

**OPTIMALISASI ALGORITMA *ECDSA* PADA QR-CODE
SERTIFIKAT DIGITAL MENGGUNAKAN *HASH BLAKE2B*
DAN *SHA-128***

TUGAS AKHIR



Putri Suci Renita

NIM. 2201020017

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG**

2026

**OPTIMALISASI ALGORITMA *ECDSA* PADA QR-CODE
SERTIFIKAT DIGITAL MENGGUNAKAN *HASH BLAKE2B*
DAN *SHA-128***

Tugas Akhir

Skema Skripsi

*Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar Sarjana Teknik
pada Program Studi Teknik Informatika*



Putri Suci Renita

NIM. 2201020017

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG**

2026

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tugas akhir berjudul “Optimalisasi Algoritma *ECDSA* pada *QR-Code* Sertifikat Digital Menggunakan *Hash BLAKE2B* dan *SHA-128*” adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Apabila di kemudian hari terbukti pernyataan saya tidak benar dan melanggar peraturan yang berlaku dalam karya tulis dan hak intelektual, maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji dan menerima sanksi lainnya sesuai dengan peraturan yang berlaku. Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Maritim Raja Ali Haji.

Tanjungpinang, 01 Juli 2026



Putri Suci Renita
NIM 2201020017

The logo of Universitas Maritim Raja Ali Haji is a circular emblem. It features a blue outer ring with the university's name in yellow. Inside the ring is a yellow sailboat on blue waves, with a red star on its mast. The text "UNIVERSITAS MARITIM RAJA ALI HAJI" is written along the top inner edge, and "PELAJARAN DAN BERTANYA TIADA JERU" is written along the bottom inner edge.

© Hak Cipta Milik Universitas Maritim Raja Ali Haji, Tahun 2021

Hak Cipta Dilindungi Undang- Undang

Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah; dan pengutipan tersebut tidak merugikan kepentingan Universitas Maritim Raja Ali Haji.

Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Universitas Maritim Raja Ali Haji.

HALAMAN PERSETUJUAN

HALAMAN PERSETUJUAN

Judul : Optimalisasi Algoritma *ECDSA* pada *QR-Code*
Sertifikat Digital Menggunakan Hash *BLAKE2B* dan
SHA-128
Nama : Putri Suci Renita
NIM : 2201020017
Program Studi : Teknik Informatika
Tanggal Persetujuan : Kamis, 11 Juni 2026

Disetujui oleh,
Komisi Pembimbing



Ferdi Chahyadi, S.Kom., M.Cs.
(Ketua)



Novrizal Fattah Fahmitra, S.Kom., M.Kom.
(Anggota)

HALAMAN PENGESAHAN

HALAMAN PENGESAHAN

Judul : Optimalisasi Algoritma *ECDSA* pada *QR-Code*
Sertifikat Digital Menggunakan *Hash BLAKE2B*
dan *SHA-128*

Nama : Putri Suci Renita

NIM : 2201020017

Telah berhasil dipertahankan di hadapan Komisi Penguji sebagai bagian persyaratan yang diperlukan dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro Dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

KOMISI PENGUJI

Ketua	: Nurul Hayaty, S.T., M.Cs.	
Anggota I	: Nolan Efranda, M.Kom.	
Anggota II	: Ir. Muhamad Fadli, M.Kom.	
Anggota III	: Ferdi Chahyadi, S.Kom., M.Cs.	
Anggota IV	: Novrizal Fattah Fahmitra, S.Kom., M.Kom.	

