DAFTAR ISI

Halaman Pernyataan ii
Halaman Pengesahan iii
Halaman Persembahan iv
Kata Pengantar v
Abstrak vi
Abstract vii
Daftar Isi viii
Daftar Tabel x
Daftar Gambar xi
Daftar Lampiran xiii
Bab I Pendahuluan 1
1.1 Latar Belakang 1
1.2 Perumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Pembatasan Masalah 3
1.5 Sistematika Penulisan 4
Bab II Tinjauan Pustaka 5
2.1 Kajian Terkait 5
2.2 Block Cipher 6
2.2.1 Confusion dan Difusion 8
2.2.2 Advance Encryption Standard (AES) 9
2.2.3 Substitution Box (S-box) 11
2.2.4 Mode Operasi Block Cipher 13
2.3 Koefisien Korelasi 15
2.4 Avalance Effect 17
2.5 Notasi Big-O 17
2.6 Brute Force 18
Bab III Metodologi Penelitian 20
3.1 Metodologi Penelitian 20
3.1.1 Perangkat Penelitian 20
3.1.1.1 Alat Penelitian 20
3.1.1.2 Perangkat Lunak 21
3.1.1.3 Perangkat Keras 21
3.1.2 Metode Penelitian 21
3.2 Perancangan Kriptografi 22
3.2.1 Skema Enkripsi dan Dekripsi 23
3.2.2 Pola Pengambilan Kunci 26
3.2.3 S-box Dinamis 30
3.3 Perancangan Aplikasi Surat Elektronik 31

3.3.1 Arsitektur Aplikasi 32
3.3.2 Diagram Arus Data (DFD) 32
3.3.3 Entity Relationship Diagram (ERD) 35
3.3.4 Kamus Data 35
3.3.5 Antarmuka Aplikasi 39

Bab IV Implementasi dan Hasil 40

4.1 Analisis Keamanan 40
4.1.1 Avalance Effect 40
4.1.2 Simulasi Waktu 41
4.1.3 Brute Force 43
4.2 Mode Operasi Block Cipher 43
4.2.1 Electronic Code Book (ECB) 43
4.2.2 Cipher Block Chaining (CBC) 45
4.2.3 Cipher Feedback (CFB) 47
4.2.1 Output Feedback (OFB) 48
4.2.2 Counter (CTR) 50
4.3 Hasil Perancangan Aplikasi 52

Bab V Kesimpulan dan Saran 56

5.1 Kesimpulan 56
5.2 Saran 57

Daftar Pustaka 58