UNIVERSITAS BINA NUSANTARA

Program Studi Ganda

Teknik Informatika – Matematika

ANALISIS DAN PERANCANGAN PROGRAM SIMULASI PENGAMANAN DATA TRANSMISI *SDR* DENGAN MENGGUNAKAN KRIPTOGRAFI METODE *SERPENT*

Michael Kohan

NIM : 0700687362

ABSTRAK

Dewasa ini, sistem komunikasi merupakan hal yang sangat penting. Salah satu alat komunikasi canggih yang banyak digunakan sekarang ini adalah *Software Defined Radio* (*SDR*). Tetapi keamanan data yang ada pada transmisi radio tidak aman karena data dapat dicuri dengan berbagai macam cara.

Untuk menyelesaikan masalah keamanan transmisi data melalui radio, *Serpent Advanced Encryption Standard* (*AES*) digunakan sebagai metode kriptografi untuk mengamankan data yang akan ditransmisikan melalui *SDR*.

Untuk mengimplementasikan kriptografi pada *SDR* ini dibutuhkan komponen yang dapat melakukan operasi-operasi aritmatik. Komponen *Field-Programmable Gate Array* (*FPGA*) adalah komponen yang cocok untuk melakukan proses kriptografi pada *SDR*.

Tujuan penelitian ini adalah untuk merancang sebuah program simulasi yang akan menggambarkan pengamanan data transmisi *SDR* dengan menerapkan algoritma *Serpent AES*. Hasil yang dicapai pada penelitian ini adalah deskripsi proses simulasi transmisi SDR yang telah diamankan dengan kriptografi dan pembuktian keamanannya. Selain itu juga didapat pembuktian keefektifan pengamanan data dengan kriptografi metode *Serpent*.

Kata Kunci: *Software Defined Radio, Field-Programmable Gate Array, Symmetric Cryptography, Cryptography, Serpent, Advanced Encryption Standard*

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa atas segala rahmat, anugerah, penyertaan serta penghiburan-Nya sehingga skripsi yang berjudul "Analisis dan Perancangan Program Simulasi Pengamanan Data Transmisi *SDR* Dengan Menggunakan Kriptografi Metode Serpent" ini dapat diselesaikan dengan baik dan tepat pada waktunya.

Atas segala bantuan, bimbingan serta kesempatan bagi penulis untuk menyelesaikan skripsi ini, maka perkenankanlah penulis untuk menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Geraldus Polla, M.App.Sc., selaku Rektor Universitas Bina Nusantara, yang telah berkenan memberikan kesempatan untuk menuntut ilmu kepada penulis di Universitas yang berada di bawah pimpinan beliau.
2. Bapak Wikaria Gazali, S.Si., MT., selaku Dekan dan Ketua Jurusan Matematika Fakultas MIPA Universitas Bina Nusantara atas perhatian, pertolongan dan pengajaran yang telah diberikan selama ini.
3. Bapak Rojali, S. Si., selaku Sekretaris Jurusan Matematika Fakultas MIPA Universitas Bina Nusantara atas perhatian, pertolongan dan pengajaran yang telah diberikan selama ini.
4. Bapak Fredy Purnomo, S.Kom.,M. Kom., selaku Ketua Jurusan Teknik Informatika Fakultas TI Universitas Bina Nusantara atas perhatian, pertolongan dan pengajaran yang telah diberikan selama ini.
5. Bapak Gintoro, S.Kom., MM, selaku Dosen Pembimbing kesatu atas yang telah banyak memberikan bantuan dan bimbingan yang diberikan selama masa penyusunan skripsi ini serta atas pengertian, pengajaran, pertolongan dan kesabarannya yang memudahkan skripsi ini terselesaikan tepat pada waktunya.
6. Bapak Sangadji, Drs., M.Sc., Ph.D, selaku Dosen Pembimbing kedua yang telah banyak memberikan bantuan dan bimbingan yang diberikan selama masa penyusunan skripsi ini serta atas pengertian, pengajaran, pertolongan dan kesabarannya yang memudahkan skripsi ini terselesaikan tepat pada waktunya.
7. Seluruh Dosen Universitas Bina Nusantara yang selama ini telah memberikan ilmu dan bimbingan akademis kepada penulis dari awal hingga akhir perkuliahan.
8. Keluarga penulis, atas doa, kasih, kesabaran, dan dukungan yang diberikan kepada penulis selama penyusunan skripsi ini.
9. Irene Vimala Tisnabudi dan Leonardus Henry Liwardy berserta keluarga mereka yang selama ini banyak memberi masukan informasi yang berarti mengenai penulisan skripsi ini dan dukungan baik dalam bentuk materi maupun moral.

10. Teman-teman seperjuangan yaitu Pascal Gerardus Angriawan dan Mery Yanti yang selama ini banyak memberi masukan informasi yang berarti mengenai penulisan skripsi ini.
11. Teman-teman jurusan ganda Teknik Informatika–Matematika angkatan 2003 atas dukungan dan bantuannya yang diberikan kepada penulis selama ini.
12. Pihak-pihak lain yang tidak dapat disebutkan satu per satu yang telah mendukung dan membantu penulis dalam penyelesaian skripsi ini.

Walaupun telah berusaha dengan sebaik mungkin dalam menyelesaikan skripsi ini, penulis menyadari begitu banyak kekurangan-kekurangan yang ditemukan dalam penulisan skripsi ini. Dengan segala kerendahan hati, penulis sangat menghargai segala saran dan kritik yang membangun dari para pembaca untuk penyempurnaan skripsi ini dimasa yang akan datang. Merupakan suatu kebahagiaan bagi penulis apabila penulisan skripsi ini dapat memberikan manfaat yang sebesar-besarnya kepada para pembaca.

Jakarta, 21 Januari 2008
Penulis

Michael Kohan
0700687362

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN