

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128
UNTUK KEAMANAN DATA PELANGGAN PADA
PROVIDER LAYANAN WIFI**

SKRIPSI

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Jenjang Strata Satu (S1)
Pada Program Studi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Ponorogo



MUHAMMAD ANDARA GHAZY AR RAMADHAN
22533623

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH PONOROGO**

2026

HALAMAN PENGESAHAN

Nama : Muhammad Andara Ghazy Ar Ramadhan
NIM : 22533623
Program Studi : Teknik Informatika
Fakultas : Fakultas Teknik
Judul Skripsi : IMPLEMENTASI KRIPTOGRAFI AES-128 UNTUK
KEAMANAN DATA PELANGGAN PADA
PROVIDER LAYANAN WIFI

Isi dan formatnya telah disetujui dan dinyatakan memenuhi syarat
Untuk melengkapi persyaratan guna memperoleh Gelar Sarjana
pada Program Studi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Ponorogo

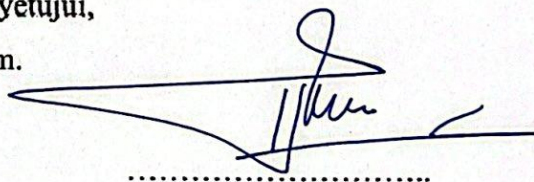
Ponorogo, 28 Juli 2026

Menyetujui,

Ismail Abdurrozzaq Z., S.Kom, M.Kom.

NIK. 19880728 201804 13

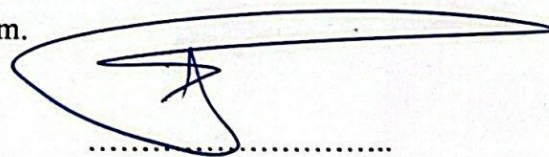
(Dosen Pembimbing Utama)



Adi Fajaryanto Cobantoro, S.Kom, M.Kom.

NIK. 19840924 201309 13

(Dosen Pembimbing Pendamping)



Mengetahui,

Ketua Program Studi Teknik Informatika



Dekan Fakultas Teknik,

Edy Kurniawan, S.T., M.T.

NIK. 19771026 200810 12



Adi Fajaryanto C., S.Kom., M.Kom.

NIK. 19840924 201309 13

PERNYATAAN ORISINALITAS SKRIPSI

Nama : Muhammad Andara Ghazy Ar Ramadhan
NIM : 22533623
Program Studi : Teknik Informatika

Dengan ini menyatakan bahwa Skripsi saya dengan judul “IMPLEMENTASI KRIPTOGRAFI AES-128 UNTUK KEAMANAN DATA PELANGGAN PADA PROVIDER LAYANAN WIFI” bahwa berdasarkan hasil penelusuran berbagai karya ilmiah, gagasan, dan masalah ilmiah dirancang/ teliti di dalam Naskah Skripsi ini adalah asli dari pemikiran saya. Tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam Naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur plagiarisme, saya bersedia Ijazah saya dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini dibuat dengan sesungguhnya dan sebenar-benarnya.

Ponorogo, 28 Juli 2026

Mahasiswa,



Muhammad Andara Ghazy Ar Ramadhan
NIM. 22533623

HALAMAN BERITA ACARA UJIAN

Nama : Muhammad Andara Ghazy Ar Ramadhan
NIM : 22533623
Program Studi : Teknik Informatika
Fakultas : Fakultas Teknik
Judul Skripsi : IMPLEMENTASI KRIPTOGRAFI AES-128 UNTUK
KEAMANAN DATA PELANGGAN PADA
PROVIDER LAYANAN WIFI

Telah diuji dan dipertahankan dihadapan

Dosen penguji tugas akhir jenjang Strata Satu (S1) pada :

Hari : Jumat

Tanggal : 24 Juli 2026

Dosen Penguji

Ismail Abdurrozzaq Z., S.Kom, M.Kom.

NIK. 19880728 201804 13

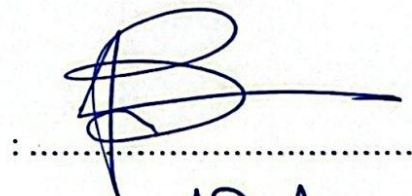
(Ketua Penguji)


:

Ir. Mohammad Bhanu S., S.T., M.Kom.

