

**IMPLEMENTASI SISTEM KEAMANAN ONE TIME PASSWORD DENGAN  
MENGUNAKAN ALGORITMA SHA 512 PADA SISTEM  
INFORMASI AKADEMIK SMPN 56 BANDUNG**

**SKRIPSI**

Diajukan Sebagai Salah Satu Syarat Untuk Mendapatkan Gelar Sarjana Teknik Pada  
Program Studi S1 Teknik Informatika Universitas Sangga Buana YPKP

Disusun Oleh :

**RISMAWAN ARDIANSYAH**

**B1031511RB5003**



**PROGRAM STUDI S1 TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS SANGGA BUANA YPKP BANDUNG**

**2019**

## LEMBAR PERSETUJUAN

Karya ditulis Oleh : Rismawan Ardiansyah

Nomor Induk Mahasiswa : B1031511RB5003

Judul : **IMPLEMENTASI SISTEM KEAMANAN ONE  
TIME PASSWORD DENGAN  
MENGUNAKAN ALGORITMA SHA 512  
PADA SISTEM INFORMASI AKADEMIK  
SMP NEGERI 56 BANDUNG**

Telah Menyetujui Laporan Tugas Akhir dengan Prosedur dan Ketentuan yang berlaku.

Bandung, 16 Agustus 2019


Disetujui Oleh :

**PEMBIMBING TUGAS AKHIR**

**Gunawan, S.T., M.Kom., MOS.** ..... 

Mengetahui:

**KETUA PRODI S1 TEKNIK INFORMATIKA**

**Riffa Haviani Laluma, S.Kom., MT.** ..... 

## LEMBAR PERSETUJUAN

Saya yang bertanda tangan dibawah ini

Karya ditulis Oleh : Rismawan Ardiansyah

NIM : B1031511RB5003

Judul : IMPLEMENTASI SISTEM KEAMANAN ONE TIME  
PASSWORD DENGAN MENGGUNAKAN ALGORITMA  
SHA 512 PADA SISTEM INFORMASI AKADEMIK  
SMPNEGERI 56 BANDUNG

Menyatakan dengan sebenarnya bahwa penulisan Skripsi ini berdasarkan hasil pemikiran dan pemaparan asli dari saya sendiri, baik untuk naskah laporan maupun kegiatan programming yang tercantum sebagai bagian dari Skripsi ini. Jika terdapat karya orang lain, saya akan mencantumkan sumber yang jelas .

Demikian pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya siap bersedia menerima sanksi akademik yang berlaku di Univeristan Sangga Buana YPKP Bandung.

Bandung, 9 September 2019

METERAI  
TEMPEL  
Rp 1000  
ENAM RIBU RUPIAH  
KISMAWAN ARDIANSYAH



Nim. B1031511RB5003

# LEMBAR PERSETUJUAN DAN PENGUJIAN TUGAS AKHIR

Tugas akhir ini diajukan Oleh

Nama : Rismawan Ardiansyah

NIM : B1031511RB5003

Program Studi : Teknik Informatika

Jenjang : Sarjana (S1)

Judul Tugas Akhir : Implementasi Sistem Keamanan One Time Password Dengan Menggunakan Algoritma SHA 512 Pada Sistem Informasi Akademik SMP Negeri 56 Bandung

Telah dipertahankan dihadapan penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh Gelar Sarjana Teknik pada Program Studi Teknik Informatika Universitas Sangga Buana YPKP Bandung.

Bandung, 9 September 2019

## PEMBIMBING TUGAS AKHIR

Pembimbing : **Gunawan, S.T., M.Kom., MOS.**



## DEWAN PENGUJI

Penguji I : Riffa Haviani Laluma, S.Kom., MT.

Penguji II : Nanang Hunaifi, S.T., MM.



## ABSTRAK

Keamanan data telah menjadi kebutuhan dasar disetiap organisasi atau lembaga pendidikan. Secara umum untuk mendukung sistem mereka, organisasi atau lembaga pendidikan memerlukan sarana komunikasi yang dapat menjamin bahwa informasi atau data yang diterima sama persis pada saat data itu direkam (*integrity*). Diperlukan sebuah sistem autentikasi yang mampu mengidentifikasi setiap user dan metode enkripsi yang dapat menekan tingkat penyerangan dan memperkecil kemungkinan terjadinya pencurian terhadap password.

