Pendahuluan

1.1 Latar belakang

Dengan berkembangnya teknologi, kehidupan kita pada saat ini banyak didukung oleh kriptografi, mulai dari *plaintext, e-mail*, transaksi di e-*banking*, transaksi di perbankan, percakapan di telepon, SMS, sampai pengaktifan Rudal menggunakan teknik kriptografi. Menurut John Wiley and Sons, *Cryptography is the art and science of keeping messages secure*[1]. Artinya kriptografi adalah seni dan ilmu untuk menjaga kemananan pesan, disebut seni karena seperti yang kita lihat pada masa lalu, orang-orang menggunakan cara unik serta berbeda-beda dalam menyampaikan sebuah pesan. Seperti misalnya dengan menuliskan pesan tersebut dan hanya dapat dibaca dengan menggulungkan pesan tersebut menggunakan bantuan batang kayu yang diameternya telah ditentukan, atau menggubah isi pesan menjadi *plaintext-plaintext* tertentu. Hal inilah yang membuat kriptografi menjadi sebuah ilmu dan memiliki seni karena cara penyampaian dari pemilik pesan ke penerima pesan memiliki cara yang unik.

Ada berbagai macam algortima kriptografi mulai dari algoritma kripogafi klasik sampai algoritma kriptografi *modern*, dari yang menggunakan *key* simetri sampai yang menggunakan *key* publik (Nir-simetri). Ada pula algoritma kriptografi dengan menggunakan fungsi HASH. Ada pula yang memodifikasi kriptografi dengan mengambil kelebihan serta meminimalisir kekurangan yang terdapat pada kriptografi tersebut sehingga menghasilkan kriptografi yang lebih baik dari pada kriptografi sebelumnya.

Selain kriptografi berkembang pula kriptanalisis, kriptanalisis adalah ilmu atau seni untuk memecahkan *plaintext* kriptografi. Kriptanalisis merupakan lawan dari kriptografi. Metode yang paling sederhana dan mudah dalam melakukan kriptanalisis adalah *Brute Force attack*. *Brute Force* adalah metode yang mencoba semua kemungkinan yang ada untuk memecahkan *plaintext*. Tetapi *Brute Force* mempunyai kompleksitas waktu yang sangat lama sehingga waktu yang diperlukan untuk memecahkan *plaintext* menjadi sangat lama.

Selain berkembangnya kriptografi dan kriptanalisis, berkembang pula *hardware* untuk komputasi kinerja tinggi, salah satunya adalah GPU (*Graphics Processing Unit*). GPU saat ini dapat memanipulasi tekstur dan simpul dengan operasi yang sama pada CPU (*Central Processing Unit*) dan menjadikan warna-warna dengan presisi yang tinggi. Karena sebagian besar perhitungan melibatkan matriks dan operasi vektor, insinyur dan ilmuwan telah mempelajari penggunaan GPU untuk perhitungan non-grafis, contohnya yaitu gererasi

uk menyelesaikan ñfungsi hashò.Saat ini GPU memiliki framebuffer (biasanya dengan kesesuaian mode VGA). Seiring dengan berkembangnya GPU berkembang pula CUDA (*Compute Unified Device Architecture*). CUDA adalah platform komputasi dan model pemrograman paralel diciptakan oleh NVIDIA. Memanfaatkan NVIDIA GPU mesin komputasi paralel, CUDA lebih efisien dalam memecahkan banyak tugas komputasi kompleks daripada CPU[2].

Pada tugas akhir ini penulis ingin menganalisa RC4yang dipecahkan oleh *Brute Force* dengan menggunakan GPU serta melihat kinerja dari GPU tersebut untuk memecahkan *plaintext* pada RC4.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah pada Tugas Akhir ini, maka dapat di rumusan masalah yang akan dibahas yaitu:

1. Bagaimana mengimplementasikan kriptanalisis dengan metode*Brute Force* dengan menggunakan CPU dan GPU.
2. Bagaimana kinerjakriptanalisis dengan metode *Brute Force* pada CPU dan GPU.

1.3 Batasan Masalah

Pada Tugas Akhir ini permasalahan dibatasi dengan beberapa batasan yaitu:

1. Kriptanalisis yang digunakan adalah *Brute Force.*
2. *Plaintext* berupa teks dari A-Z, a-z, 0-9 tanpa simbol.
3. Metode yang digunakan RC4
4. Panjang *plaintext* dari 1 sampai 6 karakter

1.4 Tujuan

Berdasarkan pada rumusan masalah yang telah ditetapkan pada Tugas Akhir ini maka tujuan dari Tugas Akhir ini adalah:

1. Dapat mengimplementasikan kriptanalisis dengan metode*Brute Force* menggunakan CPU dan GPU.
2. Dapat melakukan analisis kinerja CPU dan GPU dalam menjalankan algoritma*Brute Force*.

ligunakan untuk menyelesaikan Tugas Akhir ini adalah sebagai berikut:

1. Studi Literatur

   Studi Literatur dalam metodologi yang pertama adalah untuk mencari, mengumpulkan, dan mempelajari referensi yang bersumber dari jurnal-jurnal internasional, buku-buku, maupun sumber lain dari internet maupun intranet sebagai dasar teori dalam tugas akhir ini. Referensi yang digunakan khususnya yang berkaitan dengan kriptografi, *Brute Force*, kriptanalisis, CUDA dan GPU.

2. Perancangan Sistem

   Metodologi ini dilakukan untuk merancang alur sistem yang akan dibuat.

3. Implementasi Sistem

   Setelah melakukan perancangan sistem, Pada metodologi ini adalah tahap pengimplementasian sistem ke dalam program sesuai dengan hasil perancangan yang telah dibuat.

4. Analisis Hasil Implementasi Sistem

   Metodologi ini digunakan untuk menganalisis hasil implementasi untuk menjawab rumusan masalah yang telah dibuat.

5. Pembuatan Laporan Tugas Akhir

   Pembuatan laporan Tugas Akhir dilakukan untuk mendokumentasikan pengerjaan tugas akhir ke dalam bentuk yang tertulis.

1.6 Sistematika Penulisan

Sistematika penulisan digunakan untuk menyusun laporan Tugas Akhir agar terdokumentasi dengan baik, adapun sistematika penulisan Tugas Akhir ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab pertama yaitu pendahuluan akan dipaparkan mengenai latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, dan sistematika penulisan tugas akhir.

BAB 2 DASAR TEORI

Pada bab kedua yaitu dasar teori akan dipaparkan mengenai dasar-dasar teori yang mendukung penyelesaian tugas akhir.

AN DAN IMPLEMENTASI

lisis perancangan dan implementasi akan dijelaskan mengenai proses analisis perancangan dan implementasi yang dibangun secara jelas dan terperinci.

BAB 4 ANALISIS HASIL PENGUJIAN

Pada bab keempat yaitu analisis hasil pengujian akan dijelaskan hasil dari analisis perancangan dan implementasinya mengenai parameter-parameter dan kinerja akurasi pada metode yang digunakan dalam sistem yang telah buat pada bab analisis perancangan dan implementasi.

BAB 5 PENUTUP

Pada bab terakhir ini akan diuraikan kesimpulan dari hasil analisis yang telah dilakukan penulis. Serta saran-saran untuk pengembangan tugas akhir selanjutnya.