NIK. 19800225 201309 13

(Anggota Penguji I)


:

Indah Puji Astuti, S.Kom, M.Kom.

NIK. 19860424 201609 13

(Anggota Penguji II)


:

Mengetahui,

Ketua Program Studi Teknik Informatika


Dekan Fakultas Teknik,
Edy Kurniawan, S.T., M.T.
NIK. 19771026 200810 12


Adi Fajaryanto C., S.Kom., M.Kom.
NIK. 19840924 201309 13

BERITA ACARA BIMBINGAN SKRIPSI

Nama : MUHAMMAD ANDARA GHAZY AR
RAMADHAN

NIM : 22533623

Judul Skripsi : IMPLEMENTASI KRIPTOGRAFI AES-128
UNTUK KEAMANAN DATA PELANGGAN
PADA PROVIDER LAYANAN WIFI

Dosen Pembimbing Utama : Ismail Abdurrozzaq Zulkarnain, S.Kom, M.Kom

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Status
1	05 / 11 2025	Diskusi Tema	Mendiskusikan tema yang paling minat	✓
2	07 / 11 2025	BAB 1	• Penambahan latar belakang untuk membandingkan algoritma • Menambahkan sitasi	✓
3	25 / 11 2025	BAB 1	Penambahan/detailkan permasalahan	✓
4	05 / 12 2025	BAB 1	Mengganti objek tempat yang baru	✓
5	15 / 12 2025	BAB 1	Lanjut BAB 2 dan 3	✓

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Status
6	24 / 12 2025	BAB 2	Perbaikan tabel	✓
7	05 / 01 2026	BAB 2 dan 3	• Revisi analisis kebutuhan fungsional dan nonfungsional • Revisi panjang atribut database	✓
8	07 / 01 2026	BAB 1-3	ACC SEMPRO	✓
9	21 / 05 2026	BAB 4	Memperlihatkan revisian sempro dan sistem dasar	✓
10	18 / 06 2026	BAB 4	Merevisi bimbingan sistem sebelumnya (mendekripsi chipertext ke website online)	✓
11	30 / 06 2026	BAB 4	• Tambah pengujian sistem • Penyesuaian konsep interface BAB 3 • Diperinci pengujian enkripsi dengan website	✓
12	02 / 07 2026	BAB 4	Memperbaiki sub bab pengujian	✓

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Status
13	03 / 07 2026	BAB 4	Penyesuaian pada sub bab pengujian white box testing	✓
14	06 / 07 2026	BAB 4	Tambahkan screenshot pada tabel pengujian white box	✓
15	08 / 07 2026	BAB 5	Perbaiki kesimpulan dan saran	✓
16	10 / 07 2026	BAB 5	ACC SIDANG	✓

Dosen Pembimbing Utama,



Ismail Abdurrozzaq Zulkarnain, S.Kom, M.Kom
NIK. 1988072820180413

BERITA ACARA BIMBINGAN SKRIPSI

Nama : MUHAMMAD ANDARA GHAZY AR
RAMADHAN

NIM : 22533623

Judul Skripsi : IMPLEMENTASI KRIPTOGRAFI AES-128
UNTUK KEAMANAN DATA PELANGGAN
PADA PROVIDER LAYANAN WIFI

Dosen Pembimbing : Adi Fajaryanto Cobantoro, S.Kom, M.Kom

Pendamping

PROSES PEMBIMBINGAN

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Status
1	25 / 11 2025	BAB 1	Penambahan sitasi	✓
2	09 / 12 2025	BAB 1	Tambah referensi dan lanjut bab 1 dan 2	✓
3	12 / 12 2025	BAB 2	Tambah teori algoritma	✓
4	16 / 12 2025	BAB 2	Tambahkan ERD dan kurang DFD	✓
5	22 / 12 2025	BAB 3	Lanjut bab 3	✓

