DAFTAR ISI

ABSTRAK ..... **Error! Bookmark not defined.**

ABSTRACK ..... **Error! Bookmark not defined.**

KATA PENGANTAR ..... iv**Error! Bookmark not defined.**

DAFTAR ISI v

DAFTAR GAMBAR ix

DAFTAR TABEL x

DAFTAR SIMBOL ..... **Error! Bookmark not defined.**

DAFTAR LAMPIRAN ..... **Error! Bookmark not defined.**

BAB 1 PENDAHULUAN ..... **Error! Bookmark not defined.**

1.1 Latar Belakang Masalah ..... **Error! Bookmark not defined.**

1.2 Identifikasi Masalah ..... **Error! Bookmark not defined.**

1.3 Maksud dan Tujuan ..... **Error! Bookmark not defined.**

1.4 Batasan Masalah ..... **Error! Bookmark not defined.**

1.5 Metodologi Penelitian ..... **Error! Bookmark not defined.**

1.5.1 Metode Pengumpulan Data ..... **Error! Bookmark not defined.**

1.5.2 Metode Pembangunan Perangkat Lunak **Error! Bookmark not defined.**

1.6 Sistematika Penulisan ..... **Error! Bookmark not defined.**

BAB 2 LANDASAN TEORI 9

2.1 Sejarah Kriptografi 9

2.1.1 Kriptografi ..... **Error! Bookmark not defined.**

2.1.2 Kriptografi Simetri ..... **Error! Bookmark not defined.**4

2.1.3 Kriptografi Asimetri ..... **Error! Bookmark not defined.**5

2.1.4 Protokol Kriptografi ..... **Error! Bookmark not defined.**7

2.2 RSA (Ron Rivest, Adi Shamir, dan Len Adleman) **Error! Bookmark not defined.**8

2.2.1 Oprasional RSA ..... **Error! Bookmark not defined.**9
2.2.2 Fungsi *Totient Euler φ* 20
2.2.3 Algoritma Pembangkitan Kunci..... **Error! Bookmark not defined.**1
2.2.4 Proses Enkripsi Pesan ..... **Error! Bookmark not defined.**2
2.2.5 Proses Dekripsi Pesan ..... **Error! Bookmark not defined.**4
2.2.6 Padding Schemes ..... **Error! Bookmark not defined.**4
2.2.7 Pengesahan Pesan ..... **Error! Bookmark not defined.**5
2.2.8 Keamanan ..... **Error! Bookmark not defined.**6
2.2.9 Pembangkitan Kunci (*Key generator*) **Error! Bookmark not defined.**7
2.2.11 Distribusi Kunci ..... **Error! Bookmark not defined.**8
2.2.12 Penyerangan Waktu ..... **Error! Bookmark not defined.**9
2.2.13 Penyerangan *ciphertext* Adaptive..... 30
2.2.14 Kekuaatan dan Keamanan RSA..... 30
2.3 *Digital signature* (Tandatangan Digital)..... 31
2.4 Biometrik .....**Error! Bookmark not defined.**5
2.5 Image Processing (Pengolahan Citra) .....**Error! Bookmark not defined.**7
2.5.1 Pengertian Pengolahan Citra (Image Processing)**Error! Bookmark not defined.**7
2.5.2 Operasi Pengolahan Citra..... **Error! Bookmark not defined.**8
2.5.3 Aplikasi Pengolahan Citra dan Pengenalan Pola**Error! Bookmark not defined.**9
2.5.4 Fungsi Pengolahan Citra (*Image Processing*)..... 40
2.5.5 Analisis Pengolaha Citra Digital..... 40
2.5.5.1 Proses Penghitungan Nilai *Pixel* Citra**Error! Bookmark not defined.**3
2.5.5.2 Proses Konversi Grayscale ..... **Error! Bookmark not defined.**4
2.6 Fungsi Hash.....**Error! Bookmark not defined.**5
2.6.1 Kegunaan ..... **Error! Bookmark not defined.**7
2.6.2 Kegunaan 50
2.6.3 Algoritma 50
2.6.4 *Message digest* ..... **Error! Bookmark not defined.**2
2.6.5 MD5 ..... **Error! Bookmark not defined.**2
2.7 ASCII 74

