

DAFTAR ISI

PERNYATAAN	iii
HALAMAN PERSEMBAHAN	iv
HALAMAN MOTTO	v
PRAKATA	vi
DAFTAR ISI	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
INTISARI	xiv
ABSTRACT	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Keaslian Penelitian	4
1.7 Metodologi Penelitian	5
1.8 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	7
BAB III LANDASAN TEORI	14
3.1 Kriptografi	14
3.1.1 Kriptografi kunci simetri	17
3.1.2 Kriptografi kunci publik/asimetri	18
3.2 Pengantar Jaringan Syaraf Tiruan	21
3.2.1 Arsitektur jaringan syaraf	23
3.2.2 Jaringan syaraf tiruan <i>Radial Basis Function</i> (RBF)	25
3.2.3 Ukuran jarak	27
3.2.4 Fungsi aktivasi	28

3.2.5	Matriks, inverse dan pseudoinverse	30
3.2.6	Pembelajaran pada RBF	32
3.2.7	Bias	34
BAB IV ANALISIS DAN RANCANGAN SISTEM		35
4.1	Gambaran Umum Sistem	35
4.1.1	Ilustrasi pembangkitan kunci	40
4.1.2	Ilustrasi enkripsi dan dekripsi	41
4.2	Perancangan Arsitektur Jaringan Syaraf Tiruan	42
4.2.1	Perancangan arsitektur <i>training</i> jaringan syaraf tiruan untuk pembangkitan kunci	42
4.2.2	Perancangan proses enkripsi menggunakan bagian jaringan syaraf tiruan	47
4.2.3	Perancangan proses dekripsi menggunakan bagian jaringan syaraf tiruan	48
4.3	Metode Enkripsi/Denkripsi	50
4.3.1	Proses pembangkitan kunci	50
4.3.2	Proses enkripsi	53
4.3.3	Proses dekripsi	55
4.4	Perancangan Sistem	57
4.4.1	<i>Data Flow Diagram</i> (DFD)	57
4.4.2	Perancangan antarmuka	61
4.5	Perhitungan Manual	63
4.5.1	Perhitungan manual proses pembangkitan kunci	63
4.5.2	Perhitungan manual proses enkripsi	72
4.5.3	Perhitungan manual proses dekripsi	76
BAB V IMPLEMENTASI SISTEM		80
5.1	Lingkungan Implementasi	80
5.2	Implementasi Aplikasi	80
5.2.1	Implementasi proses pembangkitan kunci	80
5.2.2	Implementasi proses enkripsi	89
5.2.3	Implementasi proses dekripsi	91

BAB VI HASIL DAN PEMBAHASAN	94
6.1 Pengujian.....	94
6.2 Pengujian Proses Pembangkitan Kunci	94
6.3 Pengujian Enkripsi Dekripsi untuk Kerahasiaan (<i>Confidentiality</i>).....	95
6.4 Pengujian Enkripsi Dekripsi untuk Autentikasi (<i>Authentication</i>)	97
6.5 Pengujian Enkripsi Dekripsi untuk Kerahasiaan Pesan dan Autentikasi	98
6.6 Analisis Sistem dan Perbandingan Metode.....	99
BAB VII PENUTUP	107
7.1 Kesimpulan	107
7.2 Saran	107
DAFTAR PUSTAKA	108