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Status
6	29 / 12 2025	BAB 3	• Hapus tabel data terenkripsi • Revisi panjang atribut database	✓
7	07 / 01 2026	BAB 3	Revisi alur pengembangan sistem	✓
8	13 / 01 2026	BAB 3	ACC SEMPRO	✓
9	31 / 05 2026	BAB 4	Penyesuaian perhitungan enkripsi dan dekripsi	✓
10	31 / 05 2026	BAB 4	Penyesuaian perhitungan enkripsi dan dekripsi	✓
11	12 / 06 2026	BAB 4	• Memperlihatkan sistem awal/ dasar • Revisi menu sistem dan penambahan field database	✓
12	18 / 06 2026	BAB 4	Bimbingan sistem dan lanjut pembuatan di BAB 4	✓
13	26 / 06 2026	BAB 4	• Penyesuaian latar belakang tentang CBC dan IV	✓

No	Tanggal	Materi Yang Dikonsultasikan	Saran Pembimbing / Hasil	Status
			• Teori BAB 2, Flowchart, dsb • Perhitungan enkripsi dan dekripsi	
14	06 / 07 2026	BAB 4	Penyesuaian tabel path testing	✓
15	08 / 07 2026	BAB 5	Penyesuaian kesimpulan dan saran	✓
16	10 / 07 2026	BAB 5	ACC SIDANG	✓

Dosen Pembimbing Pendamping,



Adi Fajaryanto Cobantoro, S.Kom, M.Kom
NIK. 1984092420130913

MOTTO

“Terbentur, terbentur, terbentur, terbentuk.”

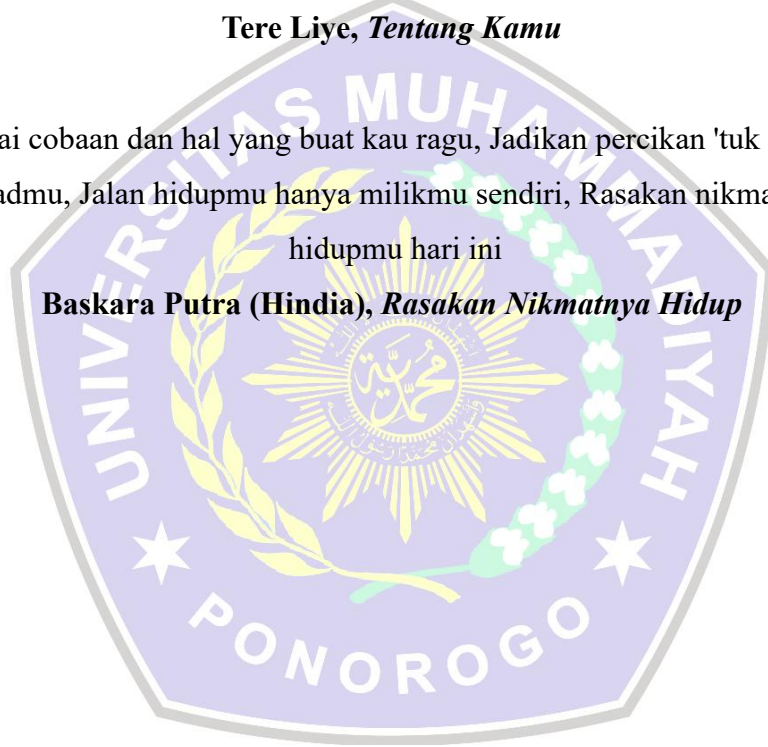
Tan Malaka

“Terimakasih atas pelajaran tentang keteguhan. Aku tau sekarang. Pertanyaan paling penting adalah bukan berapa kali kita gagal, melainkan berapa kali kita bangkit lagi, lagi, dan lagi dan lagi setelah gagal tersebut. Jika kita gagal 1000x, maka pastikan kita bangkit 1001x lagi.”

Tere Liye, Tentang Kamu

Berbagai cobaan dan hal yang buat kau ragu, Jadikan percikan 'tuk menerpa tekadmu, Jalan hidupmu hanya milikmu sendiri, Rasakan nikmatnya hidupmu hari ini

Baskara Putra (Hindia), Rasakan Nikmatnya Hidup



HALAMAN PERSEMBAHAN

Segala puji dan syukur penulis panjatkan ke hadirat Allah Swt. atas segala rahmat, nikmat, dan karunia-Nya yang telah memberikan kesehatan, kekuatan, serta kemudahan kepada penulis dalam menyelesaikan skripsi ini. Berkat pertolongan dan kehendak-Nya, seluruh proses penyusunan skripsi dapat dilalui hingga akhirnya dapat terselesaikan dengan baik.