Mengetahui,

Ketua Jurusan Teknik Elektro dan Informatika

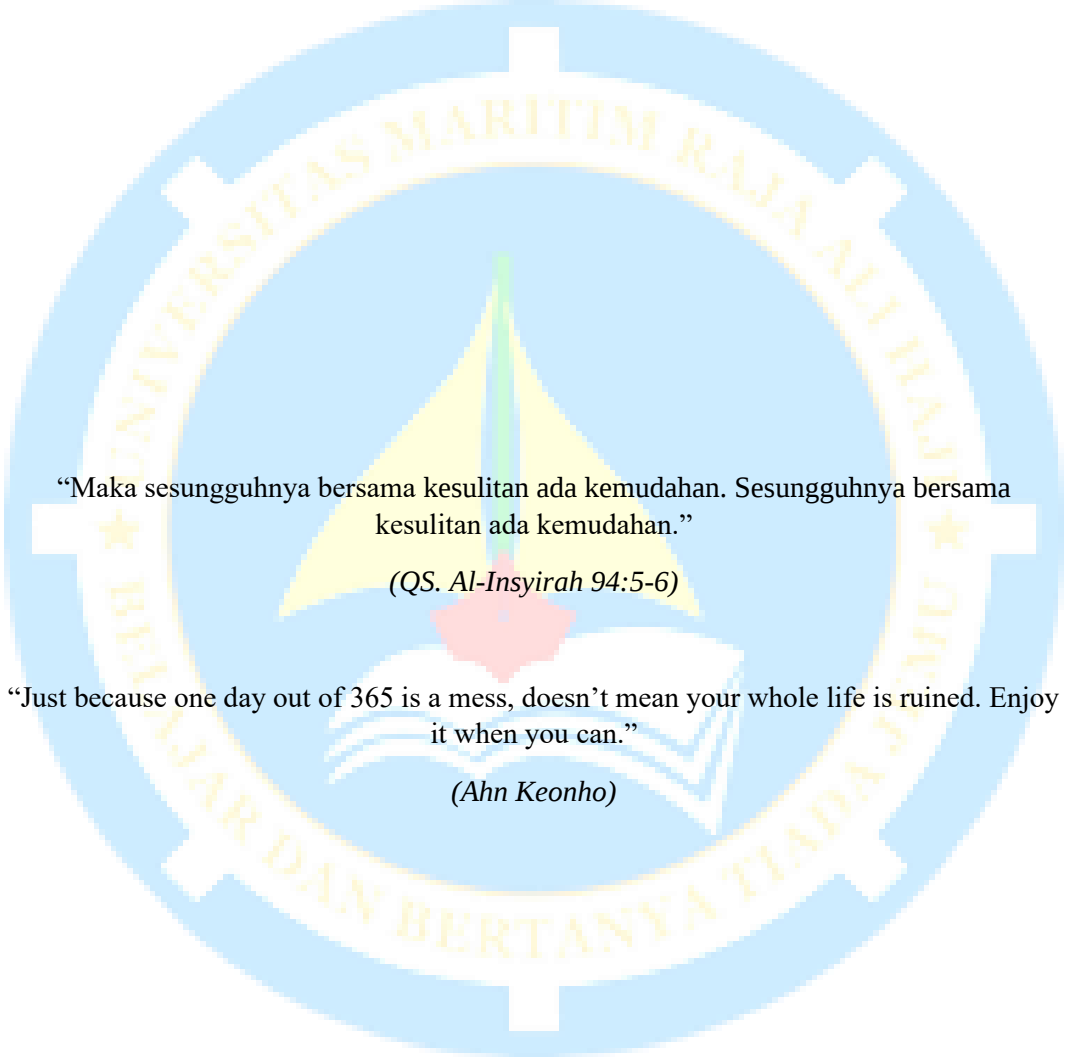



Hollanda Ayu Kusuma, S.IK., M.Si
NIP. 198904012019031016

Tanggal Ujian: 22 Mei 2026

Tanggal Lulus: 11 Juni 2026

HALAMAN MOTTO



“Maka sesungguhnya bersama kesulitan ada kemudahan. Sesungguhnya bersama kesulitan ada kemudahan.”

(QS. Al-Insyirah 94:5-6)

“Just because one day out of 365 is a mess, doesn’t mean your whole life is ruined. Enjoy it when you can.”

