DAFTAR ISI

ABSTRAK…….....i
ABSTRACT…….....ii
KATA PENGANTAR……...…….....iii
DAFTAR ISI……...…….....iv
DAFTAR GAMBAR…...…….....x
DAFTAR TABEL ……...…….....xv
DAFTAR SIMBOL……..…….....xix
DAFTAR LAMPIRAN……...…….....xxiii

BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Identifikasi Masalah..... 3
1.3 Maksud dan Tujuan 3
1.4 Batasan Masalah..... 4
1.5 Metodologi Penelitian..... 4
1.6 Metode Pengumpulan Data 4
1.7 Metode Pembangunan Perangkat Lunak 5
1.8 Sistematika penulisan 6
BAB II TINJAUAN PUSTAKA 9
2.1 Profil Institusi 9
2.1.1 Sejarah Singkat Perusahaan 9
2.1.2 Visi dan Misi 12
2.1.2.1 Visi :..... 12
2.1.2.2 Misi : 12
2.1.3 Gedung Kantor Regional III BKN Bandung..... 12

2.1.4 Stuktur Organisasi 12
2.1.4.1 Tugas Pokok dan Fungsi 13
2.2 Landasan Teori 21
2.2.1 Kriptografi 21
2.2.2 RSA 26
2.2.3 DSA 28
2.2.4 Elgamal 31
2.2.5 Diffie-Hellman 33
2.2.5.1 Cara Kerja Protokol Pertukaran Kunci Diffie Hellman 34
2.2.5.2 Pembangkitan kunci dengan algoritma Diffie-Hellman 36
2.2.6 Algoritma Rijndael 39
2.2.7 Bahasa Pemrograman C# 43
2.2.8 OOP (Object Oriented Programming) 46
2.2.8.1 Mengenal Object-Oriented Programming dengan Bahasa C# . 48
2.2.8.2 Mengenal NET Framework dan C# 49
2.2.8.3 Common Language Runtime 50
2.2.8.4 Base Class Library 51
2.2.9 Microsoft Visual Studio 51
2.2.10 MySQL 52
2.2.11 UML 53
2.2.12 Aplikasi 59
2.2.13 XAMPP 60
BAB III ANALISIS DAN PERANCANGAN SISTEM 63
3.1 Analisis Sistem 63
3.1.1 Analisis Sistem Yang Sedang Berjalan 63

3.1.1.1 Analisis Proses Kerja Sistem 63
3.1.1.2 Prosedur Pengiriman File 63
3.1.1.3 Prosedur Pengambilan File 64
3.1.2 Analisis File 65
3.1.2.1 Analisis Jaringan 65
3.1.2.2 Skema Jaringan 66
3.1.2.3 Evaluasi Sistem Yang Sedang Berjalan 67
3.1.2.4 Analisis Sistem Yang Diusulkan 68
3.1.2.5 Analisis Masalah 68
3.1.2.6 Analisis Proses Kerja Sistem 68
3.1.2.7 Analisis Algoritma Diffie-Hellman 70
3.1.2.8 Analisis Algoritma Enkripsi Rijndael 72
3.1.2.9 Analisis Algoritma Dekripsi Rijndael 81
3.1.2.10 Analisis Manajemen Kunci 85
3.1.2.11 Analisis Kebutuhan Perangkat Keras 86
3.1.3 Analisis Perangkat Lunak 88
3.1.3.1 Analisis Pengguna Sistem 88
3.1.3.2 Spesifikasi Kebutuhan Perangkat Lunak 88
3.1.4 Analisis Kebutuhan Fungsional 89
3.1.4.1 Use Case Diagram 89
3.1.4.2 Skenario Use Case 90
3.1.5 Class Diagram 109
3.1.5.1 Sequence Diagram 111
3.2 Perancangan Sistem 118
3.2.1 Perancangan Basis Data 118

