Perpustakaan Universitas Budi Luhur

PERANCANGAN IMPLEMENTASI SHA-1 *PASSWORD CRACKING* BERBASIS FPGA:

Studi Kasus Instansi XYZ

TESIS

Oleh:

SITI ZAIM

1111600423

PROGRAM STUDI: MAGISTER ILMU KOMPUTER

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2013

Perpustakaan Universitas Budi Luhur

PERANCANGAN IMPLEMENTASI SHA-1 *PASSWORD CRACKING* BERBASIS FPGA:

Studi Kasus Instansi XYZ

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer

Oleh:

SITI ZAIM

1111600423

PROGRAM STUDI: MAGISTER ILMU KOMPUTER

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2013

Perpustakaan Universitas Budi Luhur

PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama Mahasiswa : SITI ZAIM
Nomor Induk Mahasiswa : 1111600423
Program Studi : MAGISTER ILMU KOMPUTER
Konsentrasi : REKAYASA KOMPUTASI TERAPAN
Fakultas/Program : PASCA SARJANA

Menyatakan bahwa Tesis yang berjudul:

PERANCANGAN SHA-1 PASSWORD CRACKING BERBASIS FPGA : STUDI KASUS INSTANSI XYZ

1. merupakan hasil karya tulis ilmiah saya sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik pihak lain,
2. saya ijinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 16 PEBRUARI 2013

(SITI ZAIM)

Catatan: isian ditulis tangan

Perpustakaan Universitas Budi Luhur

PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa	:	Siti Zaim
Nomor Induk Mahasiswa	:	1111600423
Konsentrasi	:	Rekayasa Komputasi Terapan
Jenjang Studi	:	Strata 2
Judul	:	Perancangan SHA-1 *Password Cracking* Berbasis FPGA: Studi Kasus Instansi XYZ

Jakarta, 16 Pebruari 2013

Tim Penguji: Tanda Tangan:

Ketua,
Dr. Ir. Nazori AZ, M.T. .....

Anggota,
Dr. Moedjiono, M.Sc. .....

Hadi Syahrial, M.M, M.KOM .....

Pembimbing Utama,
Dr. Ir. Nazori, AZ, M.T. .....

Pembimbing Pendamping,
Hadi Syahrial, M.M, M.KOM .....

Ketua Program Studi

Dr. Ir. Nazori AZ, M.T.

Perpustakaan Universitas Budi Luhur

ABSTRAK

Seiring berkembangnya teknologi informasi dan komunikasi yang pesat, saat ini terdapat banyak layanan *software* yang menyediakan sistem otentikasi yang berdasarkan pada kombinasi identitas pengguna (*username*) dan *password*. *Password* tersebut disimpan dalam bentuk *digest* yang dihasilkan dari perhitungan menggunakan skema fungsi hash tertentu, salah satunya SHA-1. Instansi XYZ merupakan instansi pemerintah yang bergerak dalam bidang pengamanan informasi. Instansi XYZ membutuhkan kecepatan komputasi untuk melakukan kriptanalisis termasuk *password cracking* di dalamnya. FPGA merupakan salah satu teknologi komputasi dengan performansi tinggi. Pada penelitian ini dilakukan perancangan implementasi SHA-1 *password cracking* berbasis FPGA. SHA-1 *password cracking* dilakukan dengan menggunakan metode *brute force attack.* Hasil penelitian ini membuktikan bahwa FPGA dapat lebih cepat dari *Personal Computer* (PC) dalam melakukan SHA-1 *password* cracking. Hasil akhir dari penelitian ini berupa rancangan implementasi SHA-1 *password cracking* berbasis FPGA bagi Instansi XYZ. Dengan menggunakan rancangan ini, Instansi XYZ dapat melakukan *password cracking* dengan lebih cepat sehingga informasi dapat lebih cepat disampaikan kepada pimpinan guna pengambilan keputusan dan mendukung pencapaian misi organisasi.

Kata kunci: kriptografi, fungsi hash, *password cracking* , SHA-1, dan FPGA

Perpustakaan Universitas Budi Luhur

ABSTRACT

The development of communication and information technologies has increased dramatically. Nowadays, there are many software services that provide authentication system based on user ID (username) and password combination. Passwords are stored in digest, generated using a specific hash function schemes, such as SHA-1. XYZ Agency is a government agency engaged in information security. XYZ Agency requires computing speed to perform cryptanalysis including password cracking. FPGA is one of the high performance in computing platform. This research will be carried out the design implementation of SHA-1 password cracking based on FPGA. The design using brute force attack method to perform SHA-1 password cracking. The result of this research proof that FPGA can perrform SHA-1 password cracking faster than personal computer. The end results of this research is a draft implementation of SHA-1 password cracking based on FPGA for XYZ Agency. By implementing the design, the XYZ agency can perform password cracking faster so that the information can be delivered to the leaders quickly for decision making and support of the organization's mission.

