KRIPTANALISIS DENGAN METODE *BRUTE FORCE* PADA *GRAPHICS PROCESSING UNIT*

Rafiqa Humaira[1], Fitriyani, S.Si., M.T[2], Nurul Ikhsan, S.Si., M.Si[3]

[1,2,3]Prodi Ilmu Komputasi Telkom University, Bandung

[1]**rafiqahumaira22@gmail.com**, [2]**fitriyani.y@gmail.com**, [3]**nurul.ikhsan@yahoo.co.id**

Abstrak

Kriptografi adalah seni dan ilmu untuk menjaga kemananan pesan. Selain kriptografi berkembang pula kriptanalisis, kriptanalisis adalah ilmu atau seni untuk memecahkan plaintext 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.

Pengujian dalam penelitan ini menggunakan kriptografi RC4. Panjang plaintext dan panjang key yang digunakan 1 s/d 6 karakter. Hasil penelitian menunjukkan bahwa semakin panjang plaintext semakin lama waktu yang diperlukan untuk menemukan plaintext sedangkan panjang key tidak berpengaruh terlalu besar dalam memecahkan plaintext. GPU lebih unggul dari CPU saat panjang plaintext lebih dari 3 karakter, dengan persentase 23.11% pada saat 6 karakter panjang plaintext.

Kata kunci : Brute force, CPU, GPU, RC4

Abstract

Cryptography is the art and science to maintain security message. In addition to developing well cryptanalysis cryptography, cryptanalysis is the science or art to decode cryptography. The most simple method and easy to do cryptanalysis is Brute Force attack. Brute Force is trying all possible methods available to crack the password.

Testing in this research using RC4 cryptography. Password length and key length used 1 s / d 6 characters. The results showed bahw the longer the password the longer it takes to find a password lock has no effect while the length is too big to suss password. GPU is superior to the current CPU password length is more than 3 characters. with a percentage of 23.11 % during the 6 characters long plaintext.

Keywords: Brute force, CPU, GPU, RC4

1. Pendahuluan

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].

kriptanalisis adalah ilmu atau seni untuk memecahkan plaintext 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. 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 jurnal ini penulis menganalisa RC4 yang dipecahkan oleh Brute Force dengan menggunakan GPU serta melihat kinerja dari GPU tersebut untuk memecahkan plaintext pada RC4.

2. Kriptografi

Kriptografi adalah seni dan ilmu untuk menjaga kemananan pesan.[1] 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.

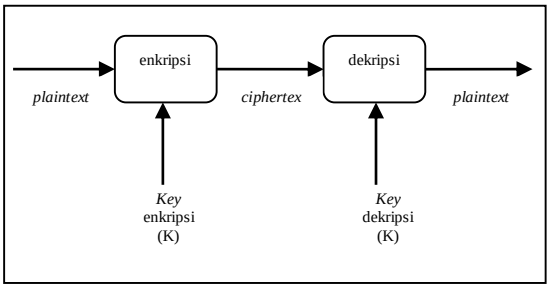
2.1 Kriptografi simetri

Kriptografi simteris atau bisa disebut kriptografi klasik merupakan kriptografi yang hanya mempunyai satu key yaitu key rahasia (pivate)[1].

Kriptografi simtris dapat digambarkan dari diagram proses dibawah ini:

Kriptografi simteris atau bisa disebut kriptografi klasik merupakan kriptografi yang hanya mempunyai satu key yaitu key rahasia (pivate)[1].

Kriptografi simtris dapat digambarkan dari diagram proses pada gambar 2



Gambar 2 proses kriptografi simetris

Dapat dilihat pada gambar 2 kriptografi simetris merupakan kriptografi yang mempunyai *key* enkripsi dan *key* dekripsi yang sama (*key* enkripsi = *key* dekripsi). Algoritma dari kriptografinya dapat disebut dengan algoritma simetri atau algoritma konvensional.

2.2 RC4

Salah satu algortima kriptografi Simetri adalah algoritma Rivest Code 4 atau yang biasa disebut RC4 yaitu salah satu algoritma key simetris yang dibuat oleh RSA Data *Security Inc* (RSADSI) yang berbentuk stream chipper. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu: Rivest Shamir Adleman). Algortima kriptografi RC4 ini menggunakan panjang key dari 1 sampai 256 bit yang digunakan untuk menginisialisasikan tabel sepanjang 256 bit[1].