*One Time Password* (OTP) merupakan suatu salah satu jenis metode autentikasi dimana administrator diharuskan menggunakan kata sandi yang bersifat *dynamic password* dengan menggunakan telepon genggam sebagai pembangkit token dan SHA-512 sebagai enkripsi untuk melindungi *username* dan *password* dari serangan *sniffer*.

Dari hasil penelitian yang dilakukan dapat diketahui bahwa sistem autentikasi menggunakan metode OTP mampu memverifikasi setiap user yang hendak mengakses ke halaman system informasi akademik ini dan SHA-512 dapat diandalkan dan dapat digunakan untuk menjamin integritas dan keaslian data user

Kata kunci : One Time Password, SHA512,Sistem Informasi Akademik

## **ABSTRACT**

*Data security has become the basic needs in every organization or educational institutions. In general to support their system, organization or institution needs means of communication which can ensure that information or data received same at the time the data was recorded (intergrity). Required a authentication system to identify every user and encryption method that can that can be reduce the degree of assault And reduce the possibilities of theft of passwords.*

*One Time Password (OTP) is a type of authentication method where administrators are required to use dynamic passwords by using a cell phone as a token generator and SHA-512 as encryption to protect usernames and passwords from sniffer attacks.*

*From the results of research conducted it can be seen that the authentication system uses the OTP method allows each user to access academic information systems and SHA-512 is reliable and can be used to guarantee the integrity and authenticity of data users.*

*Keywords : One Time Password, SHA512,Sistem Informasi Akademik*

## **KATA PENGANTAR**

Puji dan syukur penulis panjatkan kehadiran Allah SWT karena atas Rahmat dan karunia-Nya serta kepada junjungan alam Nabi Muhammad SAW sehingga penulis dapat menyelesaikan tugas akhir skripsi yang berjudul **“IMPLEMENTASI SISTEM KEAMANAN ONE TIME PASSWORD DENGAN MENGGUNAKAN ALGORITMA SHA 512 PADA SISTEM INFORMASI AKADEMIK SMP NEGERI 56 BANDUNG ”** untuk memenuhi salah satu syarat studi jenjang strata satu (S1) di Program Studi Teknik Informatika Universitas Sangga Buana YPKP.

Penyusunan skripsi ini tidak akan berhasil tanpa ada dukungan dari berbagai pihak. Oleh karena itu, penulis menulis kata pengantar ini sangat menghargai dan berterima kasih sebesar-besarnya kepada:

1. Kedua orang tua, Ibu Ayi Sugiarti dan Bapak S. Hermansyah yang selalu memberikan doa, semangat, dukungan, motivasi, dan ide kepada penulis selama proses pengerjaan tugas akhir.
2. Bapak Gunawan, S.T., M.T.,MOS. sebagai dosen pembimbingan yang telah membimbing, memberi masukan, dan mengarahkan selama pengerjaan tugas akhir.
3. Ibu Riffa Haviani Laluma, S.Kom, MT selaku Ketua Program Studi S1 Teknik Informatika Universitas Sangga Buana YPKP Bandung

4. Ibu Riffa Haviani Laluma S.Kom., MT. selaku Penguji 1 atau dosen Reviewer yang telah meluangkan waktu untuk menguji dan memberikan bimbingan dan saransaran kepada penulis dalam pengerjaan revisi laporan tugas akhir ini
5. Bapak Nanang Hunaifi, S.T., MM. selaku Penguji 2 atau dosen Reviewer yang juga telah memberikan bimbingan dan saran-saran kepada penulis dalam pengerjaan revisi laporan tugas akhir ini.
6. Keluarga besar IF angkatan 2015 yang tidak bisa disebutkan satu persatu.
7. Teman-teman seperjuangan Andri Santriyana, Angga Nugraha, Nicola Chandra Prasetyu, Rizky Fadillah, Corinus Stenly, Eggy Putra Irawan, Iman Samsuri dan Yudha Saefulloh. yang selalu mengingatkan dan saling menyemangati penulis dalam proses tugas akhir ini.
8. Pihak-pihak lain yang juga membantu penulis untuk dapat menyelesaikan tugas akhir ini yang tidak dapat disebutkan satu per satu

