

**RANCANG BANGUN APLIKASI KEAMANAN PERTUKARAN
PESAN BERBASIS DESKTOP MENGGUNAKAN
ALGORITMA RSA**

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana
Komputer (S.Kom.)**

**NAMA : SALISA FAIZATUN NASICHAH
NIM 19360019**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI INFORMASI
INSTITUT SAINS DAN TEKNOLOGI NASIONAL
JAKARTA
MARET 2023**

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini merupakan hasil karya penulis sendiri dan semua sumber baik yang dikutip ataupun yang dirujuk telah penulis nyatakan dengan benar.

Nama : Salisa Faizatun Nasichah
NIM 19360019
Tanggal : 3 Maret 2023

TTD diatas MATERAI

HALAMAN PERNYATAAN NON PLAGIAT

Saya yang bertanda tangan dibawah ini :

Nama : Salisa Faizatun Nasichah

NIM 19360019

Mahasiswa : Strata Satu (S1)

Tahun Akademik 2019

Menyatakan bahwa saya tidak melakukan kegiatan plagiat dalam penulisan Skripsi yang berjudul “Rancang Bangun Aplikasi Keamanan Pertukaran Pesan Berbasis Desktop Menggunakan Algoritma RSA”

Apabila suatu saat nanti saya terbukti melakukan plagiat, maka saya akan menerima sanksi yang telah ditetapkan.

Demikian Surat Pernyataan ini saya buat dengan sebenar-benarnya.

Jakarta, 8 Maret 2023

TTD di atas MATERAI

Salisa Faizatun Nasichah

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :

Nama : Salisa Faizatun Nasichah
NIM : 19360019
Program Studi : Teknik Informatika
Judul Skripsi : Rancang Bangun Aplikasi Keamanan Pertukaran Pesan Berbasis Desktop Menggunakan Algoritma RSA

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh Sarjana Komputer (S.Kom.) pada Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi, Institut Sains dan Teknologi Nasional.

DEWAN PENGUJI

Pembimbing : Aryo Nur Utomo, S.T., M.Kom. ()

NIDN. 0319046803

Penguji : Ir. Andi Suprianto, M.Kom. ()

NIDN. 0327025904

Penguji : Marhaeni, S.Kom, M.Kom. ()

NIDN. 0924037601

Penguji : Drs. Kurniawan Atmaja, M.Si ()

NIDN. 0328036403

Ditetapkan di : Jakarta
Tanggal : 8 Maret 2023

KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah SWT atas rahmat dan karunia-Nya sehingga saya dapat melaksanakan dan menyelesaikan tugas akhir ini yang berjudul **“Rancang Bangun Aplikasi Keamanan Pertukaran Pesan Berbasis Desktop Menggunakan Algoritma RSA”**. Penulisan tugas akhir ini dilakukan dalam rangka memenuhi salah satu syarat akademis dalam menyelesaikan Pendidikan tingkat Sarjana, Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi, Institut Sains dan Teknologi Nasional. Dalam penyusunan tugas akhir ini, saya mendapat banyak arahan, bimbingan dan bantuan dari berbagai pihak. Sehingga, pada kesempatan kali ini saya mengucapkan terimakasih kepada semua pihak yang telah membantu dalam Menyusun tugas akhir ini, antara lain:

1. Bapak Aryo Nur Utomo, S.T, M.Kom selaku Dosen Pembimbing dan Ketua Program Studi Teknik Informatika yang telah banyak membantu, membimbing, memberikan waktu luang dan mengarahkan pada proses skripsi ini sampai selesai;
2. Dosen dan karyawan Institut Sains dan Teknologi Nasional;
3. Kedua orang tua dan keluarga tercinta yang telah memberikan banyak dukungan berupa material dan moral;
4. Rekan-rekan seperjuangan dan seluruh pihak yang telah berkontribusi dalam memberikan motivasi, masukan, kerja sama, kritik dan saran yang sangat membantu.

Semoga Allah SWT berkenan membalas segala kebaikan segala kebaikan semua pihak yang telah membantu. Semoga tugas akhir ini dapat membawa manfaat bagi pengembangan ilmu pengetahuan.

