

**PERANCANGAN APLIKASI AUTENTIKASI SURAT DIGITAL DENGAN
METODE *ONE TIME PASSWORD* SHA-512 DI KANTOR PUSAT
ADMINISTRASI POLITEKNIK NEGERI SRIWIJAYA**



TUGAS AKHIR

**Disusun untuk Memenuhi Syarat Menyelesaikan Pendidikan Sarjana
Terapan Jurusan Teknik Elektro Program Studi Teknik
Telekomunikasi Politeknik Negeri Sriwijaya**

**Oleh :
SALWA KAMILA
0618 4035 1385**

**POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG
2022**

TUGAS AKHIR

PERANCANGAN APLIKASI AUTENTIKASI SURAT DIGITAL DENGAN METODE *ONE TIME PASSWORD* SHA-512 DI KANTOR PUSAT ADMINISTRASI POLITEKNIK NEGERI SRIWIJAYA



**Disusun untuk Memenuhi Syarat Menyelesaikan Pendidikan Sarjana
Terapan Jurusan Teknik Elektro Program Studi Teknik Telekomunikasi
Politeknik Negeri Sriwijaya**

Oleh :

Nama : Salwa Kamila (061840351385)
Dosen Pembimbing I : Lindawati, S.T., M.T.I.
Dosen Pembimbing II : Mohammad Fadhli, S.Pd., M.T.

**POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG**

2022

**PERANCANGAN APLIKASI AUTENTIKASI SURAT DIGITAL DENGAN
METODE *ONE TIME PASSWORD* SHA-512 DI KANTOR PUSAT
ADMINISTRASI POLITEKNIK NEGERI SRIWIJAYA**



TUGAS AKHIR

**Disusun untuk Memenuhi Syarat Menyelesaikan Pendidikan Sarjana
Terapan Pada Jurusan Teknik Elektro Program Studi Teknik
Telekomunikasi Politeknik Negeri Sriwijaya**

OLEH :

SALWA KAMILA

0618 4035 1385

Palembang, 2022

Pembimbing I

**Lindawati, S.T., M.T.I.
NIP. 197105282006042001**

Pembimbing II

**Mohammad Fadhli, S.Pd., M.T.
NIP. 199004032018031001**

Mengetahui,

**Ketua Jurusan
Teknik Elektro**

**Ir. Iskandar Lutfi, M.T.
NIP. 196705111992031003**

**Koordinator Program Studi Sarjana
Terapan Teknik Telekomunikasi**

**Lindawati, S.T., M.T.I.
NIP. 197105282006042001**

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan:

Nama : Salwa Kamila
Jenis Kelamin : Perempuan
Tempat, Tanggal Lahir : Palembang, 07 Juni 2000
Alamat : Jl. P. Ayin Komp. Persada Indah Blok F 14
NPM : 061840351385
Program Studi : Sarjana Terapan Teknik Telekomunikasi
Jurusan : Teknik Elektro
Judul Skripsi/Laporan Akhir : Perancangan Aplikasi Autentikasi Surat Digital dengan Metode *One Time Password* SHA-512 di Kantor Pusat Administrasi Politeknik Negeri Sriwijaya

Menyatakan dengan sesungguhnya bahwa:

1. Skripsi/Laporan Akhir ini adalah hasil karya saya sendiri serta bebas dari tindakan plagiasi, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.
2. Dapat menyelesaikan segala urusan terkait pengumpulan revisi Skripsi/Laporan Akhir yang sudah disetujui oleh dewan penguji paling lama 1 bulan setelah ujian Skripsi/Laporan Akhir.
3. Dapat menyelesaikan segala urusan peminjaman/penggantiaan alat/buku dan lainnya paling lama 1 bulan setelah ujian Skripsi/Laporan Akhir.

