

DAFTAR ISI

| | |
|---|------|
| HALAMAN JUDUL PETAMA..... | i |
| HALAMAN JUDUL KEDUA | ii |
| LEMBAR PENGESAHAN TUGAS AKHIR..... | iii |
| LEMBAR PENGESAHAN PENGUJI SIDANG..... | iv |
| LEMBAR PERTANGGUNGJAWABAN MATERI | v |
| ABSTRAK | vi |
| KATA PENGANTAR | vii |
| DAFTAR ISI..... | ix |
| DAFTAR GAMBAR | xii |
| DAFTAR TABEL | xiii |
| | |
| BAB I PENDAHULUAN..... | 1 |
| 1.1. Latar Belakang Masalah..... | 1 |
| 1.2. Perumusan Masalah..... | 2 |
| 1.3. Batasan Masalah..... | 2 |
| 1.4. Tujuan dan Manfaat Penelitian | 3 |
| 1.5. Metode Penelitian..... | 3 |
| 1.6. Sistematika Penulisan | 4 |
| | |
| BAB II LANDASAN TEORI | 6 |
| 2.1. Analisis | 6 |
| 2.2. Proses | 7 |
| 2.3. Enkripsi | 8 |
| 2.3.1. <i>Conventional Cryptosystem</i> | 10 |
| 2.3.2. <i>Public Key Cryptosystems</i> | 12 |
| 2.4. Sistem | 14 |

| | | |
|-----------------------------------|---|----|
| 2.4.1. | Subsistem | 14 |
| 2.4.2. | Karakteristik Sistem | 15 |
| 2.5. | Keamanan | 18 |
| 2.5.1. | Klasifikasi Keamanan | 19 |
| 2.5.2. | Insiden Keamanan Jaringan | 21 |
| 2.6. | <i>Wired Equivalent Privacy (WEP)</i> | 25 |
| 2.6.1. | <i>Authentication</i> | 27 |
| 2.6.2. | Mekanisme WEP | 30 |
| 2.7 | <i>Firewal</i> | 32 |
| BAB III METODE ENKRIPSI WEP | | 37 |
| 3.1. | Operasi Kriptografi WEP | 37 |
| 3.2. | <i>Initialization Vector (IV)</i> | 38 |
| 3.3. | <i>Rivest Code 4</i> | 39 |
| 3.3.1. | Algoritma RC 4 | 40 |
| BAB IV HASIL DAN PEMBAHASAN | | 47 |
| 4.1. | Kelemahan <i>Wired Equivalent Privacy</i> | 47 |
| 4.2. | Metode-metode Serangan pada WEP | 51 |
| 4.2.1. | WEP <i>Brute Force</i> | 51 |
| 4.2.2. | Serangan <i>Bit-Flipping</i> | 51 |
| 4.2.3. | Serangan Fluhrer, Martin, dan Shamir (FMS) | 54 |
| 4.2.4. | Serangan <i>Initialization Vector (IV) Replay</i> | 55 |
| 4.3 | Perbaikan pada WEP | 59 |
| 4.3.1 | <i>Wired Equivalent Privacy 2 (WEP2)</i> | 59 |
| 4.3.2 | <i>Wi-Fi Protected Access (WPA)</i> | 60 |

| | | |
|-------|----------------------------|----|
| BAB V | KESIMPULAN DAN SARAN | 62 |
| 5.1. | Kesimpulan | 62 |
| 5.2. | Saran-saran | 63 |

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

| | | |
|------------|---|----|
| Gambar 1.1 | Diagram Kegiatan Penelitian | 4 |
| Gambar 2.1 | Diagram Proses Enkripsi dan Dekripsi | 9 |
| Gambar 2.2 | Prinsip Dasar <i>Conventional Cryptosystem</i> | 10 |
| Gambar 2.3 | Operasi Transportasi | 11 |
| Gambar 2.4 | Prinsip Dasar <i>Public Key Cryptosystem</i> | 13 |
| Gambar 2.5 | Karakteristik Sistem | 15 |
| Gambar 2.6 | Skema Bit-bit dari WEP | 26 |
| Gambar 2.7 | Skema <i>Open System Authentication</i> | 27 |
| Gambar 2.8 | Skema <i>Shared Key Authentication</i> | 29 |
| Gambar 2.9 | Proses Enkripsi pada WEP | 31 |
| Gambar 3.1 | Operasi WEP | 36 |
| Gambar 3.2 | Enkripsi dengan menggunakan <i>Initalization Vector</i> | 39 |
| Gambar 3.3 | Skema Pemakaian RC 4 pada WEP..... | 43 |
| Gambar 4.1 | Kelemahan ICV | 52 |
| Gambar 4.2 | Serangan <i>Bit-Flipping</i> | 53 |
| Gambar 4.3 | Serangan <i>Initialization Vector Replay</i> | 55 |
| Gambar 4.4 | Ekspansi <i>Keystream</i> | 56 |

DAFTAR TABEL

| | | |
|-----------|--------------------------------------|----|
| Tabel 4.1 | Solusi Dari Celah Keamanan WEP | 58 |
|-----------|--------------------------------------|----|