(Ahn Keonho)

PRAKATA

Puji dan syukur dipanjatkan kepada Allah subhanahu wa ta'ala atas segala karunia-Nya sehingga laporan tugas akhir ini berhasil diselesaikan. Adapun judul yang diangkat dalam penelitian ini **“Optimalisasi Algoritma ECDSA pada QR-Code Sertifikat Digital Menggunakan Hash BLAKE2B dan SHA-128”**.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih kepada:

1. Bapak Ferdi Chahyadi, S.Kom., M.Cs., selaku Dosen Pembimbing I, yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan bimbingan, arahan, masukan, serta motivasi selama proses penyusunan laporan tugas akhir ini.
2. Bapak Novrizal Fattah Fahmitra, S.Kom., M.Kom., selaku Dosen Pembimbing II, yang telah memberikan bimbingan, saran, kritik, serta masukan yang membangun sehingga laporan tugas akhir ini dapat terselesaikan dengan baik.
3. Seluruh dosen Program Studi Teknik Informatika Universitas Maritim Raja Ali Haji yang telah memberikan ilmu pengetahuan, pengalaman, serta wawasan selama masa perkuliahan.
4. Seluruh staf Tata Usaha Fakultas Teknik dan Teknologi Kemaritiman Universitas Maritim Raja Ali Haji yang telah memberikan bantuan, pelayanan, serta kemudahan dalam proses administrasi akademik selama penulis menempuh pendidikan hingga penyusunan laporan tugas akhir ini.
5. Dinas Pendidikan, Kepemudaan dan Olahraga Kabupaten Lingga yang telah memberikan izin dan kesempatan kepada penulis untuk melaksanakan penelitian.
6. Bapak Rendra Twadika, S.Pd., Bapak Mokhtaraidi, S.Pd., dan Bapak Supardi, S.Pd., M.Pd., yang telah meluangkan waktu serta memberikan bantuan, informasi, dan dukungan selama proses pengumpulan data dan pelaksanaan penelitian.
7. Papa dan Mama tercinta, Rendra Twadika dan Ria Sita, yang tidak pernah lelah memberikan doa, kasih sayang, motivasi, serta dukungan moral maupun

material. Terima kasih atas setiap pengorbanan, kesabaran, dan kepercayaan yang telah diberikan. Kehadiran Papa dan Mama menjadi sumber kekuatan dan semangat bagi penulis dalam menyelesaikan laporan tugas akhir ini.

8. Kepada Leonardo Tegarsuan, yang telah memberikan doa, dukungan, motivasi, serta selalu menemani dan memberikan semangat kepada penulis selama proses penyusunan laporan tugas akhir ini.
9. Kepada Syerli, Patika, Wawa, Tarisa, Jingga dan Putri yang telah memberikan semangat, bantuan, serta kebersamaan selama masa perkuliahan hingga penyusunan laporan tugas akhir ini.
10. Semua pihak yang telah membantu dalam penyusunan laporan tugas akhir ini, baik secara langsung maupun tidak langsung, yang tidak dapat penulis sebutkan satu per satu.

Akhir kata, penulis berharap semoga laporan tugas akhir ini dapat memberikan manfaat, baik bagi penulis maupun pihak lain yang membutuhkan.

Tanjungpinang, 01 Juli 2026



Putri Suci Renita

DAFTAR ISI

HALAMAN PERSETUJUAN.....	iv
HALAMAN PENGESAHAN.....	v
HALAMAN MOTTO	vi
ABSTRAK	vii
ABSTRACT	viii
PRAKATA.....	ix
DAFTAR ISI.....	xi
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xvi
DAFTAR LAMPIRAN	xviii
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	3
C. Batasan Penelitian	3
D. Tujuan Penelitian	3
E. Manfaat Penelitian	4
BAB II KAJIAN LITERATUR	6
A. Tinjauan Pustaka	6
B. Landasan Teori.....	15
1. QR Code.....	15
2. Kriptografi.....	16
3. <i>Elliptic Curve Digital Signature Algorithm</i>	17
4. Tanda Tangan Digital.....	18
5. BLAKE2B.....	24

