# ABSTRAK

MD5 merupakan sebuah algoritma kriptografi *hash function* yang banyak digunakan sebagai *digital signature* dari sebuah *file* atau sebagai enkripsi ketika menyimpan *password* dalam *database*. Salah satu cara untuk menembus sebuah enkripsi *hash function* adalah *brute-forcing* dengan teknik *exhaustive key search*. Teknik kriptanalisis ini terbilang mudah, tetapi memiliki konsekuensi kebutuhan komputasi yang tinggi. Untuk mengatasi konsekuensi tersebut, pendekatan komputasi paralel digunakan dan dijalankan pada dua GPU kelas *high-end* dengan menggunakan dua bahasa, yaitu CUDA dan OpenCL.

Pengujian dalam penelitian ini menggunakan 1 s/d 9 digit *random string*/*random password*, yang berdasar dari 65 macam karakter. Berdasarkan set karakter tersebut, ada 2 skenario pengujian yang dilakukan. Hasil penelitian menunjukkan sebuah *high-end* GPU relatif memiliki batas kemampuan kriptanalisis hingga 9 karakter *random password*, dengan waktu kriptanalisis terlama bisa mencapai lebih dari 1 minggu. Sedangkan untuk perbandingan performansi, OpenCL pada GPU AMD menghasilkan performa kriptanalisis terbaik jika dibandingkan dengan CUDA & OpenCL yang dijalankan pada GPU NVIDIA.

Kata Kunci: MD5, Kriptanalisis, CUDA, OpenCL, GPU.