Dalam penyelesaian skripsi ini, penulis menyadari bahwa proses yang dilalui tidak terlepas dari bantuan, bimbingan, dukungan, dan doa dari berbagai pihak. Oleh karena itu, dengan penuh rasa hormat dan terima kasih, skripsi ini penulis persembahkan kepada:

1. Kedua orang tua tercinta, yang telah membesarkan dan mendidik penulis dengan penuh kasih sayang, cinta, serta kesabaran. Terima kasih atas setiap doa, dukungan, kepercayaan, dan pengorbanan yang telah diberikan, baik dalam bentuk moral maupun materiil. Segala pencapaian yang penulis raih hingga berada di titik ini tidak terlepas dari doa dan perjuangan Bapak dan Ibu. Semoga segala kebaikan, kasih sayang, dan pengorbanan yang telah diberikan senantiasa mendapat balasan terbaik dari Allah Swt.
2. Terima kasih kepada Dosen Pembimbing, Bapak Ismail Abdurrozzaq Zulkarnain, S.Kom., M.Kom., dan Bapak Adi Fajaryanto Cobantoro, S.Kom., M.Kom., yang telah membimbing dan memberikan banyak ilmu pengetahuan serta motivasi, sehingga penulis dapat menyelesaikan skripsi ini.
3. Seluruh dosen Program Studi Teknik Informatika, yang telah memberikan ilmu, pengalaman, dan bimbingan selama penulis menempuh pendidikan. Terima kasih atas ilmu dan dedikasi yang telah diberikan sebagai bekal bagi penulis di masa mendatang.
4. Teman-teman sekelas dan teman-teman Teknik Informatika angkatan 2022. Terima kasih atas segala bantuan, kebersamaan, pengalaman, dan kenangan yang telah diberikan selama masa perkuliahan.

5. Teman-teman yang tergabung dalam grup WhatsApp GH STARKOST, yang telah menjadi bagian dari perjalanan penulis selama masa perkuliahan. Terima kasih atas kebersamaan, canda tawa, diskusi, serta berbagai cerita yang terjalin di kost sebagai tempat berkumpul, mengerjakan tugas, dan saling membantu selama menjalani perkuliahan. Berbagai momen yang telah dilalui bersama menjadi bagian berharga yang akan selalu dikenang dalam perjalanan penulis menyelesaikan pendidikan.
6. Sahabat satu circle sejak masa SMA yang tergabung dalam grup WhatsApp “Kenyoters”, yang telah tumbuh bersama hingga kini dan sudah seperti keluarga bagi penulis. Terima kasih karena selalu hadir, saling mendukung, memberikan semangat, serta menjaga kebersamaan di tengah kesibukan masing-masing. Semoga persahabatan ini tetap terjaga dan kita dapat menyelesaikan setiap perjuangan serta meraih keberhasilan bersama.
7. Untuk seseorang yang belum bisa kutulis dengan jelas namanya di sini. Terima kasih telah menjadi salah satu sumber semangat dalam menyelesaikan skripsi ini yang menjadi salah satu bentuk upaya dalam memantaskan diri. Kehadiranmu, meskipun tidak selalu terlihat secara langsung, telah memberikan dorongan tersendiri bagi penulis untuk terus berusaha. Meskipun saat ini tidak diketahui keberadaanmu, entah di bumi bagian mana, dan semoga tidak sedang menggenggam tangan lain. Seperti kata B.J. Habibie, *“Kalau memang dia dilahirkan untuk saya, kamu jungkir balik pun saya yang akan dapat.”*
8. *Last but not least*, untuk diri sendiri. Terima kasih telah percaya pada diri sendiri, tetap berusaha dan bekerja keras dalam menyelesaikan apa yang telah dimulai, tidak menyerah ketika menghadapi berbagai kesulitan, dan tetap menjadi diri sendiri dalam setiap proses yang dilalui. Terima kasih telah bertahan hingga sampai di titik ini.

