Kriptanalisis pada Blowfish Cipher dengan Metode Boomerang Attack

Mufi Yanuar Triputranto / 13510106
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
mufi.yanuar@students.itb.ac.id

***Abstract*—Makalah ini memaparkan metode dan hasil kriptanalisis pada Blowfish Cipher menggunakan metode boomerang attack yang merupakan varian dari differential attack. Dari hasil uji coba diketahui bahwa blowfish tahan terhadap boomerang attack.**

***Index Terms*—Blowfish, boomerang attack**

I. PENDAHULUAN

Sebagai salah satu cipher modern, Blowfish seharusnya telah memenuhi syarat-syarat dari cipher yang baik, yaitu menerapkan prinsip confusion dan diffusion, serta tahan terhadap serangan differential. Makalah ini memaparkan salah satu teknik kriptanalisis untuk menguji Blowfish, yaitu boomerang attack yang merupakan varian dari differential attack [4].

II. HIPOTESIS

Blowfish cipher pertama kali diajukan oleh B. Scheiner pada tahun 1993[2]. Secara teoritis Blowfish telah menerapkan prinsip :

1. Confusion, karena telah ada S-Box untuk melakukan substitusi sederhana pada sebuah blok.
2. Diffusion, karena menggunakan enkripsi berulang dan jaringan Feistel[3].

Apabila pernyataan tersebut benar, maka dapat diperkirakan bahwa Blowfish akan tahan terhadap serangan differential karena pada dasarnya serangan differential dipakai untuk mengetahui hubungan antara plaintext dengan ciphertext[1]. Lebih spesifik lagi hubungan antara plaintext dan ciphertext dapat dihilangkan—atau minimal disembunyikan—dan akan sulit diserang menggunakan serangan differential karena :

1. S-Box menghilangkan hubungan linear antara plaintext dan ciphertext (confusion), *dan*
2. Jaringan Feistel menghilangkan hubungan statistik antara plaintext dengan ciphertext, artinya tiap plaintext bisa berkorespondensi dengan beberapa ciphertext dan tiap ciphertext bisa pula berkorespondensi dengan beberapa plaintext (diffusion).

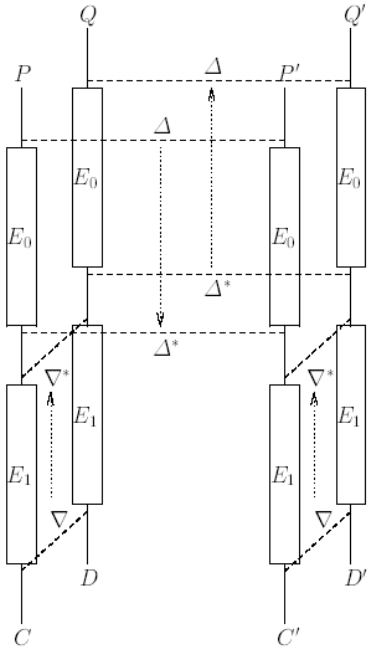
Artinya serangan differential yang bertujuan untuk mencari hubungan antara plaintext dan ciphertext akan gagal karena *plaintext dienkripsi tidak linear dan berulang kali,* dalam hal ini Blowfish memenuhinya.

III. BOOMERANG ATTACK

Untuk membuktikan hipotesis sebelumnya maka akan diujicobakan serangan differential pada Blowfish. Serangan differential yang digunakan adalah boomerang attack[4]. Secara singkat boomerang attack dapat dirumuskan sebagai berikut.

Pilih plaintext P serta vektor differential Δ dan ∇. Lalu lakukan langkah sebagai berikut :

1. Hitung $P' = P \oplus \Delta$
2. Hitung enkripsi P dan P', yaitu $C = E(P)$ dan $C' = E(P')$
3. Hitung $D = C \oplus \nabla$ dan $D' = C' \oplus \nabla$
4. Hitung dekripsi D dan D', yaitu $Q = E^{-1}(D)$ dan $Q' = E^{-1}(D')$
5. Apabila sebuah cipher dapat diserang, maka $Q \oplus Q' = \Delta$