Apabila dikemudian hari diketahui ada pernyataan yang terbukti tidak benar dan tidak dapat dipenuhi, maka saya siap bertanggung jawab dan menerima sanksi tidak diikutsertakan dalam prosesi wisuda serta dimasukkan dalam daftar hitam oleh Jurusan Teknik Elektro sehingga berdampak tertundanya pengambilan Ijazah & Transkrip (ASLI & COPY). Demikian surat pernyataan ini dibuat dengan sebenarnya dan dalam keadaan sadar tanpa paksaan.

Palembang, Agustus 2022

Yang Menyatakan,



METERAN
TEMPEK
JEDBFFAJX94848930

(Salwa Kamila)

Mengetahui,

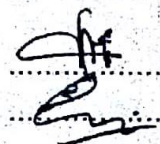
Pembimbing I

Lindawati, S.T., M.T.I.

Pembimbing II

Mohammad Fadhli, S.Pd., M.T.

* Coret yang tidak perlu



MOTTO DAN PERSEMBAHAN

“Angin tidak berhembus untuk menggoyangkan pepohonan, melainkan menguji kekuatan akarnya.”

– Ali bin Abi Thalib

“Tangga kesuksesan tak pernah penuh sesak di bagian puncak.”

– Napoleon Hill

“Dear future me, it’s okay if you didn’t turn out the way i wanted, because i’m still the one who loves and roots for you the most.”

– Hello, Me

Dengan rasa syukur yang tak terkira, Tugas Akhir ini Penulis persembahkan kepada :

- *Kedua orang tua tersayang dan tercinta, Papa Suhardi dan Almh. Mama Fatihah.*
- *Adik Saya Zahrah Wafiqah.*
- *Keluarga besar yang selalu memberikan dukungan dan semangat.*
- *Pembimbing I Ibu Lindawati, S.T., M.T.I. dan Pembimbing II Bapak Mohammad Fadhli, S.Pd., M.T. yang telah memberi banyak ilmu dan bimbingan.*
- *Teman-teman seperjuangan DIV Teknik Telekomunikasi angkatan 2018 yang telah semangat berjuang bersama.*
- *Almamaterku “Politeknik Negeri Sriwijaya”.*

ABSTRAK

Perancangan Aplikasi Autentikasi Surat Digital dengan Metode *One Time Password* SHA-512 di Kantor Pusat Administrasi Politeknik Negeri Sriwijaya

(2022 : xvi + 83 halaman + 40 gambar + 10 tabel + 11 lampiran)

SALWA KAMILA

061840351385

JURUSAN TEKNIK ELEKTRO

PROGRAM STUDI SARJANA TERAPAN TEKNIK TELEKOMUKASI

POLITEKNIK NEGERI SRIWIJAYA

Beberapa prosedur administrasi di Politeknik Negeri Sriwijaya masih dilakukan secara konvensional, dimana hal ini dianggap kurang efisien dan memakan banyak waktu. Disisi lain, suatu komunikasi dengan pihak lain memerlukan proses pertukaran informasi, sehingga dibutuhkan suatu mekanisme untuk menjamin keabsahan informasi tersebut. Maka dari itu, dikembangkan sebuah sistem surat-menyurat digital yang dapat membuktikan keaslian informasi yang diperoleh dari media digital tersebut benar dari pihak yang bersangkutan, yakni menggunakan metode autentikasi. Penambahan *One Time Password* (OTP) sebagai metode autentikasi yang menggunakan satu kunci *password* bersifat sementara dapat menjadi solusinya. Pada penelitian ini, digunakan metode *One Time Password* (OTP) sebagai sistem validasi dan algoritma *SHA-512* sebagai pembangkit kode OTP untuk menghasilkan kode acak. Sistem ini memanfaatkan teknologi android pada *mobile* untuk memudahkan akses ke sistem administrasi surat-menyurat agar lebih mudah dikunjungi dengan fitur yang mengutamakan informasi dan kecepatan akses. Hasil pengujian menggunakan *black box testing* dan *time response* menunjukkan bahwa semua menu dan fitur yang tersedia dapat diterima dan aplikasi yang dibuat sudah memiliki sistem yang berjalan sesuai kebutuhan pengguna. Lalu pada pengujian tingkat keamanan algoritma *SHA-512* didapatkan hasil bahwa bahwa sistem tidak dapat memecahkan *password* OTP dan menemukan jenis algoritma *hash* yang digunakan dan rata-rata nilai AE yang dihasilkan dari uji coba yaitu sebesar 63,91% dimana ini menunjukkan hasil enkripsi dengan kemampuan keamanan yang tinggi.

