

DAFTAR ISI

| | |
|--|------|
| HALAMAN PERSETUJUAN PENELITIAN S2 | ii |
| KATA PENGANTAR | iii |
| DAFTAR ISI | v |
| DAFTAR GAMBAR | viii |
| DAFTAR TABEL | x |
| INTISARI | xi |
| BAB I PENDAHULUAN | 1 |
| 1.1 Latar Belakang Masalah | 1 |
| 1.2 Rumusan Masalah | 3 |
| 1.3 Batasan Masalah | 3 |
| 1.4 Tujuan | 3 |
| 1.5 Manfaat | 4 |
| 1.6 Keaslian Penelitian | 4 |
| BAB II TINJAUAN PUSTAKA | 5 |
| BAB III LANDASAN TEORI | 9 |
| 3.1 RSA | 9 |
| 3.1.1 Pembangkitan Kunci | 9 |
| 3.1.2 Enkripsi | 10 |
| 3.1.3 Dekripsi | 11 |
| 3.2 Performa Enkripsi dan Dekripsi | 11 |
| 3.3 Multiple prime number RSA | 12 |
| 3.4 Serangan pada RSA | 13 |
| 3.4.1 Serangan pada sisi hardware | 13 |
| 3.4.2 Serangan pada sisi <i>software</i> | 14 |
| 3.5 <i>Metric</i> Evaluasi | 18 |
| BAB IV METODOLOGI PENELITIAN | 20 |
| 4.1 Deskripsi Penelitian | 20 |
| 4.2 Tahapan Penelitian | 20 |

| | | |
|-----------------------------------|--|----|
| 4.3 | Desain Sistem Kripto | 23 |
| 4.3.1 | <i>Small Public Key Exponent</i> | 23 |
| 4.3.2 | <i>Small Private Key Exponent</i> | 25 |
| 4.3.3 | <i>Small Prime Number</i> | 27 |
| 4.4 | Rancangan Serangan | 28 |
| 4.4.1 | Small Public Key Exponent Attack | 28 |
| 4.4.2 | Small Private Key Exponent Attack | 30 |
| 4.4.3 | Small Prime Number Attack | 31 |
| 4.5 | Rancangan Evaluasi | 33 |
| BAB V IMPLEMENTASI | | 36 |
| 5.1 | Alat dan Bahan | 36 |
| 5.2 | Pembangkitan Kunci dan <i>Plaintext</i> | 36 |
| 5.2.1 | Small Public Key Exponent | 37 |
| 5.2.2 | Small Private Key Exponent | 39 |
| 5.2.3 | Small Prime Number | 41 |
| 5.3 | Eksplorasi Sistem Kriptografi | 43 |
| 5.3.1 | Small Public Key Exponent | 44 |
| 5.3.2 | Small Private Key Exponent | 46 |
| 5.3.3 | Small Prime Number | 48 |
| BAB VI HASIL DAN PEMBAHASAN | | 52 |
| 6.1 | Analisis skema <i>small public key exponent</i> | 52 |
| 6.1.1 | Hasil untuk Public Key Exponent 3 | 52 |
| 6.1.2 | Hasil untuk Public Key Exponent 5 | 53 |
| 6.1.3 | Hasil untuk Public Key Exponent 7 | 55 |
| 6.2 | Analisis skema <i>small private key exponent</i> | 57 |
| 6.3 | Analisis skema <i>small prime number</i> | 57 |
| 6.4 | Pembahasan Hasil Evaluasi Serangan | 62 |
| 6.4.1 | Pembahasan hasil evaluasi serangan small public key exponent | 63 |

| | |
|---|----|
| 6.4.2 Pembahasan hasil evaluasi serangan small private key exponent | 64 |
| 6.4.3 Pembahasan hasil evaluasi serangan small prime number | 65 |
| BAB VII KESIMPULAN DAN SARAN | 67 |
| 7.1 Kesimpulan | 67 |
| 7.2 Saran | 67 |
| DAFTAR PUSTAKA | 68 |