Jakarta, 8 Maret 2023

Penulis

Salisa Faizatun Nasichah

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI KARYA
ILMIAH UNTUK KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Institut Sains dan Teknologi Nasional, saya yang bertanda tangan dibawah ini :

Nama : Salisa Faizatun Nasichah
NIM : 19360019
Program Studi : Teknik Informatika
Fakultas : Fakultas Sains dan Teknologi Informasi
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, saya setuju untuk memberikan kepada Institut Sains dan Teknologi Nasional berhak menyimpan, mengubah media/format, mengelola dalam bentuk pangkalan data (database) softcopy dan hardcopy, merawat dan mempublikasikan skripsi saya selama masih mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Dibuat di : Jakarta
Pada Tanggal : 8 Maret 2023

Yang menyatakan

Salisa Faizatun Nasichah

ABSTRAK

Nama : Salisa Faizatun Nasichah
Program Studi : Teknik Informatika
Judul : Rancang Bangun Aplikasi Keamanan Pertukaran Pesan Berbasis Desktop Menggunakan Algoritma RSA

Pesan merupakan kebutuhan untuk menyebarkan informasi. Namun saat ini banyak ancaman dalam proses pengiriman pesan yang dapat merusak pesan sebelum sampai di penerima. Dengan menggunakan metode keamanan kriptografi, pesan dapat diamankan dari proses sebelum dikirim oleh pengirim dan setelah diterima oleh penerima. Penelitian ini, bertujuan untuk merancang sebuah aplikasi pertukaran pesan dengan menerapkan algoritma Rivest-Shamir-Adleman (RSA). Hasil penelitian ini adalah sebuah aplikasi pertukaran pesan berbasis desktop dengan penambahan proses enkripsi-dekripsi. Dalam penelitian ini, aplikasi chat yang dibuat berhasil dalam mengamankan pesan dengan menggunakan algoritma kriptografi RSA.

Kata Kunci :

Pesan, Kriptografi, algoritma Rivest-Shamir-Adleman (RSA)

ABSTRACT

Name : Salisa Faizatun Nasichah
Study Program : Informatics Engineering
Title : The Application Reconstruction on the Secure Messaging System Based on Desktop Using RSA Algorithm

Messages are a necessity for disseminating information. However, there are currently many threats in the message delivery process that can damage the message before it reaches the recipient. By using cryptographic security methods, messages can be secured from the process before being sent by the sender and after being received by the recipient. This research aims to design a message exchange application by applying the Rivest-Shamir-Adleman (RSA) algorithm. The result of this research is a desktop-based message exchange application with addition of an encryption-decryption process. In this study, the chat application created was successful in securing messages using RSA cryptographic algorithm.

Keywords:

Message, Cryptography, Rivest-Shamir-Adleman (RSA)

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERNYATAAN ORISINALITAS.....	ii
HALAMAN PERNYATAAN NON PLAGIAT	iii
HALAMAN PENGESAHAN.....	iv
KATA PENGANTAR	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS	vi
ABSTRAK.....	vii
ABSTRACT.....	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
DAFTAR RUMUS.....	xiv
DAFTAR PSEUDOCODE	xv
LAMPIRAN.....	xvi
1. PENDAHULUAN.....	1
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah.....	2
1.3. Batasan Masalah	3
1.4. Tujuan Penelitian	3
1.5. Manfaat Penelitian	3
2. TINJAUAN PUSTAKA	4
2.1. Penelitian Terdahulu.....	4
2.2. Algoritma.....	5
2.3. Kriptografi	6
2.4. Algoritma Rivest Shamir Adleman (RSA).....	10
2.5. Keamanan RSA	15
2.6. Kelebihan dan Kekurangan RSA	16
2.7. ASCII Code	16
2.8. Java.....	17
2.9. Netbeans	18
2.10. Jaringan.....	18

2.11. MySQL	20
2.12. XAMPP	20
2.13. Unified Modeling Language (UML)	22
2.14. Entity-Relationship Diagram (ERD)	22
3. METODOLOGI PENELITIAN	24
3.1. Metodologi Penelitian Prototype	24
3.2. Tahapan Penelitian	25
3.3. Identifikasi Masalah	26
3.4. Studi Literatur	27
3.5. Analisis Kebutuhan Sistem	27
3.6. Perancangan Sistem	28
3.7. Desain Aplikasi	36
3.8. Implementasi RSA	41
3.9. Pembuatan Laporan	46
4. HASIL DAN PEMBAHASAN	47
4.1. Proses Login dan Registrasi	47
4.2. Menu Utama, View Log dan Help	50
4.3. Form Chat	52
4.4. Blackbox Testing	58
5. PENUTUP	69
5.1. Simpulan	69
5.2. Saran	69
DAFTAR PUSTAKA	70

DAFTAR TABEL

Tabel 2. 1 Perbandingan Peneliti Terdahulu	4
Tabel 3. 1 Database User	29
Tabel 3. 2 Database Chat	30
Tabel 3. 3 Informasi Form Login	36
Tabel 3. 4 Informasi Form Registrasi	37
Tabel 3. 5 Informasi Form Menu Utama	38
Tabel 3. 6 Informasi Form View Log	39
Tabel 3. 7 Informasi Form Chat	40
Tabel 4. 1 Pengujian Form Login	58
Tabel 4. 2 Pengujian Form Registrasi	61
Tabel 4. 3 Pengujian Form Menu Utama	64
Tabel 4. 4 Pengujian Form Chat	66
Tabel 4. 5 Pengujian Pilih Teman Chat	67