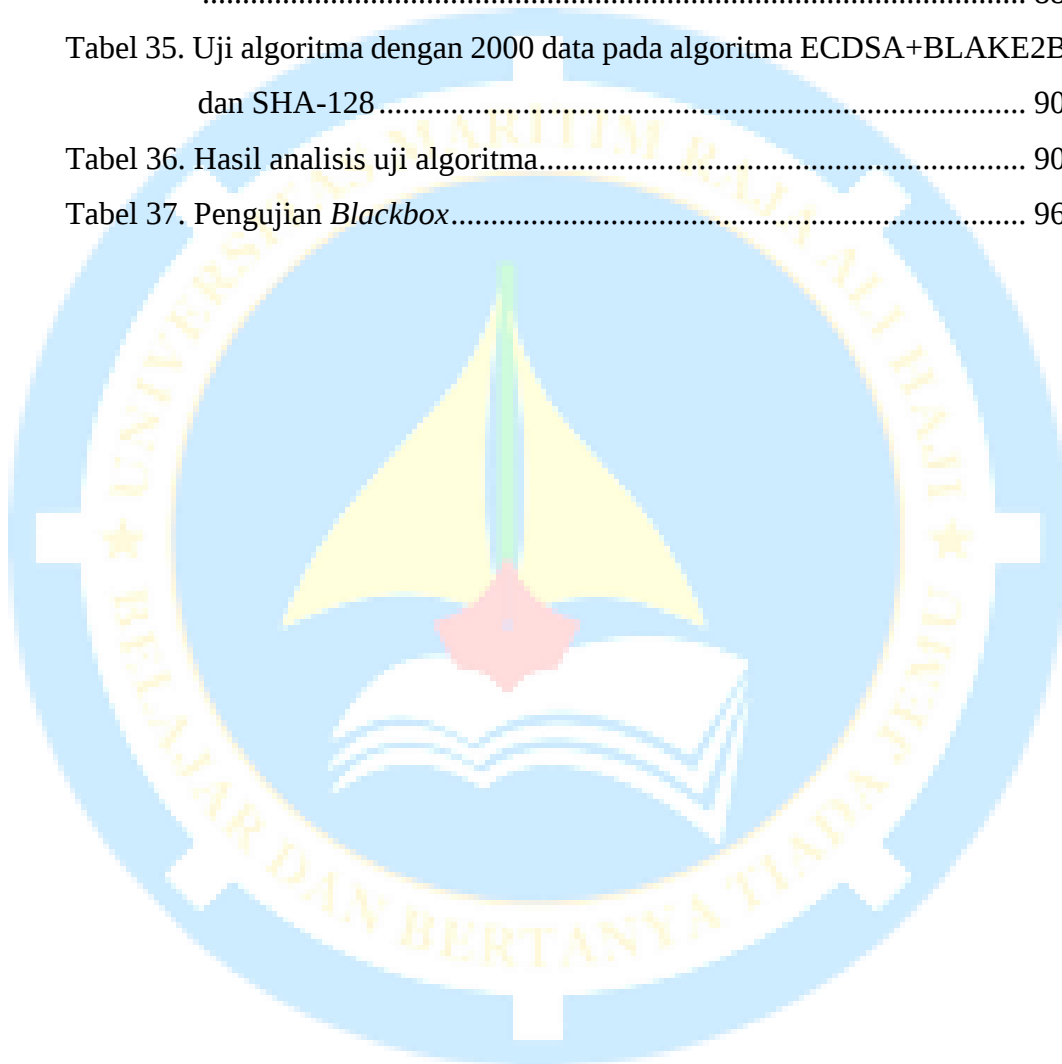
6. Secure Hash Algorithm (SHA)	26
7. Indikator Pengukuran Kinerja Algoritma.....	27
BAB III METODE PENELITIAN.....	31
A. Waktu dan Tempat Penelitian	31
1. Tantangan dan hambatan.....	32
B. Bahan dan Alat	32
1. Bahan Penelitian.....	32
2. Alat Penelitian.....	33
C. Prosedur Pelaksanaan Penelitian.....	34
1. Tahapan Penelitian	34
2. Variabel dan Jenis Data Penelitian.....	35
3. Rancangan Percobaan	36
4. Diagram Alir Prosedur Penelitian	37
5. Prosedur Analisis Data	38
D. Perancangan Sistem	38
1. Arsitektur Sistem Tanda Tangan Digital.....	38
2. Perancangan Proses Tanda Tangan Digital ECDSA.....	42
3. Mekanisme Integrasi QR-Code pada Sertifikat Digital	45
4. Rancangan Antarmuka	46
E. Analisis Data	48
1. Model Analisis	48
2. Teknik Analisis	49
3. Proses Perhitungan Manual Hash SHA-128	53
4. Proses Perhitungan Manual Hash BLAKE2B.....	59
5. Proses Perhitungan Manual ECDSA.....	65
6. Rencana Penyajian Hasil.....	67

