

DAFTAR ISI

HALAMAN JUDUL	ii
HALAMAN PENGESAHAN	iii
PERNYATAAN	iv
HALAMAN PERSEMBAHAN	v
PRAKATA.....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xiii
DAFTAR TABEL.....	xv
INTISARI	xvi
ABSTRACT.....	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian.....	5
1.5 Kontribusi Penelitian	5
BAB II TINJAUAN PUSTAKA	6
2.1 Penelitian terkait Keamanan SCADA	6
2.2 Penelitian terkait Peningkatan Keamanan Protokol DNP3	8
2.3 Penelitian terkait Keamanan Transmisi Data dalam SCADA	16
BAB III LANDASAN TEORI	21

3.1 SCADA.....	21
3.2 Transmisi Data pada SCADA	22
3.3 Protokol DNP3	23
3.4 Keamanan Data	25
3.5 <i>Cipher</i> Beaufort	27
3.6 <i>Cipher</i> RC4.....	27
3.7 Super Enkripsi	29
BAB IV METODOLOGI PENELITIAN	30
4.1 Gambaran Umum	30
4.1.1 <i>Model Sistem Berjalan</i>	32
4.1.2 <i>Usulan Model Penelitian</i>	33
4.2 Metodologi Penelitian	34
4.2.1 <i>Studi Literatur</i>	34
4.2.2 <i>Model Super Enkripsi</i>	35
4.2.3 <i>Pengambilan Data</i>	35
4.2.4 <i>Pembacaan Data IL</i>	37
4.2.5 <i>Mengubah ke format satu baris</i>	37
4.2.6 <i>Pembangkitan kunci awal (K1)</i>	37
4.2.7 <i>Pembangkitan kunci Beaufort Enkripsi (K2)</i>	37
4.2.8 <i>Enkripsi Beaufort</i>	38
4.2.9 <i>Pembangkitan kunci RC4 Enkripsi (K3 & K4)</i>	38
4.2.10 <i>Enkripsi RC4</i>	44
4.2.11 <i>Pembangkitan kunci Beaufort Dekripsi (K2)</i>	45

4.2.12	<i>Pembangkitan kunci RC4 Dekripsi (K3 & K4)</i>	45
4.2.13	<i>Dekripsi RC4</i>	45
4.2.14	<i>Dekripsi Beaufort</i>	46
4.2.15	<i>Mengubah ke format data string banyak baris</i>	46
4.2.16	<i>Analisis Model</i>	46
a.	<i>Analisis Ruang Kunci</i>	46
b.	<i>Analisis Korelasi</i>	46
c.	<i>Analisis Entropi</i>	47
d.	<i>Analisis Kecepatan Proses</i>	48
e.	<i>Analisis Kompleksitas Waktu</i>	48
BAB V MODEL ENKRIPSI DARI SUPER ENKRIPSI BRC4.....		50
5.1	<i>Pembacaan data IL</i>	51
5.2	<i>Mengubah ke format satu baris numerik</i>	51
5.3	<i>Pembangkitan Kunci Awal Acak (K1)</i>	52
5.4	<i>Pembangkitan kunci Beaufort Enkripsi (K2)</i>	53
5.5	<i>Enkripsi Beaufort</i>	55
5.6	<i>Pembangkitan kunci RC4 enkripsi (K3 dan K4)</i>	56
5.7	<i>Enkripsi RC4</i>	60
BAB VI MODEL DEKRIPSI DARI SUPER ENKRIPSI BRC4.....		62
6.1	<i>Retrieve Kunci Awal Acak K1</i>	63
6.2	<i>Pembangkitan kunci Beaufort Dekripsi (K2)</i>	63
6.3	<i>Pembangkitan kunci RC4 Dekripsi (K3 dan K4)</i>	64
6.1	<i>Dekripsi RC4</i>	65

6.2 Dekripsi Beaufort	66
6.3 Model Akhir	67
BAB VII HASIL DAN ANALISIS	68
7.1 Hasil.....	68
7.1.1 Hasil Pembacaan Data IL-1 dari Program PLC.....	68
7.1.2 Hasil Mengubah Data IL-1 ke format satu baris.....	69
7.1.3 Hasil Konversi Data Plaintext menjadi Numerik	69
7.1.4 Hasil Pembangkitan kunci awal (K1).....	71
7.1.5 Hasil Pembangkitan Kunci Beaufort Enkripsi (K2)	72
7.1.6 Hasil Enkripsi Beaufort	73
7.1.7 Hasil Pembangkitan Kunci RC4 Enkripsi (K3 dan K4)	74
7.1.8 Hasil Enkripsi RC4	75
7.1.9 Hasil Pembangkitan Kunci Beaufort Dekripsi (K2)	76
7.1.10 Hasil Pembangkitan Kunci RC4 Dekripsi (K3 & K4)	77
7.1.11 Hasil Dekripsi RC4.....	77
7.1.12 Hasil Dekripsi Beaufort.....	78
7.1.13 Hasil Model Akhir.....	79
7.1.14 Hasil Simulasi Protokol DNP3	80
7.2 Analisis	88
7.2.1 Analisis Ruang Kunci.....	88
7.2.2 Analisis Korelasi.....	88
7.2.3 Analisis Entropi	90
7.2.4 Analisis Kecepatan Proses.....	91

7.2.5 Analisis Kompleksitas Waktu.....	96
BAB VIII PENUTUP	98
8.1 Kesimpulan.....	98
8.2 Saran.....	98
DAFTAR PUSTAKA	100
Lampiran 1 Kecepatan proses enkripsi dan dekripsi IL-1 (1.086 karakter)	111
Lampiran 2 Kecepatan proses enkripsi dan dekripsi IL-2 (7.158 karakter)	112
Lampiran 3 Kecepatan proses enkripsi dan dekripsi IL-3 (33.046 karakter).....	113
Lampiran 4 Kompleksitas Waktu Algoritma Enkripsi	114
Lampiran 5 Kompleksitas Waktu Algoritma Dekripsi	118
Lampiran 6 Program Proses Enkripsi	123
Lampiran 7 Program Proses Dekripsi	127
Lampiran 8 Data <i>Plaintext</i> IL-1, IL-2 dan IL-3	131