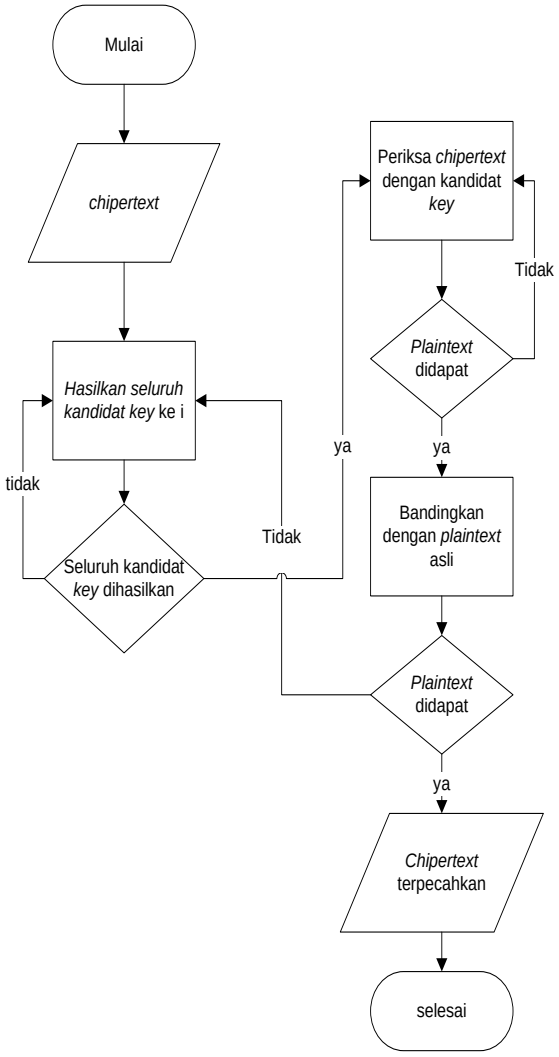
Berikut adalah *psudocode* RC4:

```
        //inisialisasi larik state
        for i = 0 to 255
               fqa[i]:= i
        end for
        //menjalankan KSA
        for i=0 to 255
               j=(key[i%key.Length]+
               fqa[i] + j) % 256
                x = fqa[i]
                swap (fqa [i], fqa [j])
                fqa[j] = x
        end for
        //menjalankan PRGA
        for i=0 to 255
               y = i % 256
                j = (fqa[y] + j) % 256
                x = fqa[y]
                swap (fqa [i], fqa [j])
                fqa[j] = x
               output(input[i]^
               fqa[(fqa[y]+fqa[j])
               %256])
      end for
```

3. Brute Force

Brute Force atau dikenal juga dengan istilah *exhaustive search* merupakan teknik serangan pada *plaintext* dengan mencoba semua kemungkinan. Tetapi merupakan teknik serangan yang sangat boros kerena memerlukan kompleksitas waktu yang besar. Kompleksitas waktu dari *Brute Force* dapat dilihat dari iterasi algoritmanya.

Kelebihan dari *Brute Force* adalah sederhana, mudah, dan pasti menemukan jawabannya. Sedangkan kekurangan dari *Brute Force* adalah tidak efisien, lambat dan tidak kreatif.



Gambar 2 diagram alir kriptanalisis menggunakan brute force

4. GPU

Graphics Processing Unit atau yang biasa disebut dengan GPU diperkenalkan pertama kali pada tanggal 31 Agustus 1999 untuk industri personal computer (PC). Definisi dari GPU adalah prosesor chip tunggal yang terintegrasi dengan transformasi, pencahayaan, pengaturan segitiga, dan mampu memproses minimal 10 juta persegi per detik. [5]

5. CUDA

CUDA adalah platform komputasi paralel dan model pemrograman yang diciptakan oleh NVIDIA. Hal ini memungkinkan peningkatan dramatis dalam kinerja komputasi dengan memanfaatkan kekuatan dari graphics processing unit (GPU). Dengan jutaan GPU CUDA-*enabled* terjual hingga saat ini, pengembang perangkat lunak, ilmuwan dan peneliti menemukan penggunaan luas mulai untuk komputasi GPU dengan CUDA[6].