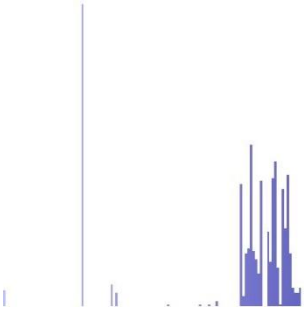


Gambar 1. Ilustrasi Boomerang Attack

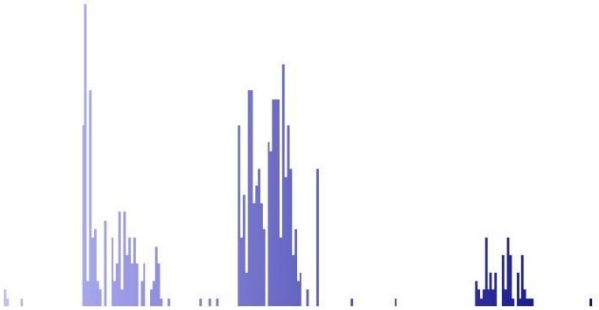
IV. UJI COBA

Untuk enkripsi digunakan tools cipher Blowfish online yang ada di laman web *http://symmetric-ciphers.online-domain-tools.com/#function=blowfish*. Uji coba dilakukan pada Blowfish yang bekerja pada mode CBC dengan kunci tertentu. Plaintext yang digunakan adalah teks yang ada di laman web yang dipilih secara acak.

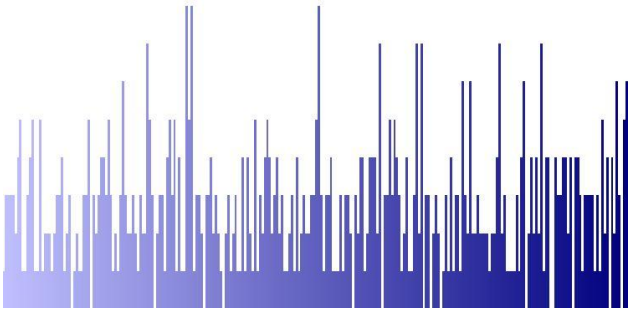
V. HASIL UJI COBA



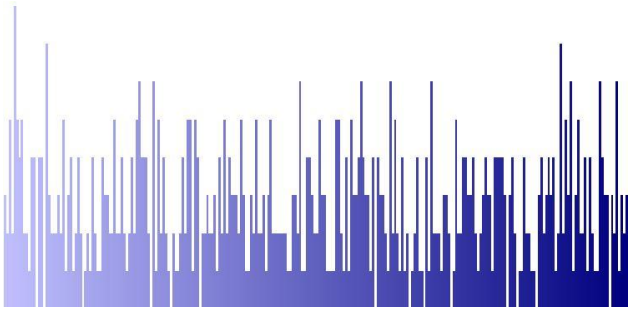
Gambar 2. Statistik P



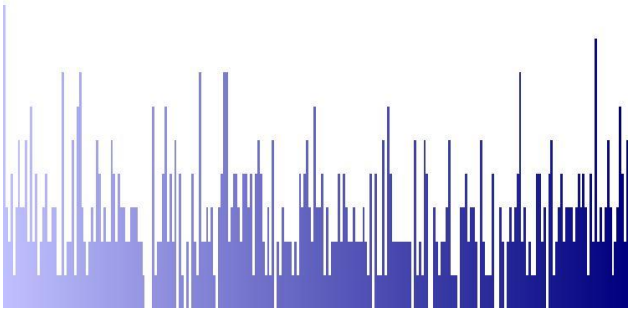
Gambar 3. Statistik P'



Gambar 4. Statistik Q



Gambar 5. Statistik Q'



Gambar 5. Statistik Q ⊕ Q'

Δ = 03 01 A0 00 50 40 00 01
∇ = 00 00 00 00 00 00 00 01

Dari uji coba, hasil yang didapat ialah Q ⊕ Q' ≠ Δ. Secara statistik hasil Q ⊕ Q' pun tidak menghasilkan suatu pola. Ini berarti algoritma Blowfish tahan terhadap serangan dengan metode boomerang attack. Meskipun begitu tidak menutup kemungkinan bahwa Blowfish dapat diserang dengan metode differential yang lain.

VI. REFERENSI

1. A.Shamir, E. Biham and. "Differential Cryptanalysis of the Data Encryption Standard." *Springer Verlag*, 1993.

2. Schneier, Bruce. "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)." *Springer Verlag*, 1993: 191-204.

3. Shanon, C. E. "Communication Theory of Secrecy Systems." 1949.

4.Wagner, David. "The boomerang attack." 1999.

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, 29 April 2010

Mufi Yanuar Triputranto / 13510106