3.2.1.1 Skema Relasi 118
3.2.1.2 Struktur Tabel 119
3.2.2 Perancangan Struktur Menu 121
3.2.3 Perancangan Antarmuka 122
3.2.3.1 Perancangan Antarmuka Client 122
3.2.3.2 Perancangan Antarmuka Login Client 122
3.2.3.3 Perancangan Antarmuka Menu Utama Client 122
3.2.3.4 Perancangan Antarmuka Data Kunci 123
3.2.3.5 Perancangan Antarmuka Data File Terkirim 123
3.2.3.6 Perancangan Antarmuka Data File Diterima 124
3.2.3.7 Perancangan Antarmuka Bangkitkan Kunci 124
3.2.3.8 Perancangan Antarmuka Server 125
3.2.3.9 Perancangan Antarmuka Login Server 125
3.2.3.10 Perancangan Antarmuka Menu Utama Server 126
3.2.3.11 Perancangan Antarmuka Data Client 126
3.2.3.12 Perancangan Antarmuka Data file 127
3.2.4 Perancangan Pesan 127
3.2.4.1 Perancangan Pesan Username Harus Diisi (M01) 127
3.2.4.2 Perancangan Pesan Password Harus Diisi (M02) 127
3.2.4.3 Perancangan Pesan Login Sukses (M03) 128
3.2.4.4 Perancangan Pesan Username Dan Password Salah (M04) . 128
3.2.4.5 Perancangan Pesan Data Belum Dipilih (M05) 128
3.2.4.6 Perancangan Pesan Yakin Data Dihapus? (M06) 129
3.2.4.7 Perancangan Pesan Data Masih Kosong (M07) 129
3.2.4.8 Perancangan Pesan Data Berhasil Ditambah (M08) 129

3.2.4.9 Perancangan Pesan Data Berhasil Diedit (M09) 130
3.2.4.10 Perancangan Pesan Data Berhasil Dihapus (M10)..... 130
3.2.4.11 Perancangan Pesan Data Gagal Dihapus (M11) 130
3.2.4.12 Perancangan Pesan Data Gagal Diedit (M12)..... 131
3.2.4.13 Perancangan Pesan Data Gagal Dihapus (M13) 131
3.2.4.14 Perancangan Pesan Generate Kunci Berhasil (M14)..... 131
3.2.4.15 Perancangan Pesan Generate Kunci Gagal (M15) 132
3.2.4.16 Perancangan Pesan Upload Berhasil (M16)..... 132
3.2.4.17 Perancangan Pesan Upload Gagal (M17) 132
3.2.4.18 Perancangan Pesan Enkripsi Berhasil (M18)..... 133
3.2.4.19 Perancangan Pesan Enkripsi Gagal (M19)..... 133
3.2.4.20 Perancangan Pesan Download Berhasil (M20)..... 133
3.2.4.21 Perancangan Pesan Download Gagal (M21) 134
3.2.4.22 Perancangan Pesan Dekripsi Berhasil (M22)..... 134
3.2.4.23 Perancangan Pesan Dekripsi Gagal (M23) 134
3.2.5 Perancangan Jaringan Semantik..... 135
BAB IV IMPLEMENTASI DAN PENGUJIAN..... 137
4.1 Implementasi 137
4.1.1 Implementasi Perangkat Lunak..... 137
4.1.2 Implementasi Perangkat Keras..... 137
4.1.3 Batasan implementasi 138
4.1.4 Implementasi Antarmuka..... 138
4.1.4.1 Implementasi Antarmuka Client 138
4.1.4.2 Implementasi Antarmuka Login Server..... 143
4.2 Implementasi Basis Data..... 146

4.3 Pengujian Sistem 148
4.3.1 Rencana Pengujian 149
4.3.2 Pengujian *Black Box* 151
4.3.2.1 Pengujian pada Client 151
4.3.2.2 Pengujian pada Server 156
4.3.3 Pengujian Beta 159
4.3.3.1 Hasil Kuisioner Pengujian Beta 159
4.3.3.2 Kuisioner Aplikasi kriptografi untuk keamanan data 160
4.3.3.3 Kesimpulan Pengujian Beta 165
BAB V KESIMPULAN DAN SARAN 167
5.1 Kesimpulan 167
5.2 Saran 167
DAFTAR PUSTAKA 169