Dengan memanfaatkan NVIDIA GPU menjadi mesin komputasi paralel, CUDA lebih efisien dalam memecahkan banyak tugas komputasi kompleks daripada CPU[7]. CUDA juga menyediakan metode yang eksplisit untuk mengatur arsitektur memorinya, sehingga meningkatkan seluruh kinerja dari aplikasinya.

6. Spesifikasi prangkat

Spesifikasi prangkat yang digunakan adalah sebagai berikut:

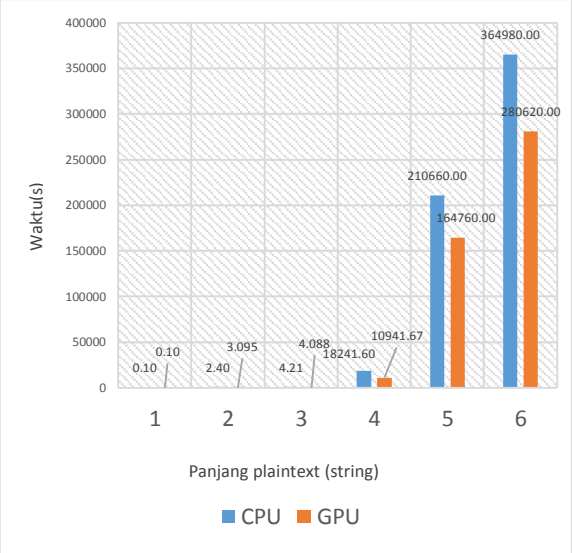
a. Bahasa pemrograman : C#, CUDAFY
b. Perangkat Lunak untuk development : Microsoft Visual Studio 2010
c. Perangkat Keras: Lenovo B490, Nvidia geforce 705M 1GB, i3-3110M (2.4 GHz, Cache 3MB), RAM 4 GB DDR3, 500 GB HDD
d. Sistem Operasi: Windows 7, 64 bit

7. Hasil dan Analisis

Setelah dilakukan penelitian didapatkan hasil pengujian kriptanalisis, beberapa hal yang dapat dianalisis terkait dengan implementasi, kinerja serta tingkat akurasi selama pengujian berlangsung.

7.1 Pengaruh Panjang *plaintext* pada pemecahan *plaintext*

Dari 6 percobaan berdasarkan panjang plaintext didapat rata-rata waktu CPU dan GPU.



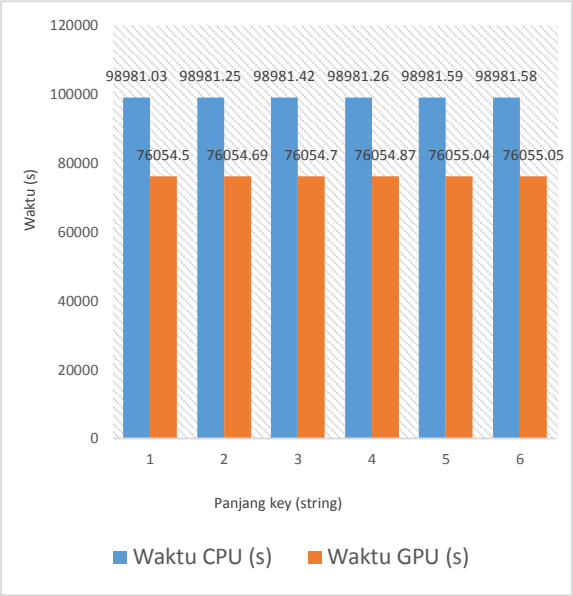
Tabel 1 Waktu rata-rata CPU dan GPU berdasaran panjang *plaintext*

Dapat dilihat dari Tabel 1, panjang plaintext 1 s/d 3 karakter, chipertext dapat dipecahkan dalam hitungan kurang dari 5 detik. Peningkatan waktu yang signifikan dari panjang plaintext 4 karakter menjadi 18,241.6 detik pada CPU dan 10,941.67 detik pada GPU, dengan selisih perbandingan adalah 40.02% . Waktu terus dengan signifikan naik saat panjang plaintext 5 karakter menjadi 210,660 detik pada CPU dan 164,760 detik pada GPU, dengan selisih perbandingan adalah 21.79%. Dan terakhir pada panjang plaintext 6 karater waktu yang dihasilkan semakin naik yaitu 364,980 detik pada CPU dan 280,620 detik pada GPU, dengan selisih perbandingan adalah 23.11%.

