ANALISA PERBANDINGAN DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4, RC4-2S, DAN RC4ITZ PADA ARSITEKTUR MULTIPROSESOR

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar

Sarjana Komputer (S.Kom.)

Joshua Alamsyah

12110110094

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG

2016

HALAMAN PEGESAHAN SKRIPSI

ANALISA PERBANDINGAN DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4, RC4-2S, DAN RC4ITZ PADA ARSITEKTUR MULTIPROSESOR

Oleh

Nama	:	Joshua Alamsyah
NIM	:	12110110094
Program Studi	:	Teknik Informatika
Fakultas	:	Teknologi Informasi dan Komunikasi

Tangerang, 22 Agustus 2016

Ketua Sidang	Dosen Penguji
Seng Hansun, S.Si., M.Cs.	Marcel Bonar Kristanda, S.Kom., M.Sc.
Dosen Pembimbing I	Dosen Pembimbing II
Hargyo Nugroho, S.Kom., M.Sc.	Ranny, S.Kom., M.Kom.

Mengetahui,
Ketua Program Studi
Teknik Informatika

Maria Irmina Prasetiyowati, S.Kom., M.T.

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya,

Nama : Joshua Alamsyah

NIM : 12110110094

Program Studi : Teknik Informatika

Fakultas : Teknologi Informasi dan Komunikasi

menyatakan bahwa skripsi yang berjudul "Analisa Perbandingan dan Implementasi Algoritma Kriptografi RC4, RC4-2S, dan RC4itz pada Arsitektur Multiprosesor" ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari ditemukan kecurangan atau penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 22 Agustus 2016

Joshua Alamsyah

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya sehingga penulis mampu menyelesaikan skripsi yang berjudul "Analisa Perbandingan dan Implementasi Algoritma Kriptografi RC4, RC4-2S, dan RC4itz pada Arsitektur Multiprosesor" dengan baik.

Dalam menyusun skripsi ini penulis mendapat banyak bantuan dari berbagai pihak, oleh sebab itu izinkan penulis mengucapkan terima kasih sebanyak-banyaknya kepada:

1. Dr. Ninok Laksono, selaku Rektor Universitas Multimedia Nusantara.
2. Kanisius Karyono, S.T., M.T., Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Maria Irmina Prasetiyowati, S.Kom, M.T., selaku ketua program studi Teknik Informatika Universitas Multimedia Nusantara.
4. Hargyo Nugroho, S.Kom., dan Ranny, S.Kom., M.Kom., M.Sc., selaku dosen-deosen pembimbing yang telah membimbing pembuatan skripsi dan memberi arahan dan saran selama proses skripsi sehingga skripsi ini dapat terselesaikan tanpa adanya halangan.
5. Sahabat-sahabat penulis yang saling memberikan dukungan dan bantuan dalam menyelesaikan skripsi.
6. Dosen dan pegawai Universitas Multimedia Nusantara yang telah membantu penulis sehingga skripsi ini dapat terselesaikan.
7. Orang tua dan keluarga penulis yang telah memberikan banyak bantuan dan dukungan kepada penulis.
8. Pihak-pihak lain yang tidak dapat disebutkan satu per satu dan telah membantu penulis dan memberikan dukungan selama pengerjaan skripsi.

Semoga skripsi ini dapat bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi, bagi para pembaca, terutama rekan-rekan mahasiswa di Universitas Multimedia Nusantara.

Tangerang, Agustus 2016

Joshua Alamsyah

ANALISA PERBANDINGAN DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI RC4, RC4-2S, DAN RC4ITZ PADA ARSITEKTUR MULTIPROSESOR

ABSTRAK

Kriptografi atau enkripsi merupakan salah satu metode pengamanan dokumen berbentuk digital. Salah satu algoritma enkripsi berbentuk *stream cipher* adalah RC4. Kecepatan dari algoritma RC4 dalam melakukan proses enkripsi merupakan salah satu hal yang disegani oleh penggunanya. Namun, seiring waktu, terdapat serangan-serangan yang memanfaatkan kelemahan dari algoritma RC4 seperti serangan korelasi *state tables*. Oleh sebab tersebut, dirancanglah varian dari algoritma RC4 yaitu RC4-2S dan RC4itz. Arsitektur multiprosesor merupakan sebuah arsitektur yang menggunakan prosesor dari CPU dan juga GPU untuk melakukan komputasi. Implementasi algoritma-algoritma kriptografi RC4 dan variannya dalam arsitektur multiprosesor dipilih untuk meningkatkan performa dari algoritma RC4 dan variannya. Dari permasalahan sebelumnya, disusunlah penelitian untuk menganalisa perbandingan RC4, RC4-2S, dan RC4itz dalam sebuah implementasi arsitektur multiprosesor dengan menggunakan API CUDA. Penelitian dilakukan dalam empat uji coba dan mengenkripsi dokumen digital berbentuk pdf dengan ukuran berbeda. Setelah uji coba telah selesai dilaksanakan, diperoleh hasil akhir berupa rata-rata peningkatan tertinggi sebesar 1585% untuk algoritma RC4, peningkatan tertinggi sebesar 2808% untuk algoritma RC4-2S, dan peningkatan tertinggi sebesar 5181% untuk algoritma RC4itz dalam implementasi algoritma pada arsitektur multiprosesor serta hasil analisa perbandingan performa dari algoritma kriptografi RC4, RC4-2S, dan RC4itz.

Kata Kunci: Arsitektur Multiprosesor, CUDA, Kriptografi, RC4, RC4-2S, RC4itz

ANALYSIS AND IMPLEMENTATION OF RC4, RC4-2S, AND RC4ITZ CRYPTOGRAPHIC ALGORITHM IN A MULTIPROCESSOR ARCHITECTURE

ABSTRACT

Cryptography or encyrption is a method of securing a digital document. RC4 is a *stream cipher* based encryption algorithm. One of the key factors of RC4 was its speed in encrypting data. As the algorithm was gradually being used, there has been attacks that exploited the weaknesses of the algorithm such as the 'state-table correlation' attack. As a result, variants of RC4 algorithm such as RC4-2S and RC4itz were developed to overcome RC4's weakness and improve its performance. A multiprocessor architecture make use of the processing power of CPU and GPU to make computations. Implementation of each algorithm in the multiprocessor architecture was proposed in order to increase the performance of RC4 and its variants. For the reasons stated above, a research was conducted in order to analyse the different performance of each encryption algorithm in a multiprocessor architecture implementation using the CUDA API. Four experiments were conducted to implement RC4, RC4-2S and RC4itz in the multiprocessor architecture by ecrypting different sized digital documents. The result of the research was a maximum average increase of 1585% for RC4's performance, 2808% increase for RC4-2S' performance, and 5181% increase for RC4itz's performance for their implementation in a multiprocessor architecture as well as a performance analysis for each encryption.

Key Words: CUDA, Cryptography, Multiprocessor Architecture, RC4, RC4-2S, RC4itz

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR RUMUS