2.8 Base64 .....**Error! Bookmark not defined.**6

2.8.1 Penggunaan Base64 ..... **Error! Bookmark not defined.**7

2.8.2 Implementasi Pada .NET ..... **Error! Bookmark not defined.**1

2.9 OpenSSL .....**Error! Bookmark not defined.**1

2.10 Keamanan Jaringan .....**Error! Bookmark not defined.**2

2.11 Serangan Terhadap Jaringan Komputer .....**Error! Bookmark not defined.**4

2.11.1 Serangan Aktif ..... **Error! Bookmark not defined.**4

2.11.2 Serangan Pasif..... **Error! Bookmark not defined.**5

BAB 3 ANALISIS DAN PERANCANGAN ..... **Error! Bookmark not defined.**7

3.1 Analisis Sistem.....**Error! Bookmark not defined.**7

3.1.1 Dekripsi Umum..... **Error! Bookmark not defined.**8

3.1.1.1 Analisis OpenSSL..... **Error! Bookmark not defined.**9

3.1.1.2 Analisis Pembuatan Kunci..... **Error! Bookmark not defined.**9

3.1.1.3 Analisi Proses Signing ..... **Error! Bookmark not defined.**2

3.1.1.4 Analisis Proses Verify..... **Error! Bookmark not defined.**2

3.1.2 Analisis Spesifikasi Kebutuhan Perangkat lunak**Error! Bookmark not defined.**5

3.1.2.1 Kebutuhan Non-Fungsional ..... **Error! Bookmark not defined.**5

3.1.2.2 Kebutuhan Fungsional ..... **Error! Bookmark not defined.**5

3.1.3 Analisis Kebutuhan Non-fungsional... **Error! Bookmark not defined.**5

*3.1.3.1 Analisis Kebutuhan Perangkat Lunak***Error! Bookmark not defined.**6

*3.1.3.2 Analisis Kebutuhan Perangkat Keras***Error! Bookmark not defined.**6

3.1.3.3 Analisis Pengguna ..... **Error! Bookmark not defined.**7

3.1.4 Analisis Kebutuhan Fungsional ..... **Error! Bookmark not defined.**7

3.1.4.1 Identifikasi Aktor ..... **Error! Bookmark not defined.**8

3.1.4.2 Use Case ..... **Error! Bookmark not defined.**8

3.1.4.3 Use Case Skenario..... **Error! Bookmark not defined.**9

3.1.4.4 Activity Diagram..... **Error! Bookmark not defined.**1

3.1.4.5 Sequence Diagram ..... **Error! Bookmark not defined.**3

3.1.4.6 Class Diagram..... **Error! Bookmark not defined.**5

3.2 Perancangan Sistem.....**Error! Bookmark not defined.**6

3.2.1 Perancangan Struktur Menu..... **Error! Bookmark not defined.**6

3.2.2 Perancangan Antarmuka ..... **Error! Bookmark not defined.**8

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM**Error! Bookmark not defined.**

4.1 Implementasi .....**Error! Bookmark not defined.**

4.2 Pengujian Sistem .....**Error! Bookmark not defined.**

4.2.1 Simulasi Tandatangan Digital dengan Satu Signer.**Error! Bookmark not defined.**4

4.2.1.1 Proses Pembuatan Kunci Privat dan Publik serta Proses Signing**Error! Bookmark n**

4.2.2 Proses Verifikasi ..... **Error! Bookmark not defined.**8

BAB 5 KESIMPULAN DAN SARAN ..... **Error! Bookmark not defined.**7

5.1 Kesimpulan.....**Error! Bookmark not defined.**

5.2 Saran.....**Error! Bookmark not defined.**8

DAFTAR PUSTAKA 129