7. Rencana Interpretasi Data	68
BAB IV HASIL DAN PEMBAHASAN	69
A. Hasil Implementasi Sistem <i>E-Sign</i> Sertifikat Digital	69
1. Implementasi Halaman <i>Dashboard</i>	69
2. Implementasi Halaman <i>Upload</i> Sertifikat	69
3. Implementasi Halaman Data Sertifikat	70
4. Implementasi Halaman Verifikasi Sertifikat	71
B. Hasil Implementasi Struktur Metadata dan QR-Code	73
C. Pembahasan Pengujian Algoritma Penandatanganan	74
1. ECDSA Tanpa Hash	75
2. ECDSA dan SHA-128	79
3. ECDSA dan BLAKE2b	82
4. ECDSA Kombinasi BLAKE2b dan SHA-128	86
5. Hasil Analisis Uji Algoritma Penandatanganan	90
D. Pengujian <i>Generate QR</i> dengan <i>Digisign</i> dan Tidak	93
E. Pengujian <i>Blackbox</i> Sistem <i>E-Sign</i> Sertifikat Digital	96
BAB V PENUTUP	98
A. Kesimpulan	98
B. Saran	98
DAFTAR PUSTAKA	99
LAMPIRAN	103

DAFTAR TABEL

Tabel 1. Penelitian Terdahulu	8
Tabel 2. Encoding mode	15
Tabel 3. Tabel Secp256r1	20
Tabel 4. Kategori Penilaian <i>Avalanche Effect</i>	29
Tabel 5. Kategori Penilaian Keandalan (Reliability)	30
Tabel 6. Bahan penelitian yang digunakan	32
Tabel 7. Perangkat keras yang digunakan.....	33
Tabel 8. Perangkat lunak yang digunakan	33
Tabel 9. Variabel dan jenis data penelitian	35
Tabel 10. Rancangan percobaan	37
Tabel 11. Data Sampel Waktu Eksekusi (ms) per Percobaan.....	49
Tabel 12. Rekapitulasi Waktu Eksekusi Rata-rata.....	50
Tabel 13. Kategori Penilaian <i>Avalanche Effect</i> dan Hasil Sampel	51
Tabel 14. Perbandingan Nilai Hash Tiap Bit	51
Tabel 15. Kategori Penilaian Keandalan Sistem.....	52
Tabel 16. Data Sampel Pengujian Verifikasi per Algoritma	52
Tabel 17. Konversi ASCII Ke Hex pada proses SHA-128.....	53
Tabel 18. Proses Padding pada SHA-128	54
Tabel 19. Inisialisasi Vektor Pada Proses BLAKE2B	59
Tabel 20. Blok Pesan pada proses blake2b	60
Tabel 21. Hasil Padding Teks pada proses Blake2b	60
Tabel 22. Metode Little Endian pada Proses Blake2b	61
Tabel 23. Metode Big-endian pada proses BLAKE2B.....	61
Tabel 24. Hasil pemetaan 16 word BLAKE2B.....	61
Tabel 25. Round G pada proses BLAKE2B	64
Tabel 27. Data yang digunakan sebagai pemrosesan algoritma	74
Tabel 28. Komponen R dan S pada proses <i>ECDSA</i> tanpa Hash	76
Tabel 29. Uji algoritma dengan 2000 data pada algoritma <i>ECDSA</i> Tanpa Hash	78
Tabel 30. Komponen R dan S pada proses <i>ECDSA</i> + <i>SHA-128</i>	80