Kata Kunci : *Android, Autentikasi, One Time Password (OTP), SHA-512, Surat Digital.*

ABSTRACT

Design of Digital Letter Authentication Application with One-Time Password SHA-512 at The Administrative Office of The State Polytechnic of Sriwijaya

(2022 : xvi + 83 pages + 40 pictures + 10 tables + 11 appendixes)

SALWA KAMILA

061840351385

ELECTRICAL ENGINEERING DEPARTMENT

TELECOMMUNICATION ENGINEERING STUDY PROGRAM

STATE POLYTECHNIC OF SRIWIJAYA

Some administrative procedures at the State Polytechnic of Sriwijaya are still carried out conventionally, which is deemed less efficient and takes much time. On the other hand, communication with other parties requires a process of exchanging information, so a system is needed to confirm the validity of the information. Therefore, a digital letter system that can prove the validity of the information gained through the digital media right from the party concerned is developing. This can be overcome using the authentication method. Adding One Time Password (OTP) as an authentication method that employs one temporary password key can be the solution. This study used the One Time Password (OTP) method as a validation system and the SHA-512 algorithm as an OTP code generator to generate random codes. This system leverages android technology on mobile to ease access to the correspondence administration system to make it easier to visit with features that prioritize information and access speed. The black box testing and time response revealed that all available menus and features were appropriate, and the application already had a system that functions according to user needs. Then in testing the security level of the SHA-512 algorithm, the result was obtained that the system could not crack the OTP password and found the type of hash algorithm used and the average AE value generated from the trial was 63.91% which showed encryption results with high-security capabilities.

Keywords : *Android, Authentication, Digital Letter, One-Time Password (OTP), SHA-512.*

KATA PENGANTAR

Puji syukur penulis panjatkan atas kehadiran Allah SWT, yang telah memberikan rahmat serta karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul “**Perancangan Aplikasi Autentikasi Surat Digital dengan Metode *One Time Password* SHA-512 di Kantor Pusat Administrasi Politeknik Negeri Sriwijaya**”. Tugas akhir ini dibuat untuk memenuhi syarat menyelesaikan pendidikan Sarjana Terapan Teknik Telekomunikasi Jurusan Teknik Elektro Politeknik Negeri Sriwijaya Palembang.

Pada penelitian dan penyusunan tugas akhir ini, penulis mengucapkan terima kasih kepada **Ibu Lindawati, S.T., M.T.I** selaku Dosen Pembimbing I dan **Bapak Mohammad Fadhli, S.Pd., M.T.** selaku Dosen Pembimbing II yang telah memberikan bimbingan, pengarahan dan nasihatnya kepada penulis dalam menyelesaikan tugas akhir ini. Selain itu, penulis juga mengucapkan terima kasih kepada:

1. Kedua orang tua penulis bapak **Suhardi** dan Almh. ibu **Fatihah** serta adik **Zahrah Wafiqah** yang selalu memberikan dukungan dan semangat secara moril maupun materil.
2. Bapak **Dr. Dipl. Ing. Ahmad Taqwa, M.T.**, selaku Direktur Politeknik Negeri Sriwijaya.
3. Bapak **Ir. Iskandar Lutfi, M.T.**, selaku Ketua Jurusan Teknik Elektro Politeknik Negeri Sriwijaya.
4. Bapak **Destra Andika Pratama, S.T., M.T.**, selaku Sekretaris Jurusan Teknik Elektro Politeknik Negeri Sriwijaya.
5. Ibu **Lindawati, S.T., M.T.I**, selaku Ketua Program Studi Sarjana Terapan Teknik Telekomunikasi Politeknik Negeri Sriwijaya.
6. Bapak/Ibu Dosen Program Studi Sarjana Terapan Teknik Telekomunikasi Politeknik Negeri Sriwijaya.
7. Sahabat *4 Sehat 5 Rebahan*, Redho, Prisa, Alda dan sahabat lainnya yang selalu menemani penulis selama mengerjakan tugas akhir ini.