Penulis menyadari bahwa tugas skripsi ini masih jauh dari kata sempurna. Oleh karena itu, penulis sangat mengharapkan saran dan masukan untuk pengembangan skripsi ini. Akhirnya, semoga skripsi ini dapat memberikan dampak positif terhadap pengembangan ilmu pengetahuan bagi seluruh manusia dan membantu semua pihak yang berkepentingan.

Bandung, 09 September 2019

Rismawan Ardiansyah



## DAFTAR ISI

LEMBAR PERSETUJUAN .....	
LEMBAR PERSETUJUAN .....	ii
LEMBAR PERSETUJUAN DAN PENGUJIAN TUGAS AKHIR.....	iii
ABSTRAK .....	iv
ABSTRACT.....	v
KATA PENGANTAR .....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR .....	xi
DAFTAR TABEL.....	xiv
BAB I.....	1
PENDAHULUAN .....	1
1.1. Latar Belakang Masalah .....	1
1.2. Rumusan Masalah.....	3
1.3. Maksud dan Tujuan .....	3
1.4. Metode Penelitian .....	4
1.4.1. Teknik Pengumpulan Data.....	5
1.4.2. Metode Pengembangan Sistem .....	5
1.5. Ruang Lingkup .....	9
1.6. Tempat Penelitian .....	9
1.7. Sistematika Penulisan .....	10
BAB II.....	12
LANDASAN TEORI.....	12
2.1. Konsep Dasar Pengembangan Sistem.....	12
2.1.1. Pengertian Sistem.....	12
2.1.2. Pengertian Informasi .....	12
2.2. Konsep Dasar Sistem Informasi Akademik.....	13
2.2.1. Pengertian Akademik.....	13
2.2.2. Pengertian Sistem Informasi .....	13

2.3.	SMS (Short Messaging Service).....	15
2.3.1.	Pengenalan Dasar SMS.....	15
2.3.2.	SMS Gateway.....	16
2.4.	Keamanan Komputer .....	17
2.4.1.	Serangan Komputer .....	19
2.4.2.	Autentikasi .....	20
2.4.3.	Algoritma Kriptograf .....	24
2.4.4.	Jenis Algoritma Kriptografi .....	27
2.5.	Program Penunjang Penelitian.....	37
2.5.1.	PHP .....	37
2.5.2.	MySQL .....	37
2.5.3.	Basis Data .....	38
2.5.4.	<i>Java Script</i> .....	41
2.6.	Metode Penelitian .....	42
BAB III .....		46
ANALISA DAN PERANCANGAN SISTEM.....		46
3.1.	Analisa Sistem .....	46
3.1.1.	Analisa Masalah.....	46
3.1.2.	Analisa Sistem yang Dibutuhkan.....	47
3.1.3.	Rancangan Sistem yang Diusulkan.....	51
3.1.4.	Use Case Diagram.....	53
3.1.5.	Activity Diagram .....	62
3.1.6.	Class Diagram.....	74
3.1.7.	Sequence Diagram .....	75
3.2.	Perancangan Interface.....	81
3.2.1.	Perancangan <i>Interface</i> Login .....	82
3.2.2.	Perancangan Interface Mengelola data .....	83
3.2.3.	Perancangan <i>Interface</i> Guru.....	91
BAB IV .....		94
IMPLEMENTASI DAN PENGUJIAN .....		94
4.1.	Implementasi.....	94

4.1.1. Implementasi Basis Data.....	94
4.1.2. Implementasi Antar Muka .....	97
4.2. Pengujian Perangkat Lunak .....	107
4.2.1. Pengujian Non Fungsional .....	107
4.2.2. Kasus Dan Hasil Pengujian.....	109
4.3. Kesimpulan Pengujian .....	113
BAB V .....	114
KESIMPULAN DAN SARAN.....	114
5.1. Kesimpulan .....	114
5.2. Saran .....	114
DAFTAR PUSTAKA .....	116
LAMPIRAN I .....	116
LAMPIRAN II .....	11624