Tabel 31. Uji algoritma dengan 2000 data pada algoritma <i>ECDSA+SHA-128</i>	82
Tabel 32. Komponen R dan S pada proses <i>ECDSA+BLAKE2B</i>	84
Tabel 33. Uji algoritma dengan 2000 data pada algoritma Ecdsa dan Blake2b	86
Tabel 34. Komponen R dan S pada proses ECDSA+BLAKE2B Dan SHA-128	88
Tabel 35. Uji algoritma dengan 2000 data pada algoritma ECDSA+BLAKE2B dan SHA-128	90
Tabel 36. Hasil analisis uji algoritma.....	90
Tabel 37. Pengujian <i>Blackbox</i>	96



DAFTAR GAMBAR

Gambar 1. Contoh QR-Code untuk pesan “Hello World”	15
Gambar 2. Algoritma Kriptografi Simetris	17
Gambar 3. Algoritma Kriptografi Asimetris	17
Gambar 4. Alur Tanda Tangan Digital dengan Fungsi <i>Hash</i> dan algoritma kriptografi kunci <i>public</i>	19
Gambar 5. Visualisasi Parameter Domain Kurva Eliptik pada Algoritma ECDSA ..	20
Gambar 6. Tahapan ECDSA	21
Gambar 7 Inisialisasi dari variabel <i>v</i> untuk fungsi <i>f</i>	25
Gambar 8. Fungsi <i>G</i> Kurva Eliptik	25
Gambar 9. Hasil akhir fungsi <i>F</i> Kurva Eliptik	25
Gambar 10. Mekanisme algoritma <i>BLAKE2B</i>	26
Gambar 11. Ilustrasi Mekanisme <i>Hash</i> pada <i>SHA</i>	27
Gambar 12. Peta Lokasi Penelitian	31
Gambar 13. Tampak depan kantor Dinas Pendidikan, Kepemudaan dan Olahraga Kabupaten Lingga yang akan dilakukan penelitian	31
Gambar 14. Diagram Alir Prosedur Penelitian	37
Gambar 15. Arsitektur sistem tanda tangan digital pada <i>admin</i>	38
Gambar 16. Arsitektur sistem tanda tangan digital	40
Gambar 17. Proses penandatanganan digital <i>ECDSA (Private key)</i>	42
Gambar 18. Proses verifikasi tanda tangan digital (<i>Public key</i>)	44
Gambar 19. Mekanisme Integrasi <i>QR-Code</i> pada Sertifikat Digital	45
Gambar 20. <i>Wireframe User</i>	46
Gambar 21. <i>Wireframe Admin</i>	47
Gambar 22. Rumus mencari nilai <i>h[0]</i>	60
Gambar 23. Halaman <i>Dashboard</i>	69
Gambar 24. Halaman <i>Upload Sertifikat</i>	70
Gambar 25. Halaman Data Sertifikat	71
Gambar 26. Halaman Verifikasi Sertifikat	72
Gambar 27. Hasil metadata	73
Gambar 28. Metadata <i>ECDSA-Tanpa Hash</i>	75
Gambar 29. Proses Pesan ke dalam serialisasi	76