DAFTAR GAMBAR

Gambar 2. 1 Penggunaan Dua Kunci	11
Gambar 2. 2 ASCII Code	17
Gambar 3. 1 Metode Prototype	24
Gambar 3. 2 Tahapan Penelitian	26
Gambar 3. 3 ERD Database	28
Gambar 3. 4 PDM Database.....	29
Gambar 3. 5 Use Case Diagram	30
Gambar 3. 6 Activity Diagram Login User.....	32
Gambar 3. 7 Activity Diagram Registrasi User	33
Gambar 3. 8 Activity Diagram Form Help	33
Gambar 3. 9 Activity Diagram Form Chat.....	34
Gambar 3. 10 Activity Diagram View Log.....	35
Gambar 3. 11 Class Diagram Aplikasi.....	35
Gambar 3. 12 Desain Form Login.....	37
Gambar 3. 13 Desain Form Registrasi	38
Gambar 3. 14 Desain Menu Utama.....	39
Gambar 3. 15 Desain View Log.....	40
Gambar 3. 16 Desain Form Chat.....	41
Gambar 3. 17 Pembuatan Kunci	41
Gambar 3. 18 Proses Enkripsi.....	44
Gambar 3. 19 Proses Dekripsi.....	45
Gambar 4. 1 Tampilan Form Login	47
Gambar 4. 2 Tampilan Message Login Gagal	47
Gambar 4. 3 Tampilan Form Registration	48
Gambar 4. 4 Pengisian Data Form Registration.....	48
Gambar 4. 5 Proses Generate Berhasil.....	49
Gambar 4. 6 Simpan data	49
Gambar 4. 7 Proses Login User	50
Gambar 4. 8 Message Login Berhasil	50
Gambar 4. 9 Tampilan Form Menu Utama.....	51
Gambar 4. 10 Tampilan Log Pengiriman.....	51
Gambar 4. 11 Tampilan Form Help	52
Gambar 4. 12 Tampilan List Of Active Friends.....	52
Gambar 4. 13 Pemilihan Teman.....	53
Gambar 4. 14 Pengisian Nilai D	53
Gambar 4. 15 Tampilan Form Chat	54
Gambar 4. 16 Sintaks Proses Enkripsi	54
Gambar 4. 17 Sintaks Proses Dekripsi.....	55

Gambar 4. 18 Pengiriman Pesan Ke Teman	55
Gambar 4. 19 Tampilan Pesan Di Aplikasi Teman.....	56
Gambar 4. 20 Membalas Pesan.....	56
Gambar 4. 21 Tampilan Balasan Pesan dari Teman	57
Gambar 4. 22 Tampilan Message Log Out	57
Gambar 4. 23 Kembali Ke Form Login	57
Gambar 4. 24 Message Login Berhasil	60
Gambar 4. 25 Message Login Gagal.....	60
Gambar 4. 26 Message Data Berhasil Disimpan	63
Gambar 4. 27 Message Data Harus Diisi	63
Gambar 4. 28 Identitas User 1 di Menu Utama	65
Gambar 4. 29 Identitas User 2 di Menu Utama	65
Gambar 4. 30 Tampilan Plaintext Pada Penerima	67
Gambar 4. 31 Message Dialog untuk Isi Nilai D	67
Gambar 4. 32 Pemilihan Teman Chat.....	68
Gambar 4. 33 Identitas Teman di Form Chat.....	68

DAFTAR RUMUS

Rumus 2. 1 Nilai n	11
Rumus 2. 2 Nilai ϕ	11
Rumus 2. 3 Nilai gcd.....	12
Rumus 2. 4 Nilai C	12
Rumus 2. 5 Nilai M	12

DAFTAR PSEUDO CODE

Pseudo Code 3. 1 Pemilihan Nilai p dan q	42
Pseudo Code 3. 2 Perhitungan Nilai n	42
Pseudo Code 3. 3 Menghitung Nilai ϕ	42
Pseudo Code 3. 4 Mencari Nilai e	42
Pseudo Code 3. 5 Menghitung Nilai gcd	43
Pseudo Code 3. 6 Menghitung Nilai d	43
Pseudo Code 3. 7 Coding Enkripsi Pesan	44
Pseudo Code 3. 8 Coding Dekripsi Pesan.....	45

LAMPIRAN

Lampiran 1 : Lembar Konsultasi Bimbingan Tugas Akhir	72
Lampiran 2 : Source Code Aplikasi Chat	73