8. Teman-teman TEA dan TEB angkatan 2018 yang telah semangat dan berjuang bersama mengerjakan tugas akhir.
9. Semua pihak yang telah banyak membantu penulis dalam pelaksanaan dan penyusunan tugas akhir ini.

Penulis berharap semoga tugas akhir ini bermanfaat bagi kita semua, umumnya para pembaca dan khususnya penulis serta bagi mahasiswa Politeknik Negeri Sriwijaya Jurusan Teknik Elektro Program Studi Sarjana Terapan Teknik Telekomunikasi.

Palembang, Agustus 2022

Salwa Kamila

DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL	ii
HALAMAN PENGESAHAN	iii
LEMBAR PERNYATAAN	iv
MOTTO DAN PERSEMBAHAN	v
ABSTRAK	vi
ABSTRACT	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xiv
DAFTAR PERSAMAAN	xv
DAFTAR LAMPIRAN	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	3
1.3 Pembatasan Masalah	3
1.4 Tujuan.....	3
1.5 Manfaat	4
1.6 Metode Penulisan	4
1.6.1 Metode Studi Pustaka	4
1.6.2 Metode Eksperimen.....	5
1.6.3 Metode Observasi	5
1.6.4 Metode Wawancara	5
1.7 Sistematika Penulisan.....	5
BAB II TINJAUAN PUSTAKA	7
2.1 Sistem Informasi	7
2.2 Surat Digital.....	7
2.3 Autentikasi	7
2.4 <i>One Time Password (OTP)</i>	8
2.5 Fungsi <i>Hash</i>	9
2.6 <i>SHA-512 (Secure Hash Algorithm 512)</i>	10
2.7 <i>QR Code (Quick Response Code)</i>	13
2.8 Perangkat Lunak Pembangun Aplikasi	14
2.8.1 Android	14
2.8.2 Android Studio	15
2.8.3 <i>Java</i>	15
2.8.4 <i>Android Software Development Kit (SDK)</i>	15
2.8.5 <i>XAMPP</i>	16
2.8.6 <i>My SQL</i>	16
2.8.7 <i>Hypertext Preprocessor (PHP)</i>	17
2.8.8 <i>Hyper Text Markup Language (HTML)</i>	17