## DAFTAR GAMBAR

Gambar 1.4 Waterfall (Sommerville, 2011) .....	6
Gambar 2.2.2.1. Blok Sistem Informasi yang Berinteraksi .....	14
Gambar 2.4.3. Proses enkripsi dan Dekripsi.....	26
Gambar 2.4.4.3. Fungsi Hash Satu Arah.....	29
Gambar 2.4.4.3.2.1. <i>Message with padding and size</i> .....	31
Gambar 2.4.4.3.2.2. <i>Input Formatting</i> .....	33
Gambar 2.4.4.3.2.3. <i>Rounds and Addition</i> .....	34
Gambar 2.6. Metode <i>Waterfall</i> SDLC .....	42
Gambar 3.1.3. Sistem yang diusulkan .....	52
Gambar 3.1.4. Usecase Diagram.....	53
Gambar 3.1.5.1. Activity Diagram Login .....	62
Gambar 3.1.5.2. Activity Diagram Authentikasi .....	63
Gambar 3.1.5.3.1. Activity Diagram Jadwal.....	64
Gambar 3.1.5.3.2. Activity Diagram Guru .....	65
Gambar 3.1.5.3.3. Activity Diagram Siswa .....	66
Gambar 3.1.5.3.4. Activity Diagram Nilai.....	67
Gambar 3.1.5.3.5. Activity Diagram Mata Pelajaran.....	68
Gambar 3.1.5.3.6. Activity Diagram Pengaturan.....	69
Gambar 3.1.5.4.1. Activity Diagram Jadwal.....	70
Gambar 3.1.5.4.2. Activity Diagram Kelas.....	71
Gambar 3.1.5.4.3. Activity Diagram Absen .....	72
Gambar 3.1.5.4.4. Activity Diagram Nilai.....	73
Gambar 3.1.6. Class Diagram .....	74
Gambar 3.1.7.1. Sequence Diagram Login .....	76
Gambar 3.1.7.2.2. Sequence Diagram Guru .....	77
Gambar 3.1.7.2.2.1. Sequence Diagram Jadwal .....	77
Gambar 3.1.7.2.3. Sequence Diagram Siswa.....	77
Gambar 3.1.7.2.4. Sequence Diagram Nilai .....	78
Gambar 3.1.7.2.5. Sequence Diagram Mata Pelajaran .....	78
Gambar 3.1.7.2.6. Sequence Diagram Admin .....	78
Gambar 3.1.7.2.7. Sequence Diagram Profile Sekolah.....	79
Gambar 3.1.7.2.9. Sequence Diagram Running Text .....	79
Gambar 3.1.7.2.8. Sequence Diagram Profile Sekolah.....	79
Gambar 3.1.7.3.1. Sequence Diagram Jadwal (Guru) .....	80
Gambar 3.1.7.3.2. Sequence Diagram Kelas (Guru) .....	80
Gambar 3.1.7.3.3. Sequence Diagram Nilai (Guru).....	81
Gambar 3.2.1.1. Interface Login .....	82
Gambar 3.2.1.2. Interface OTP .....	83
Gambar 3.2.2.1. Interface Halaman Admin .....	83

