

DAFTAR ISI

BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	6
1.3 Tujuan Penelitian	7
1.4 Batasan Masalah	7
1.5 Manfaat Penelitian	7
1.6 Kontribusi Penelitian	8
BAB II TINJAUAN PUSTAKA.....	9
2.1 Penelitian terkait Modifikasi Algoritma RSA	9
2.2 Penelitian terkait Model Otentikasi	15
2.3 Penelitian terkait Model Pengamanan Pengiriman Data	25
BAB III DASAR TEORI	34
3.1 Pemantauan Radiasi	34
3.2 Keamanan Jaringan Komputer	37
3.3 Kerahasiaan Data.....	40
3.3.1 Sistem kriptografi	40
3.3.2 Kriptografi kunci simetri	42
3.3.3 Kriptografi kunci asimetri.....	44
3.3.4 Kinerja sistem kriptografi	47
3.4 Keutuhan Data.....	49
3.5 Otentikasi Pesan dan Entitas Pengirim.....	52
BAB IV METODOLOGI PENELITIAN	55
4.1 Sistem Berjalan.....	55
4.2 Rancang Bangun Model	56
4.3 Perangkat Eksperimen	61
4.4 Data Pengujian	63
4.5 Pengujian Model.....	66
4.5.1. Kinerja komputasi	66
4.5.2. Kinerja keamanan	68
4.5.3. Kinerja jaringan	73

BAB V SISTEM KRIPTOGRAFI EPNR	74
5.1 Konsep Multi-prima <i>EPNR</i>	74
5.2 Algoritma <i>EPNR</i>	76
5.3 Eksperimen Eksekusi Algoritma <i>EPNR</i>	78
5.4 Analisis Kinerja Komputasi Algoritma <i>EPNR</i>	81
5.4.1 Durasi pembangkitan kunci	81
5.4.2 Durasi enkripsi	85
5.4.3 Durasi dekripsi	87
5.5 Analisis Kinerja Keamanan Algoritma <i>EPNR</i>	88
5.5.1 Nilai Avalanche effect	89
5.5.2 Nilai entropi Shannon	90
5.5.3 Ketahanan terhadap Wiener attack	91
5.5.4 Ketahanan terhadap Factorization attack.....	92
5.6 Perbandingan Modifikasi Algoritma <i>RSA</i>	96
BAB VI MODEL OTENTIKASI PERANGKAT BARU	100
6.1 Model Otentikasi Awal	100
6.2 Eksperimen Eksekusi Model Otentikasi.....	106
6.3 Analisis Kinerja Komputasi Model Otentikasi	108
6.3.1. Durasi pembangkitan kunci	108
6.3.2. Durasi enkripsi	110
6.3.3. Durasi dekripsi	111
6.3.4. Total durasi proses otentikasi	113
6.4 Analisis Kinerja Keamanan Model Otentikasi	114
6.4.1 Ketahanan terhadap Statistical attack	114
6.4.2 Ketahanan terhadap Replay attack	116
6.4.3 Ketahanan terhadap MITM attack	118
6.5 Analisis Kinerja Jaringan Model Otentikasi	123
6.5.1 Throughput.....	124
6.5.2 Waktu tunda.....	126
6.6 Perbandingan dengan Model Otentikasi pada Sistem Lain.....	128
BAB VII MODEL PENGAMANAN PENGIRIMAN DATA	136
7.1 Model Pengamanan Pengiriman Data	136
7.2 Eksperimen Eksekusi Model Pengamanan Pengiriman Data.....	141
7.3 Analisis Kinerja Komputasi Model Pengamanan Pengiriman Data sisi	
<i>Client</i>	143
7.3.1. Durasi pembangkitan kunci asimetri	143

7.3.2. Durasi enkripsi ganda terhadap ID _s	145
7.3.3. Durasi dekripsi terhadap kunci AES terenkripsi.....	147
7.3.4. Durasi enkripsi data dengan kunci AES	148
7.3.5. Durasi pembangkitan Hash(Data).....	149
7.3.6. Durasi pengiriman data	150
7.4 Analisis Kinerja Komputasi Model Pengamanan Pengiriman Data sisi	
Server	151
7.4.1. Durasi pembangkitan kunci RSA	152
7.4.2. Durasi dekripsi ganda terhadap Hash(ID _s) terenkripsi	153
7.4.3. Durasi pembangkitan kunci AES.....	154
7.4.4. Durasi enkripsi terhadap kunci AES.....	154
7.4.5. Durasi penerimaan data	155
7.4.6. Durasi dekripsi data terenkripsi AES.....	156
7.4.7. Durasi pengecekan nilai Hash(Data)	157
7.5 Analisis Kinerja Keamanan Model Pengamanan Pengiriman Data	158
7.5.1 Keamanan pertukaran kunci AES.....	158
7.5.2 Ketahanan terhadap Brute Force attack	158
7.5.3 Ketahanan terhadap MITM attack	159
7.5.4 Ketahanan terhadap pemalsuan data.....	162
7.6 Analisis Kinerja Jaringan Model Pengamanan Pengiriman Data.....	163
7.6.1 Throughput pengiriman data.....	165
7.6.2 Waktu tunda.....	166
7.7 Perbandingan dengan Model Pengamanan Pengiriman Data pada Sistem	
Lain	168
BAB VIII PENUTUP	177
8.1 Kesimpulan	177
8.2 Saran	180
DAFTAR PUSTAKA	181
LAMPIRAN A.....	194
LAMPIRAN B	196
LAMPIRAN C.....	200
LAMPIRAN D	207