Gambar 30. <i>Infrakey</i> tanpa Hash.....	76
Gambar 31. Visualisasi Garis Kurva Eliptik Pada <i>ECDSA</i> tanpa Hash.....	77
Gambar 32. Validasi Integritas <i>ECDSA</i> -Tanpa Hash	77
Gambar 33. Hasil Uji 2000 data menggunakan Algoritma <i>ECDSA</i> Tanpa Hash	78
Gambar 34. Metadata <i>ECDSA</i> + <i>SHA-128</i>	79
Gambar 35. Hasil <i>Payload ECDSA+SHA-128</i>	79
Gambar 36. <i>Infrakey ECDSA+SHA-128</i>	80
Gambar 37. Visualisasi Garis Kurva Eliptik Pada <i>ECDSA</i> dan <i>SHA-128</i>	80
Gambar 38. Validasi Integritas <i>ECDSA+SHA-128</i>	81
Gambar 39. Hasil Uji 2000 data menggunakan Algoritma <i>ECDSA+ SHA-128</i>	82
Gambar 40. Metadata <i>ECDSA+BLAKE2B</i>	83
Gambar 41. Hasil Hash <i>ECDSA+BLAKE2B</i>	83
Gambar 42. <i>Infrakey ECDSA+BLAKE2B</i>	84
Gambar 43. Visualisasi Garis Kurva Eliptik Pada <i>ECDSA</i> dan <i>BLAKE2b</i> ...	84
Gambar 44. Validasi Integritas <i>ECDSA+BLAKE2B</i>	85
Gambar 45. Uji 2000 data <i>ECDSA+BLAKE2B</i>	85
Gambar 46. Metadata <i>ECDSA+BLAKE2B</i> Dan <i>SHA-128</i>	86
Gambar 47. Hasil Hash <i>ECDSA+BLAKE2B</i> Dan <i>SHA-128</i>	87
Gambar 48. <i>Infrakey ECDSA+BLAKE2B</i> Dan <i>SHA-128</i>	87
Gambar 49. Visualisasi Garis Kurva Eliptik Pada <i>ECDSA</i> kombinasi <i>SHA-128</i> dan <i>BLAKE2b</i>	88
Gambar 50. Validasi Integritas <i>ECDSA+BLAKE2B</i> Dan <i>SHA-128</i>	89
Gambar 51. Uji 2000 Data <i>ECDSA+BLAKE2B</i> Dan <i>SHA-128</i>	89
Gambar 52. Perbandingan <i>Avalanche Effect</i> (%).....	90
Gambar 53. Perbandingan Waktu Eksekusi Rata-rata (ms).....	91
Gambar 54. Perbandingan Nilai Efisiensi (pts)	92
Gambar 55. Perbandingan Reliabilitas (%).....	92

DAFTAR LAMPIRAN

Lampiran 1 Kurva Eliptik	103
Lampiran 2 Pembangkitan kunci private dan kunci publik	103
Lampiran 3 Menghitung nilai <i>hash</i> pesan.....	103
Lampiran 4 Menghitung nilai Empheral-key.....	103
Lampiran 5 Menghitung titik kurva eliptik.....	103
Lampiran 6 Hitung komponen tanda tangan pertama.....	103
Lampiran 7 Menghitung komponen tanda tangan kedua.....	103
Lampiran 8 Hasil hitung tanda tangan	103
Lampiran 9 Tahap verifikasi menghitung <i>invers</i> S	103
Lampiran 10 Verifikasi dua parameter komponen	104
Lampiran 11 Hitung titik kombinasi hasil	104
Lampiran 12 Penentuan nilai verifikasi	104
Lampiran 13 Pembangkitan Keabsahan tanda tangan	104
Lampiran 14 Verifikasi penerima kunci	104
Lampiran 15 Hitung nilai <i>hash</i> Verifikasi penerima kunci.....	104
Lampiran 16 Pembuktian hasil verifikasi kunci	104
Lampiran 17 Dokumentasi Bersama Sekretaris Dinas Pendidikan, Kepemudaan dan Olahraga Kabupaten Lingga	105
Lampiran 18 Dokumentasi Bersama Sekretaris Dinas Pendidikan, Kepemudaan Dan Olahraga Kabupaten Lingga(2).....	105
Lampiran 19 Dokumentasi Bersama Staff Dinas Pendidikan, Kepemudaan dan Olahraga Kabupaten Lingga	106