

DAFTAR ISI

| | |
|----------------------------------|-------------|
| Halaman Judul | ii |
| Halaman Pengesahan | iii |
| Halaman Pernyataan | iv |
| Halaman Persembahan | v |
| Halaman Motto | vi |
| PRAKATA | vii |
| DAFTAR ISI | ix |
| DAFTAR TABEL | xii |
| DAFTAR GAMBAR | xiii |
| INTISARI | xv |
| ABSTRACT | xvi |
| I PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 3 |
| 1.3 Batasan Masalah | 3 |
| 1.4 Tujuan Penelitian | 4 |
| 1.5 Manfaat Penelitian | 4 |
| 1.6 Sistematika Penulisan | 4 |
| II TINJAUAN PUSTAKA | 6 |
| III LANDASAN TEORI | 8 |
| 3.1 Kriptografi | 8 |
| 3.2 <i>Finite State Automata</i> | 10 |
| 3.3 Protokol <i>Ping-Pong</i> | 12 |

| | | |
|-----------|--|-----------|
| 3.3.1 | Definisi | 12 |
| 3.3.2 | Algoritma Pengujian Keamanan | 16 |
| 3.4 | <i>Breadth-First Search</i> | 20 |
| IV | RANCANGAN PENELITIAN | 24 |
| 4.1 | Permasalahan Umum | 24 |
| 4.2 | Desain Algoritma | 25 |
| 4.2.1 | Algoritma Pengujian Keamanan Protokol <i>Ping-Pong</i> | 25 |
| 4.2.2 | Algoritma Pembuatan <i>Counterexample</i> | 25 |
| 4.3 | Rancangan Program | 32 |
| 4.3.1 | <i>Input</i> Program | 32 |
| 4.3.2 | Penyimpanan <i>Input</i> | 33 |
| 4.3.3 | Pembentukan NFA | 33 |
| 4.3.4 | Pembentukan Relasi Reruntuhan | 34 |
| 4.3.5 | Pencarian <i>Counterexample</i> | 34 |
| 4.3.6 | <i>Output</i> | 37 |
| 4.4 | Rancangan Pengujian | 38 |
| V | IMPLEMENTASI | 39 |
| 5.1 | Praproses | 39 |
| 5.1.1 | Pengindeksan Operator | 39 |
| 5.1.2 | <i>Cancellation Rules</i> | 40 |
| 5.2 | Pengolahan <i>Input</i> | 40 |
| 5.3 | Pembentukan NFA | 41 |
| 5.4 | Pembentukan Relasi Reruntuhan | 42 |
| 5.5 | Pencarian <i>Counterexample</i> | 43 |
| 5.5.1 | Pembuatan Graf | 43 |
| 5.5.2 | Penelusuran | 43 |
| 5.6 | <i>Output</i> | 44 |
| VI | HASIL DAN PEMBAHASAN | 51 |
| 6.1 | Protokol 1 | 51 |
| 6.2 | Protokol 2 | 52 |
| 6.3 | Protokol 3 | 54 |
| 6.4 | Protokol 4 | 56 |
| 6.5 | Protokol 5 | 58 |

| | | |
|------------|-----------------------|-----------|
| 6.6 | Protokol 6 | 60 |
| 6.7 | Protokol 7 | 62 |
| VII | PENUTUP | 65 |
| 7.1 | Kesimpulan | 65 |
| 7.2 | Saran | 65 |
| | DAFTAR PUSTAKA | 66 |