Gambar 3.2.2.2. Interface Jadwal .....	84
Gambar 3.2.2.3. Interface Guru .....	84
Gambar 3.2.2.4. Interface Siswa .....	85
Gambar 3.2.2.5.1. Interface Nilai .....	85
Gambar 3.2.2.5.2. Interface Nilai .....	86
Gambar 3.2.2.6. Interface Kelas .....	86
Gambar 3.2.2.7.2. Interface Deskripsi (Mata Pelajaran) .....	87
Gambar 3.2.2.7.1. Interface Mata Pelajaran .....	87
Gambar 3.2.2.7.3. Interface KKM (Mata Pelajaran) .....	88
Gambar 3.2.2.8.1. Interface Pengguna (Pengaturan) .....	88
Gambar 3.2.2.8.2. Interface Profile Sekolah (Pengaturan) .....	89
Gambar 3.2.2.8.3. Interface Ubah Semester (Pengaturan).....	89
Gambar 3.2.2.8.5. Interface Running Text (Pengaturan).....	90
Gambar 3.2.2.8.4. Interface Ubah Password (Pengaturan).....	90
Gambar 3.2.3.1. Interface Guru .....	91
Gambar 3.2.3.2. Interface Jadwal Guru .....	91
Gambar 3.2.3.3. Interface Kelas .....	92
Gambar 3.2.3.4.1. Interface Nilai .....	92
Gambar 3.2.3.4.3. Interface Masukan Nilai.....	93
Gambar 3.2.3.4.2. Interface Lihat Nilai .....	93
Gambar 4.1.1.2 Tabel Guru .....	95
Gambar 4.1.1.1 Tabel Admin .....	95
Gambar 4.1.1.3 Tabel Siswa .....	95
Gambar 4.1.1.4 Tabel Nilai.....	95
Gambar 4.1.1.6 Tabel Mata Pelajaran .....	96
Gambar 4.1.1.5 Tabel Kelas.....	96
Gambar 4.1.1.7 Tabel Deskripsi .....	96
Gambar 4.1.1.8 Tabel KKM .....	96
Gambar 4.1.1.9. Tabel Profil Sekolah.....	97
Gambar 4.1.1.10. Tabel Ubah Semester .....	97
Gambar 4.1.2.1.2. <i>Invalid User</i> .....	98
Gambar 4.1.2.1.1. Halaman Login Admin.....	98
Gambar 4.1.2.2.1. Halaman Autentikasi.....	99
Gambar 4.1.2.3.1. Halaman Utama Admin .....	100
Gambar 4.1.2.3.2. Halaman Jadwal (Admin) .....	100
Gambar 4.1.2.3.3. Halaman Siswa (Admin).....	101
Gambar 4.1.2.3.4. Halaman Guru (Admin) .....	101
Gambar 4.1.2.3.5. Halaman Mata Pelajaran (Admin) .....	102
Gambar 4.1.2.3.6. Halaman Hasil Nilai (Admin) .....	102
Gambar 4.1.2.3.7. Halaman Nilai (Admin) .....	102
Gambar 4.1.2.3.8. Halaman KKM (Admin) .....	103

Gambar 4.1.2.3.9. Halaman Deskripsi (Admin) .....	103
Gambar 4.1.2.3.10. Halaman Pengaturan (Admin).....	103
Gambar 4.1.2.3.12. Halaman Ubah Semester (Admin) .....	104
Gambar 4.1.2.3.11. Halaman Profil Sekolah (Admin) .....	104
Gambar 4.1.2.3.13. Halaman Ubah Password (Admin) .....	104
Gambar 4.1.2.3.14. Halaman Running Text (Admin) .....	105
Gambar 4.1.2.4.1. Halaman Utama (Guru).....	105
Gambar 4.1.2.4.3. Halaman Siswa (Guru).....	106
Gambar 4.1.2.4.2. Halaman Jadwal (Guru) .....	106
Gambar 4.1.2.4.4. Halaman Nilai (Guru) .....	106

## DAFTAR TABEL

Tabel 2.4.4.3.2. Parameter Fungsi Hash .....	30
Tabel 3.1.4.1.1. Deskripsi Login.....	54
Tabel 3.1.4.1.2. Deskripsi Autentikasi.....	55
Tabel 3.1.4.1.3. Data Jadwal.....	56
Tabel 3.1.4.1.4. Data Guru.....	57
Tabel 3.1.4.1.5. Data Siswa .....	58
Tabel 3.1.4.1.6. Data Nilai .....	59
Tabel 3.1.4.1.7. Data Mata Pelajaran .....	60
Tabel 3.1.4.1.8. Data Pengaturan .....	61
Tabel. 4.2.1. Pengujian Non Fungsional.....	107
Tabel. 4.2.2.1. Pengujian Login .....	110
Tabel. 4.2.2.2. Pengujian Mengelola Admin .....	111
Tabel. 4.2.2.3. Pengujian Mengelola Guru .....	112