# DAFTAR ISI

**LEMBAR PENGESAHAN**

**PERNYATAAN KEASLIAN**

**ABSTRAK** . . . . . i

**ABSTRACT** . . . . . ii

**KATA PENGANTAR** . . . . . iii

**DAFTAR ISI** . . . . . v

**DAFTAR GAMBAR** . . . . . ix

**DAFTAR TABEL** . . . . . x

**DAFTAR SIMBOL** . . . . . xi

**BAB I PENDAHULUAN**

1.1 Latar Belakang . . . . . 1

1.2 Identifikasi dan Rumusan Masalah 5 . . . . . 5

1.2.1 Identifikasi Masalah 5 . . . . . 5

1.2.2 Rumusan Masalah 5 . . . . . 5

1.3 Batasan Masalah . . . . . 6

1.4 Tujuan Penelitian. . . . . 6

1.5 Kegunaan Penelitian . . . . . 7

1.5.1 Kegunaan Praktis . . . . . 7

1.5.2 Kegunaan Akademik. . . . . 7

1.6 Lokasi dan Waktu Penelitian. . . . . 8

**BAB II LANDASAN TEORI**

2.1 Konsep Dasar Algoritma. . . . . 10

2.1.1 Sejarah Algoritma . . . . . 10

2.1.2 Dasar Algoritma. . . . . 10

2.1 Konsep Dasar Algoritma Kriptografi . . . . . 12

2.2.1 Kriptografi. . . . . 12

2.2.2 Algoritma Kriptografi . . . . . 13

2.2.3 Algoritma Kriptografi Kunci- Simetris . . . . . 15

2.2.4 Algoritma Kriptografi Kunci-Asimetris . . . . . 17

2.3 Oracle . . . . . 21

2.3.1 Oracle Corporation . . . . . 21

2.3.2 RDMS Oracle . . . . . 22

2.4 PL/SQL Oracle 10g . . . . . 22

2.5 Oracle Form Developer . . . . . 24

2.6 Flowchart . . . . . 24

**BAB III METODOLOGI PENELITIAN**

3.1 Analisis Algoritma Kriptografi RSA. . . . . 26

3.2 Langkah Kerja Algoritma RSA. . . . . 26

3.3 Contoh Kasus Enkripsi . . . . . 30

3.3.1 (RSA) Modulus 2 Digit . . . . . 30

3.3.2 (RSA) Modulus 3 Digit . . . . . 37

3.4 Analisis Hardware dan Software . . . . . 44

3.4.1 Perangkat Keras (Hardware) . . . . . 44

3.4.2 Perangkat Lunak (Software) . . . . . 44

**BAB IV PERANCANGAN**

4.1 Perancangan. . . . . 46

4.1.1 Perancangan Algoritma Pembentukan Kunci RSA di Oracle . . . . 48

4.1.2 Perancangan Algoritma Enkripsi RSA di Oracle . . . . . 51

4.1.3 Perancangan Algoritma Dekripsi RSA di Oracle . . . . . 54

4.2 Rancangan Antarmuka. . . . . 56

4.2.1 Rancangan Menu Utama . . . . . 56

4.2.2 Rancangan Antarmuka Pembentukan Kunci . . . . . 57

4.2.3 Rancangan Antarmuka Form Data Diri Client . . . . . 59

4.2.4 Rancangan Antarmuka Proses Enkripsi . . . . . 60

4.2.5 Rancangan Antarmuka Proses Dekripsi . . . . . 61

4.3 Analisa Perancangan . . . . . 62

**BAB V IMPLEMENTASI**

5.1 Instalasi Oracle 10g . . . . . 64

5.2 Menghubungkan Oracle 10g Client ke Server . . . . . 65

5.3 Menghubungkan OFD Client ke Server . . . . . 68

5.4 Penggunaan Program . . . . . 70

5.4.1 Menu Utama . . . . . 71

5.4.2 Form Pembentukan Kunci . . . . . 71

5.4.3 Form Data Diri Pengguna . . . . . 73

5.4.4 Antarmuka Proses Enkripsi . . . . . 75

5.4.5 Antarmuka Form Data Pengguna. . . . . 75

5.4.6 Antarmuka Form Dekripsi . . . . . 76

**BAB VI KESIMPULAN DAN SARAN**

6.1 Kesimpulan. . . . . 79

6.2 Saran. . . . . 79

**DAFTAR PUSTAKA**

**LAMPIRAN**