***Keywords**: cryptography, hash function, password cracking, SHA-1, and FPGA*

Perpustakaan Universitas Budi Luhur

KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Alhamdulillah, segala puji dan syukur senantiasa terpanjatkan kehadirat Allah SWT yang telah berkenan memberikan rahmat dan ridhoNya, sehingga penyusunan tesis berjudul "PERANCANGAN SHA-1 PASSWORD CRACKING BERBASIS FPGA: Studi Kasus Instansi XYZ" dapat selesai tepat waktu. Rasa terima kasih dan penghargaan setulusnya penulis sampaikan kepada:

1. Ayah, Ibu, Kakak dan Adik yang senantiasa memberikan kasih sayang, cinta, semangat dan pengorbanan serta do'a yang tak senantiasa mengalir.
2. Bapak Dr. Ir. Nazori AZ, M.T, Bapak Hadi Syahrial, M.M, M.KOM, Bapak Dr. Moedjiono, M.Sc dan Bapak Assoc. Prof. Dr. Teddy Mantoro atas masukan dan saran yang diberikan dalam peyusunan tesis.
3. Abang, Mbak, dan adik rekans Subdit Nalkripto atas segala bantuan, semangat dan motivasi yang diberikan.
4. Teman, Saudari, Adikku Nitia dan Ica, *thanks for everything*, yakin optimis berbuah manis, *good memories, we make it!*
5. Sacha Moleller, Daniel Siebert, *Steffen* Möller, Jost Bissel, Gerd Pfeiffer, and Tim Pietruck, *thank you so much for sharing knowledge freely, It's amazing*!
6. Mas Coudry, Mbak Ifah, Nahot, dan rekans MKOM UBL 2011.

Tak ada yang sempurna, karena kesempurnaan hanya milikNya. Penulis menyadari tesis ini masih jauh dari sempurna. Untuk itu penulis mengharapkan kritik dan saran untuk penulisan penelitian yang lebih baik. Saran dan kritik dapat dkirimkan ke alamat email bealfathunnisa@gmail.com.

Wassalamu'alaikum Wr.Wb

Jakarta, Pebruari 2013

@lfathunnisa

Perpustakaan Universitas Budi Luhur

DAFTAR ISI

Perpustakaan Universitas Budi Luhur

Perpustakaan Universitas Budi Luhur

DAFTAR GAMBAR

Perpustakaan Universitas Budi Luhur

DAFTAR TABEL

Perpustakaan Universitas Budi Luhur

DAFTAR LAMPIRAN

Perpustakaan Universitas Budi Luhur

DAFTAR PUSTAKA

[Alkalbani 2010] Alkalbani, Abdullah Said, Mantoro, Teddy, Osman, Abu., Comparison between RSA Hardware and Software Implementation for WSNs Security Schemes. *Proceeding 3rd International Conference on ICT4M* , (2010): 84-89.

[Chu 2008] Chu, Pong P., "*FPGA Prototyping by VHDL Examples: Xilinx Spartan -3 Version*", New Jersey: John Wiley & Sons, Inc., 2008.

[FIPS 2012] _____."*FIPS PUB 180 – 4: Secure Hash Standard (SHS)*". Gaithersburg: FIPS Publication. 2012.

[Fischer 2007] Fischer, Thorsten. "Everyday Password Cracking". *IRM Research White Paper*, IRM PLC, (Desember, 2007): 16 pages.

[Guneysu 2009] Guneysu, Tim, Erhan."Cryptography and Cryptanalysis on Reconfigurable Devices." Ph.D, diss,. Ruhr-University Bochum, 2009.

[Hanamakumar 2011] Hanamakumar, Veerla, Syamsundar. "Cost-Efficient SHA Hardware Accelerator". *IJAEST*, vol.no.5, (2011): 37-52.

[Hulton 2009] Hulton, David, Hur, Mark. "Using FPGA Cluster for Fast Password Recovery". *A Pico Computing Data Security White Paper.*(November, 2009): 4 pages.

[Jarvinen 2004] Jarvinen, Kimmo. "Design and Implementation of a SHA-1 Module on FPGAs". 2004.

[Kumar 2006] Kumar, asndeep, Paar, Christof. "Breaking Ciphet with COPACOBANA – A Cost-Optimized Parallel Code Breaker". *IACR Proceeding.* 2006.

[Kusbandono 2004] Kusbandono, Arif., "Implementasi Algoritma AES-128 pada Mikrokontroler 8051." Bachelor Thesis, Institut Teknologi Bandung, Bandung, 2004.

[Menezes 1996] Menezes, Alfred J., Oorschot, Paul C. , "*Handbook of Applied Cryptography*", Waterloo: CRC Press, 1996.

[Simon 2007] Marechal, Simon. "Advances in password cracking" . *J Comput Virol*, vol.4, (2008):73-81.