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES-128 UNTUK KEAMANAN DATA PELANGGAN PADA PROVIDER LAYANAN WIFI

Muhammad Andara Ghazy Ar Ramadhan, Ismail Abdurrozzaq Zulkarnain, Adi
Fajaryanto Cobantoro

Program Strata Satu (S1) Prodi Teknik Informatika, Fakultas Teknik, Universitas
Muhammadiyah Ponorogo

e_mail: andaraghazy@gmail.com

ABSTRAK

Perkembangan teknologi informasi mendorong penyedia layanan internet untuk mengelola data pelanggan secara digital, namun penyimpanan data pribadi seperti nama, nomor induk kependudukan, dan nomor telepon dalam basis data meningkatkan risiko akses tidak sah dan penyalahgunaan informasi. Penelitian ini bertujuan untuk mengimplementasikan algoritma *Advanced Encryption Standard (AES)*-128 dengan mode *Cipher Block Chaining* pada sistem pengelolaan data pelanggan provider layanan WiFi guna meningkatkan keamanan data yang disimpan. Penelitian menggunakan metode pengembangan Waterfall yang meliputi analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan. Sistem dikembangkan berbasis web menggunakan bahasa pemrograman PHP dan basis data *MySQL*. Proses enkripsi dilakukan sebelum data pelanggan disimpan ke dalam basis data, sedangkan proses dekripsi dilakukan ketika data akan ditampilkan kembali kepada pengguna yang memiliki hak akses. Pengujian sistem menggunakan *White Box Testing* dengan teknik *Path Testing* menunjukkan bahwa seluruh jalur independen pada modul login dan modul enkripsi berhasil dieksekusi sesuai dengan logika program. Selain itu, hasil implementasi membuktikan bahwa data pelanggan berhasil diubah menjadi bentuk *ciphertext* sehingga tidak dapat dibaca secara langsung di dalam basis data, kemudian dapat dikembalikan menjadi data asli melalui proses dekripsi menggunakan kunci yang sesuai. Berdasarkan hasil penelitian, implementasi algoritma *Advanced Encryption Standard (AES)*-128 mampu meningkatkan keamanan penyimpanan data pelanggan pada provider layanan WiFi.

Kata Kunci: AES-128, *Cipher Block Chaining*, keamanan data, kriptografi, provider layanan WiFi

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas segala rahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Kriptografi AES-128 Untuk Keamanan Data Pelanggan Pada Provider Layanan Wifi" dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Ponorogo.

Penulis menyadari bahwa penyusunan skripsi ini tidak terlepas dari bantuan, bimbingan, doa, serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Edy Kurniawan, S.T., M.T., selaku Dekan Fakultas Teknik, dan Bapak Adi Fajaryanto Cobantoro, S.Kom., M.Kom., selaku Ketua Program Studi Teknik Informatika, atas dukungan dan kemudahan administrasi yang diberikan.
2. Bapak Ismail Abdurrozzaq Zulkarnain, S.Kom, M.Kom., selaku Dosen Pembimbing Utama, dan Bapak Adi Fajaryanto Cobantoro, S.Kom, M.Kom., selaku Dosen Pembimbing Pendamping, yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan bimbingan, arahan, serta motivasi selama proses penyusunan skripsi ini.
3. Bapak Ir. Mohammad Bhanu Setyawan, S.T., M.Kom. dan Ibu Indah Puji Astuti, S.Kom, M.Kom., selaku Dosen Penguji, atas segala saran dan masukan yang membangun demi kesempurnaan skripsi ini.
4. Seluruh Bapak dan Ibu Dosen Program Studi Teknik Informatika Universitas Muhammadiyah Ponorogo yang telah memberikan bekal ilmu pengetahuan yang sangat bermanfaat.
5. Keluarga tercinta, Ayah dan Ibu, atas doa yang tak pernah putus, cinta, serta pengorbanan moril maupun materiil. Skripsi ini penulis persembahkan sebagai tanda bakti dan terima kasih.