2.8.9	<i>Java Script</i>	18
2.8.10	<i>Cascading Style Sheets (CSS)</i>	19
2.8.11	<i>Framework Laravel</i>	19
2.8.12	<i>Hypertext Transfer Protocol (HTTP)</i>	21
2.9	Penelitian Sebelumnya (<i>State of the Art</i>)	21
BAB III METODOLOGI PENELITIAN 23		
3.1	Kerangka Penelitian	23
3.2	Studi Literatur	23
3.3	Pengumpulan Data	24
3.4	Analisis Sistem	24
3.5	Perancangan Sistem	25
3.5.1	Pengembangan Perangkat Lunak (Aplikasi)	25
3.5.2	Perancangan <i>One Time Password</i> dengan Algoritma <i>SHA-512</i>	27
3.5.2.1	Arsitektur Perancangan Kode <i>One Time Password</i>	27
3.5.2.2	Alur Kerja Fungsi <i>Hash</i>	28
3.5.3	Mengembangkan <i>Prototype</i>	29
3.5.4	Kebutuhan Perangkat Keras (<i>Hardware</i>)	32
3.5.5	Kebutuhan Perangkat Lunak (<i>Software</i>)	33
3.6	Pengujian Sistem	33
3.6.1	Pengujian Menu Aplikasi dengan <i>Black Box Testing</i>	34
3.6.2	Pengujian <i>Time Response</i> Pembangkitan Kode OTP	34
3.6.3	Pengujian Tingkat Keamanan Algoritma <i>SHA-512</i> sebagai pembangkit <i>One Time Password</i>	34
3.6.3.1	Pengujian Menggunakan <i>Software CrackStation</i>	34
3.6.3.2	Pengujian <i>Avalanche Effect (AE)</i>	36
BAB IV HASIL DAN PEMBAHASAN 37		
4.1	Implementasi Hasil Aplikasi	37
4.1.1	Proses Kerja Sistem Aplikasi	37
4.1.2	Sistem <i>Database</i>	39
4.1.3	Tampilan Aplikasi Berbasis Android	39
4.1.4	Tampilan Aplikasi Berbasis Web	47
4.1.5	Implementasi Algoritma <i>SHA-512</i> pada kode <i>One Time Password</i>	56
4.2	Hasil Pengujian Sistem	57
4.2.1	Hasil Pengujian Aplikasi menggunakan <i>Black Box Testing</i>	57
4.2.2	Hasil Pengujian <i>Time Response</i> Pembangkitan kode <i>One Time Password</i>	64
4.2.3	Hasil Pengujian Tingkat Keamanan Algoritma <i>SHA-512</i>	75
4.2.3.1	Pengujian Menggunakan <i>Software CrackStation</i>	75
4.2.3.2	Pengujian <i>Avalanche Effect (AE)</i>	77
4.3	Analisa Hasil	79
4.3.1	Analisa Hasil Pengujian <i>Black Box Testing</i>	79

4.3.2 Analisa Hasil Pengujian <i>Time Response</i> Pembangkitan Kode OTP.....	79
4.3.3 Analisa Hasil Pengujian menggunakan <i>Software</i> <i>CrackStation</i>	80
4.3.4 Analisa Hasil Pengujian <i>Avalanche Effect</i> (AE).....	80
BAB V KESIMPULAN DAN SARAN	82
5.1 Kesimpulan.....	82
5.2 Saran.....	83
DAFTAR PUSTAKA	
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2.1 <i>Input dan Output Fungsi Hash</i>	10
Gambar 2.2 Proses I Algoritma SHA-512	11
Gambar 2.3 Proses II Algoritma SHA 512	12
Gambar 3.1 Diagram Alir Penelitian	23
Gambar 3.2 Menu pada Aplikasi Android	25
Gambar 3.3 Menu Aplikasi Web Pengguna.....	26
Gambar 3.4 Menu Aplikasi Web Admin	26
Gambar 3.5 Arsitektur Perancangan Kode OTP	27
Gambar 3.6 Alur Kerja Fungsi <i>Hash</i>	28
Gambar 3.7 <i>Prototype</i> (a) <i>log in</i> dan (b) list menu aplikasi.....	29
Gambar 3.8 <i>Prototype</i> menu (a) beranda dan (b) surat masuk.....	30
Gambar 3.9 <i>Prototype</i> (a) menu surat belum tanda tangan dan (b) <i>input</i> kode OTP	30
Gambar 3.10 <i>Prototype</i> halaman awal <i>website</i>	31
Gambar 3.11 <i>Prototype</i> halaman <i>log in</i> web.....	31
Gambar 3.12 <i>Prototype</i> tampilan utama web.....	32
Gambar 3.13 Halaman web <i>CrackStation</i>	35
Gambar 3.14 Masukkan <i>Password</i> dengan fungsi <i>hash</i> SHA-512	35
Gambar 3.15 Tekan <i>captcha</i> “ <i>I’m not a robot</i> ” dan Tombol <i>Crack Hashes</i>	35
Gambar 4.1 Diagram Alir Proses Kerja Aplikasi	38
Gambar 4.2 Tampilan <i>Tables</i> pada Database.....	39
Gambar 4.3 (a) <i>Splash Screen</i> dan (b) Halaman <i>Log In</i> Android.....	40
Gambar 4.4 List Menu Aplikasi Android	40
Gambar 4.5 Menu Beranda Android.....	41
Gambar 4.6 Menu Profil	42
Gambar 4.7 (a) Menu Surat Belum Tanda Tangan (b) Halaman <i>Input</i> Kode OTP (c) Notifikasi Kode OTP pada <i>Email</i> Pengguna dan (d) Halaman Disposisi Surat	43
Gambar 4.8 Menu Riwayat Disposisi	44
Gambar 4.9 (a) Menu Surat Masuk dan (b) Halaman Tambah Surat Masuk.....	45
Gambar 4.10 (a) Menu Surat Keluar dan (b) Halaman Tambah Surat Keluar.....	46
Gambar 4.11 (a) Implementasi <i>QR Code</i> pada Surat (b) Hasil Scan isi <i>QR Code</i>	46
Gambar 4.12 Tampilan Awal <i>Website</i>	47
Gambar 4.13 Halaman <i>Log In Website</i>	48
Gambar 4.14 Menu Beranda <i>Website</i> disisi (a) Admin (b) Pengguna.....	49
Gambar 4.15 Menu (a) Surat Masuk (b) Tambah Surat Masuk	50
Gambar 4.16 Menu (a) Surat Keluar (b) Tambah Surat Keluar	51
Gambar 4.17 Menu Disposisi Surat.....	52
Gambar 4.18 Menu (a) Data Pengguna (b) Tambah Pengguna Baru	53
Gambar 4.19 Menu (a) Atur Pengguna (b) Tambah Pengguna dengan Peran.....	54
Gambar 4.20 Menu (a) Atur Peran Pengguna (b) Tambah Peran Pengguna	55
Gambar 4.21 Menu Profil Pengguna dan Keluar Akun.....	55
Gambar 4.22 Kode Program Implementasi Algoritma SHA-512	56

