ABSTRAKSI

Di penelitian ini dibahas perbandingan dua metode differential attack MD5. Metode differential attack pada MD5 digunakan untuk menemukan pasangan dua blok data yang masing-masing memiliki nilai digest MD5 yang sama. Dua metode tersebut adalah teknik yang dikemukakan Jun Yajima dkk. dan teknik yang dikemukakan Xiaoyun Wang dkk.. Keduanya memberikan teknik differential untuk menemukan pasangan 2 blok data kolisi.

Data kolisi dicari secara *exhaustive* dengan melibatkan parameter kondisi variabel tiap iterasi dan parameter selisih (difference) variabel tiap iterasi. Parameter-parameter ini yang digunakan sebagai acuan pencarian exhaustive pasangan 2 blok data.

Perbandingan dua teknik ini dilakukan dengan pencarian pasangan blok kedua dengan data input pasangan blok pertama. Pengujian teknik Jun dengan memberi input pasangan blok pertama data milik Wang ke pencarian pasangan blok kedua teknik Jun serta sebaliknya untuk pengujian teknik Wang. Pengujian kedua adalah pengujian parameter kondisi. Pasangan 2 blok data yang kolisi diinputkan ke parameter kondisi masing-masing teknik, dengan demikian diketahui parameter suatu teknik yang memberikan hasil terpenuhi atau tidak terpenuhi. Parameter kondisi teknik Jun menerima input pasangan 2 blok data valid yang berasal dari pencarian teknik Wang serta sebaliknya untuk pengujian parameter kondisi Teknik Wang.

Hasil pengujian menunjukkan bahwa teknik pencarian milik Jun lebih banyak memberikan hasil dan lebih cepat daripada teknik pencarian Wang. Lebih umum lagi dikatakan bahwa teknik pencarian Wang adalah subset dari teknik pencarian Jun.

Kata kunci : MD5, Collision, Kriptanalisa, Differential Attack