6. Sahabat dan rekan-rekan seperjuangan angkatan 2022, terima kasih atas kebersamaan, semangat, dan dukungan yang telah dibagikan selama masa perkuliahan.
7. Semua pihak yang telah membantu yang tidak dapat penulis sebutkan satu per satu, terima kasih atas kontribusi yang telah diberikan.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan dan belum sempurna. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun dari berbagai pihak demi penyempurnaan karya ilmiah ini di masa mendatang. Penulis berharap skripsi ini dapat memberikan manfaat serta menjadi referensi bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan informasi dan kriptografi.

Ponorogo, 28 Juli 2026

Penulis



Muhammad Andara Ghazy Ar Ramadhan

DAFTAR ISI

HALAMAN PENGESAHAN.....	i
PERNYATAAN ORISINALITAS SKRIPSI.....	ii
HALAMAN BERITA ACARA UJIAN	iii
BERITA ACARA BIMBINGAN SKRIPSI	iv
MOTTO.....	x
HALAMAN PERSEMBAHAN	xi
ABSTRAK	xiii
KATA PENGANTAR.....	xiv
DAFTAR ISI	xvi
DAFTAR GAMBAR	xix
DAFTAR TABEL.....	xx
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan.....	4
1.4 Batasan Masalah.....	4
1.5 Manfaat	4
BAB II TINJAUAN PUSTAKA	6
2.1 Penelitian Terdahulu.....	6
2.2 Landasan Teori	10
2.2.1 Keamanan Data	10
2.2.2 Kriptografi.....	11
2.2.3 Advanced Encrypton Standard (AES)	12

2.2.4	Proses Enkripsi dan Dekripsi	14
2.2.5	<i>Website</i>	21
2.2.6	PHP	21
2.2.7	<i>Visual Studio Code</i>	22
2.2.8	<i>Database</i>	22
2.2.9	XAMPP	23
2.2.10	MYSQL	23
2.2.11	<i>Flowchart</i>	23
2.2.12	<i>Data Flow Diagram (DFD)</i>	25
2.2.13	<i>Use case diagram</i>	26
2.2.14	ERD	28
2.2.15	<i>Waterfall</i>	29
2.2.16	<i>White Box Testing</i>	30
BAB III METODOLOGI PENELITIAN		32
3.1	Tahapan Penelitian	32
3.2	Identifikasi Masalah	34
3.3	Studi Literatur	34
3.4	Pengumpulan Data	35
3.5	Analisis Kebutuhan	36
3.6	Perancangan Sistem	37
3.6.1	<i>Flowchart</i>	37
3.6.2	<i>Data Flow Diagram (DFD) Level 0</i>	39
3.6.3	<i>Data Flow Diagram (DFD) Level 1</i>	40
3.6.4	<i>Use case diagram</i>	43
3.6.5	ERD	44

3.6.6	Konsep User Interface.....	48
3.7	Implementasi Algoritma AES-128	50
3.8	Pengujian Sistem.....	51
3.9	Pemeliharaan	52
BAB IV HASIL DAN PEMBAHASAN.....		54
4.1	Implementasi Database	54
4.2	Implementasi Sistem	55
4.2.1	Menu Login.....	56
4.2.2	Menu Dashboard	56
4.2.3	Menu Data Pelanggan	57
4.2.4	Implementasi Algoritma AES-128	58
4.3	Pengujian Sistem (<i>White Box</i>).....	70
4.3.1	Pengujian Modul Login Admin.....	70
4.3.2	Pengujian Modul Enkripsi Data Pelanggan	74
4.3.3	Rekapitulasi Hasil Pengujian <i>White Box</i>	78
4.4	Pengujian Algoritma AES-128.....	81
BAB V KESIMPULAN DAN SARAN.....		84
5.1	Kesimpulan	84
5.2	Saran.....	84
DAFTAR PUSTAKA		86
LAMPIRAN.....		93

