

## DAFTAR TABEL

<b>Tabel 3.1</b>	Nilai korelasi menggunakan pola masukan kunci 1-2-3-4 .....	28
<b>Tabel 3.2</b>	Perbandingan rata-rata korelasi tiap pola.....	29
<b>Tabel 3.3</b>	Langkah pembangkitan s-box dinamis .....	30
<b>Tabel 3.4</b>	Spesifikasi tabel user .....	36
<b>Tabel 3.5</b>	Spesifikasi tabel mail .....	36
<b>Tabel 3.6</b>	Spesifikasi tabel attachment.....	37
<b>Tabel 3.7</b>	Spesifikasi tabel mail_map .....	38
<b>Tabel 4.1</b>	Perbandingan waktu rata-rata proses enkripsi per 500 block data....	41
<b>Tabel 4.2</b>	Hasil percobaan mode operasi ECB .....	44
<b>Tabel 4.3</b>	Hasil percobaan mode operasi CBC .....	45
<b>Tabel 4.4</b>	Hasil percobaan mode operasi CFB.....	47
<b>Tabel 4.5</b>	Hasil percobaan mode operasi OFB .....	49
<b>Tabel 4.6</b>	Hasil percobaan mode operasi CTR .....	51
<b>Tabel 4.7</b>	Daftar menu pada aplikasi surat elektronik .....	53
<b>Tabel 4.8</b>	Daftar fitur aplikasi surat elektronik.....	55

## DAFTAR GAMBAR

<b>Gambar 2.1</b>	Skema enkripsi dan dekripsi block cipher .....	6
<b>Gambar 2.2</b>	Transformasi subbytes .....	9
<b>Gambar 2.3</b>	Transformasi shiftrows.....	10
<b>Gambar 2.4</b>	Transformasi mixcolumns.....	10
<b>Gambar 2.5</b>	Matrix tetap dalam langkah transformasi mixcolumns .....	10
<b>Gambar 2.6</b>	Transformasi addroundkey.....	11
<b>Gambar 2.7</b>	S-box standard AES .....	12
<b>Gambar 2.8</b>	Invers s-box standard AES.....	12
<b>Gambar 2.9</b>	Operasi block cipher dengan ECB .....	13
<b>Gambar 2.10</b>	Operasi block cipher dengan CBC .....	14
<b>Gambar 2.11</b>	Operasi block cipher dengan CFB .....	14
<b>Gambar 2.12</b>	Operasi block cipher dengan OFB .....	15
<b>Gambar 2.13</b>	Operasi block cipher dengan CTR .....	15
<b>Gambar 3.1</b>	Skema proses enkripsi.....	24
<b>Gambar 3.2</b>	Skema proses dekripsi.....	25
<b>Gambar 3.3</b>	Pola pengambilan kunci .....	26
<b>Gambar 3.4</b>	Pola masukan matrix .....	27
<b>Gambar 3.5</b>	S-box berdasarkan kunci rahasia.....	31
<b>Gambar 3.6</b>	Inverse s-box berdasarkan kunci rahasia.....	31
<b>Gambar 3.7</b>	Arsitektur aplikasi email .....	32
<b>Gambar 3.8</b>	Diagram konteks aplikasi.....	32
<b>Gambar 3.9</b>	Diagram oveview aplikasi.....	33
<b>Gambar 3.10</b>	DFD proses 1.0.....	34
<b>Gambar 3.11</b>	DFD proses 2.0.....	34
<b>Gambar 3.12</b>	ERD aplikasi .....	35
<b>Gambar 3.13</b>	Rancangan antarmuka aplikasi.....	39
<b>Gambar 4.1</b>	Diagram Pengujian Avalance Effect.....	40
<b>Gambar 4.2</b>	Halaman utama aplikasi .....	52
<b>Gambar 4.3</b>	Form pembuatan surat baru.....	53
<b>Gambar 4.4</b>	Tampilan surat.....	54

## DAFTAR LAMPIRAN

Lampiran A Percobaan pola masukan kunci.....	A-1
Lampiran B Pengujian avalance effect .....	B-1
Lampiran C Simulasi waktu enkripsi.....	C-1