DAFTAR TABEL

Tabel 2.1 Proses Inisialisasi	11
Tabel 2.2 Tabel <i>State of the Art</i>	21
Tabel 3.1 Perangkat Keras Pendukung	32
Tabel 3.2 Perangkat Lunak Pendukung	33
Tabel 4.1 Hasil <i>Black Box Testing</i> Aplikasi berbasis Android	57
Tabel 4.2 Hasil <i>Black Box Testing</i> Aplikasi berbasis Web	60
Tabel 4.3 Hasil Uji Coba Pembangkitan Kode OTP di server lokal	65
Tabel 4.4 Hasil Uji Coba Pembangkitan Kode OTP di server <i>Web Hosting</i>	70
Tabel 4.5 Hasil Pengujian dengan <i>CrackStation</i>	75
Tabel 4.6 Hasil Pengujian <i>Avalanche Effect (AE)</i>	77

DAFTAR PERSAMAAN

Persamaan 2.1 Fungsi <i>Hash</i>	9
Persamaan 2.2 Proses SHA-512	13
Persamaan 3.1 Rumus Perhitungan <i>Avalanche Effect</i> (AE).....	36

DAFTAR LAMPIRAN

- Lampiran 1** Daftar Riwayat Hidup
- Lampiran 2** Lembar Kesepakatan Bimbingan TA Pembimbing I
- Lampiran 3** Lembar Kesepakatan Bimbingan TA Pembimbing II
- Lampiran 4** Lembar Konsultasi Pembimbing I
- Lampiran 5** Lembar Konsultasi Pembimbing II
- Lampiran 6** Lembar Rekomendasi Tugas Akhir
- Lampiran 7** Lembar Revisi Ujian Tugas Akhir
- Lampiran 8** *Letter of Acceptance*
- Lampiran 9** *Submitted Journal*
- Lampiran 10** Tabel Hasil Pengujian
- Lampiran 11** Kode Program Aplikasi