

## DAFTAR ISI

HALAMAN	
HALAMAN TESIS .....	i
HALAMAN PENGESAHAN .....	ii
PERNYATAAN .....	iii
PRAKATA.....	iv
DAFTAR ISI.....	v
DAFTAR GAMBAR .....	vii
DAFTAR TABEL.....	ix
INTISARI .....	x
ABSTRACT.....	xi
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian.....	3
1.6 Keaslian Penelitian .....	3
1.7 Metodologi Penelitian .....	3
1.8 Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA .....	6
BAB III LANDASAN TEORI.....	10
3.1 Kriptografi .....	10
3.2 Algoritme Kunci Simetri .....	10
3.3 Algoritme Kunci Asimetri .....	12
3.4 Playfair CBC .....	14
3.4.1 Enkripsi .....	14
3.4.2 Dekripsi.....	15
3.4.3 Elliptic Curve .....	16
3.5 REpresentational State Transfer .....	24
3.5.1 Memodelkan <i>resource</i> dengan POST .....	25
3.5.2 Memodelkan <i>resource</i> dengan GET .....	25
3.5.3 Memodelkan <i>resource</i> dengan PUT .....	26
3.5.4 Memodelkan <i>resource</i> dengan DELETE.....	27
3.5.5 Cara kerja REST .....	27
BAB IV ANALISIS DAN PERANCANGAN SISTEM.....	29
4.1 Analisis Sistem .....	29
4.2 Gambaran Umum Sistem .....	29
4.3 Perancangan Sistem.....	34
4.3.1 Proses pembangkitan kunci simetri .....	34
4.3.2 Proses pembangkitan kunci asimetri.....	38
4.3.3 Proses enkripsi .....	45

4.3.4	Proses dekripsi .....	54
4.4	Data Flow Diagram (DFD).....	61
4.5	Perancangan Antarmuka.....	65
<b>BAB V IMPLEMENTASI.....</b>		<b>72</b>
5.1	Implementasi Aplikasi.....	72
5.1.1	Implementasi proses pembangkitan kunci <i>Playfair CBC</i> .....	72
5.1.2	Implementasi proses pembangkitan kunci <i>Elliptic Curve</i> .....	72
5.1.3	Implementasi proses enkripsi.....	73
5.1.4	Implementasi proses dekripsi.....	74
<b>BAB VI HASIL DAN PEMBAHASAN .....</b>		<b>76</b>
6.1	Pengujian .....	76
6.1.1	Proses enkripsi dan dekripsi <i>Playfair CBC</i> .....	76
6.1.2	Proses enkripsi dan dekripsi <i>Elliptic Curve</i> .....	78
6.2	Analisis Hasil Implementasi Metode.....	79
6.2.1	Perhitungan sistem dan manual enkripsi, dekripsi <i>Playfair CBC</i> .....	79
6.2.2	Perhitungan sistem dan manual enkripsi, dekripsi <i>Elliptic Curve</i> ....	80
6.2.3	Penyerangan <i>Brute Force</i> pada <i>Playfair CBC</i> .....	81
6.2.4	Penyerangan <i>Brute Force</i> pada <i>Elliptic Cuve</i> .....	82
<b>BAB VII PENUTUP .....</b>		<b>84</b>
7.1	Kesimpulan.....	84
7.2	Saran .....	84
<b>DAFTAR PUSTAKA .....</b>		<b>85</b>
<b>LAMPIRAN.....</b>		<b>88</b>