

**IMPLEMENTASI SISTEM KRIPTOGRAFI RSA *SIGNATURE*  
DENGAN *SHA-256* PADA MEKANISME AUTENTIKASI *REST*  
*API***



oleh

ILYAS MAHFUD

M0118035

SKRIPSI

ditulis dan diajukan untuk memenuhi sebagian persyaratan  
memeroleh gelar Sarjana Matematika

**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
UNIVERSITAS SEBELAS MARET  
SURAKARTA**

**2022**

## DAFTAR ISI

PERNYATAAN . . . . .	ii
RINGKASAN . . . . .	iii
SUMMARY . . . . .	iv
MOTO . . . . .	v
PERSEMBAHAN . . . . .	vi
PRAKATA . . . . .	vii
DAFTAR ISI . . . . .	ix
DAFTAR TABEL . . . . .	x
DAFTAR GAMBAR . . . . .	xi
<b>I PENDAHULUAN</b>	<b>1</b>
1.1 Latar Belakang Masalah . . . . .	1
1.2 Perumusan Masalah . . . . .	2
1.3 Tujuan . . . . .	3
1.4 Manfaat Penelitian . . . . .	3
<b>II LANDASAN TEORI</b>	<b>4</b>
2.1 Tinjauan Pustaka . . . . .	4
2.2 Teori Penunjang . . . . .	5
2.2.1 Pengertian Dasar Kriptografi . . . . .	5
2.2.2 Algoritme <i>RS256</i> . . . . .	7
2.2.3 Algoritme RSA . . . . .	7
2.2.4 <i>SHA-256</i> . . . . .	8
2.2.5 <i>REST API</i> . . . . .	13

2.2.6	<i>JSON Web Token (JWT)</i> . . . . .	15
2.2.7	Java Spring Boot . . . . .	15
2.3	Kerangka Pemikiran . . . . .	16
<b>III METODE PENELITIAN</b>		<b>18</b>
<b>IV HASIL DAN PEMBAHASAN</b>		<b>19</b>
4.1	Implementasi <i>RS256</i> dengan Perhitungan Matematis . . . . .	19
4.2	Implementasi <i>RS256</i> dengan Program . . . . .	32
4.2.1	Menyiapkan Arsitektur Spring Boot . . . . .	32
4.2.2	<i>Model</i> . . . . .	34
4.2.3	<i>Repository</i> . . . . .	35
4.2.4	<i>UserDetails</i> . . . . .	35
4.2.5	<i>JWT Token Provider</i> . . . . .	35
4.2.6	<i>JWT Filter</i> . . . . .	38
4.2.7	<i>Web Security</i> . . . . .	39
4.2.8	<i>Controller</i> . . . . .	40
4.2.9	Pengujian Program . . . . .	44
<b>V PENUTUP</b>		<b>48</b>
5.1	Kesimpulan . . . . .	48
5.2	Saran . . . . .	48
<b>DAFTAR RUJUKAN</b>		<b>49</b>
<b>LAMPIRAN</b>		<b>51</b>