Hal ini terjadi karena semakin panjang jumlah plaintext semakin lama iterasi yang diperlukan untuk mencari dan menggembalikan chipertext menjadi plaintext. Saat jumlah plaintext adalah 1 maka kemungkinan yang dicari hanya sebatas A-Z, a-z, 0-9. Saat jumlah plaintext adalah 2 maka kemungkinan yang dicari meningkat. Sampai jumlah plaintext adalah 6 maka iterasi yang dihasilkan sangatlah banyak. Inilah yang menyebabkan panjang key sangat mempengaruhi waktu yang dihasilkan untuk memecahkan plaintext.

7.2 Pengaruh panjang *key* pada pemecahan *plaintext*

Dari 6 percobaan berdasarkan panjang key didapat rata-rata waktu CPU dan GPU.



Tabel 2 Waktu rata-rata CPU dan GPU berdasaran panjang *key*

Dari percobaan panjang key 1, 2, 3, 4, 5 dan 6. Dapat dilihat dari Tabel 4-4 dan Grafik 4-6 perbedaan waktu pada setiap percobaan tidak terlalu signifikan, ini dikarenakan pencarian panjang key terjadi pada awal pemecahan plaintext. Sedangkan lama penghasilan karakter plaintext tergantung pada panjang plaintext.

7.3 Perbandingan waktu rata-rata GPU dan CPU

Dari percobaan yang telah dilakukan didapatkan waktu rata-rata pada CPU dan GPU, hasil perbandingan waktu rata-rata antara CPU dan GPU dapat dilihat pada Tabel 4-13 dan grafik 4-3. Pada tabel 4-13 dapat dilihat bahwa saat plaintext berjumlah 1, 2 dan 3 karakter CPU lebih unggul walaupun tidak terlalu besar perbedaan yang dihasilkan. Sedangkan untuk plaintext yang melebihi 3, yaitu 4, 5 dan 6 karakter perbandingannya terlihat dengan jelas. Faktor yang menyebabkan hal ini terjadi saat chipertext dipecahkan menggunakan CPU iterasi yang dilakukan sangat banyak karena dilakukan secara serial sedangkan pada GPU pengerjaan iterasi dibagi ke dalam thread dan blocks yang dilakukan secara paralel sehingga iterasi yang terjadi pada GPU lebih singkat daripada pada CPU.

8. Kesimpulan

Dari hasil pengujian dan analisis sistem yang telah dilakukan, dapat diambil kesimpulan sebagai berikut:

a. Proses kriptanalisis dengan metode brute force pada CPU dan GPU telah berhasil diimplementasikan. Semakin panjang plaintext yang diinputkan maka semakin besar waktu yang diperlukan untuk memecahkan chipertext. Panjang key tidak terlalu mempengaruhi waktu yang diperlukan untuk memecahkan chipertext.

b. Perbandingan CPU dan GPU, Pada panjang plaintext 1-3 karater hanya terlihat perbedaan waktu yang tidak singnifikan walaupun CPU lebih unggul, tetapi pada panjang plaintext 4-6 sangat terlihat jelas perbedaan waktu yang dihasilkan. Pada plaintext 6 karakter. CPU memerlukan waktu 364,980s, dan sedangkan pada GPU hanya memerlukan waktu 280,620s dengan kata lain lebih singkat

Daftar Pustaka:

[1] Munir, Rinaldi. 2006. *Kriptografi*, Informatika

[2] Li, Qinjian. *Implementation and Analysis of AES Encryption on GPU*. Center for High Performance Computing. Northwestern Polytechnical University, China.

[3] Nishikawa, Iwai, & Kurokawa. *High-Performance Symmetric Block Ciphers on CUDA. Dept. of Computer Science. National Defense Academy of Japan.*

[4] Suryani, Karina Novita. 2009. *Algoritma RC4 sebagai metode enkripsi.* Sekolah Teknik Elektro dan Informatika ITB.

[5] http://www.nvidia.com/object/gpu.html

[6] http://www.nvidia.com/object/cuda_home_new.html

[7] Purnomo, DKK. *Implementasi Algoritma Kriptografi RC4 Pada DSP TMS320C6713 Sebagai Pendukung Sekuritas Jaringan Komunikasi Voice over Internet Protocol(VoIP).* Jurnal EECCIS Vol. 6, No. 2, Desember 2012