \rightarrow \Delta Y_0 = 2$ with probability 12/16
S_1: $\Delta X_1 = 4 \rightarrow \Delta Y_1 = 2$ with probability 10/16

Jadi, dengan mempertimbangkan $\Delta X_1, \Delta X_2$ dan perluasan, E yang saya modifikasi untuk E = [0 2 1 3 0 1 2 3], perbedaan untuk putaran pertama diberikan oleh:

$$\Delta U_1 = [0\,0\,0\,0\,0\,1\,0\,0]$$

Ekspansi hanya suatu bentuk "difusi pemanis" dan tidak menambah linearitas-non cipher. Perubahan ini adalah membuat derivasi dari perbedaan input lebih jelas, ekspansi tidak menjadi perhatian utama di sini.

Kemudian, mengingat ΔX_0 ,dan ΔX_1 permutasi P yang berikut, kita akan mendapatkan perbedaan output untuk putaran 1:

$$\Delta V_1 = [0\,1\,0\,0\,0\,1\,0\,1]$$

Putaran 1 ini berkarakteristik memegang dengan probabilitas 12/16 · 10/16 = 15 / 32, yang berarti bahwa untuk setiap 32 acak dan merata pasang dipilih plaintexts dengan perbedaan ΔU_1 kita berharap untuk menemukan sekitar 1 pasang cipherteks yang sesuai yang memenuhi perbedaan ΔV_1.\ Pasangan dengan plaintext yang menghasilkan ΔU_1 cipherteks yang sesuai yang menghasilkan ΔV_1 disebut pasangan benar.

Karakteristik diferensial dapat menjadi yang terbaik divisualisasikan menggunakan angka yang digunakan oleh Biham .

Untuk putaran cipher N, kita perlu mencari karakteristik diferensial N-1 putaran untuk membayangkan serangan. Sejak S-DES adalah cipher putaran 2, putaran 1 karakteristik yang kita diperoleh adalah cukup.

4.4 Kesimpulan

Menggunakan parameter dibahas, serangan dilakukan pada S_0 dan S_1**.** Serangan itu sangat sukses dan dapat mengekstrak subkunci seluruh putaran 2. Ini adalah sebenarnya 8 bit dari DES 10-bit kunci S, 2 bit masih hilang. Jadi, kita sekarang dapat mencoba semua 2^2 kemungkinan bit hilang yang sepele. Juga, dengan subkey itu, maka seluruh kunci dapat diturunkan tanpa mencoba 2^2 kemungkinan.

REFERENCES

[CA92] Adams, C. (1992), On immunity against Biham and Shamir's differential cryptanalysis.
Information Processing Letters. 41: 77-80.

[AC97] Anne Canteaut (1997), Differential cryptanalysis of Fesitel ciphers and differentially
d-uniform mappings,Domaine de Voluceau, France.

[MP96] A. Menezes,P. van Oorschot, S. Vanstone (1996), Handbook of Applied Cryptography,
CRC Press.

[AG00] Anna Gorska et. al. (2000), New Experimental Results in Differential-Linear Cryptanalysis of
Reduced Variant of DES, Polish Academy of Sciences

[BV95] Buttyan, L. and I Vajda (1995), Searching for the best linear approximation of DES-like
cryptosystems. Electronics Letters. 31(11): 873-874.

[BS96] Bruce Schneier (1996), Applied Crytography,Second Edition, John Wiley and Sons,

[BE99] Bruce Schneier et. al. (1999), The Twofish Encryption Algorithm, John Wiley and
Sons.

[BS00] Bruce Schneier (2000), A Self-Study Course in Block-Cipher Cryptanalysis, Counterpane
Internet Security

[BS01] Bruce Schneier (2001), Why Cryptography Is Harder Than It LooKS, Counterpane
Internet Security

[HM95] C. Harpes, G. Kramer, and J. L. Massey (1995), A generalization of linear cryptanalysis
and the applicability of Matsui's piling-up lemma, Lecture Notes in Computer Science, 921.

[CY01]Chan Yeob Yeun Design (2000), Analysis and applications of cryptographic techniques,
Department of Mathematics, Royal Holloway University of London.

[DH01]Daithi Hanluain.(2001) Got Your Number Ericsson ON: The New World of Communication, Issue
3. 2001

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 22 Maret 2011

ttd

Rio Cahya Dwiyanto 13506041