DAFTAR GAMBAR

Gambar 2. 1 Proses Kriptografi	12
Gambar 2. 2 Proses enkripsi pada Algoritma AES	15
Gambar 2. 3 Skema AddroundKey	16
Gambar 2. 4 Pengaruh Pemetaan pada setiap byte	17
Gambar 2. 5 Transformasi ShiftRows.....	17
Gambar 2. 6 Perkalian Matriks	18
Gambar 2. 7 Proses dekripsi pada Algoritma AES	19
Gambar 2. 8 Transformasi InvShiftRows.....	19
Gambar 2. 9 Perkalian matriks InvMixColumns	20
Gambar 2. 10 Metode Waterfall.....	29
Gambar 3. 1 Alur Pengembangan Sistem (Waterfall).....	32
Gambar 3. 2 Flowchart Algoritma AES-128.....	38
Gambar 3. 3 DFD Level 0.....	39
Gambar 3. 4 DFD Level 1.....	41
Gambar 3. 5 Use case diagram.....	43
Gambar 3. 6 Tabel Relasi	45
Gambar 3. 7 Entity Relationship Diagram.....	45
Gambar 3. 8 Menu Dashboard	49
Gambar 3. 9 Menu Data Pelanggan	50
Gambar 4. 1 Struktur Tabel Admin	54
Gambar 4. 2 Struktur Tabel Kunci	54
Gambar 4. 3 Struktur Tabel Pelanggan	55
Gambar 4. 4 Hasil Penyimpanan Data pada Database	55
Gambar 4. 5 Menu Login	56
Gambar 4. 6 Menu Dashboard	57
Gambar 4. 7 Menu Data Pelanggan	57
Gambar 4. 8 Flow Graph Modul Login	71
Gambar 4. 9 Flow Graph Modul Enkripsi Data Pelanggan	75
Gambar 4. 10 Pengujian AES-128 di website.....	82

DAFTAR TABEL

Tabel 2. 1 Penelitian terdahulu.....	6
Tabel 2. 2 Putaran Kunci AES.....	13
Tabel 2. 3 S-Box SubBytes	16
Tabel 2. 4 Invers S-box	20
Tabel 2. 5 Tabel Flowchart.....	24
Tabel 2. 6 Komponen DFD	26
Tabel 2. 7 Simbol-Simbol Use case diagram	27
Tabel 2. 8 Simbol-simbol ERD	28
Tabel 3. 1 ADMIN_OPERATOR.....	46
Tabel 3. 2 Tabel PELANGGAN.....	46
Tabel 3. 3 Tabel Kunci_AES.....	48
Tabel 3. 4 Tabel Path Testing	51
Tabel 4. 1 Plaintext.....	58
Tabel 4. 2 Secret Key	59
Tabel 4. 3 Initialization Vector (IV).....	59
Tabel 4. 4 Hasil XOR Plaintext dengan IV.....	60
Tabel 4. 5 Hasil AddroundKey Awal.....	60
Tabel 4. 6 Hasil SubBytes round 1	61
Tabel 4. 7 Hasil ShiftRows round 1	61
Tabel 4. 8 Hasil MixColumns round 1	62
Tabel 4. 9 Hasil AddroundKey round 1	62
Tabel 4. 10 Hasil round 2	63
Tabel 4. 11 Hasil round 3	63
Tabel 4. 12 Hasil Akhir Enkripsi.....	64
Tabel 4. 13 Padding Blok Kedua (PKCS#7).....	64
Tabel 4. 14 Hasil Enkripsi Padding Blok Kedua.....	65
Tabel 4. 15 Dekripsi: Ciphertext Blok Pertama	66
Tabel 4. 16 Dekripsi: Hasil AddroundKey Awal (round 10).....	66
Tabel 4. 17 Dekripsi: Hasil Inverse ShiftRows round 10.....	67

Tabel 4. 18 Dekripsi: Hasil Inverse SubBytes round 10	67
Tabel 4. 19 Dekripsi: Hasil AddroundKey round 10.....	67
Tabel 4. 20 Dekripsi: Hasil Inverse MixColumns round 10	68
Tabel 4. 21 Dekripsi: Hasil round 9 Dekripsi	68
Tabel 4. 22 Dekripsi: Hasil round 8 Dekripsi	69
Tabel 4. 23 Hasil Akhir Dekripsi.....	69
Tabel 4. 24 Hasil Pengujian White Box Modul Login.....	73
Tabel 4. 25 Hasil Pengujian White Box Modul Enkripsi Data Pelanggan.....	77
Tabel 4. 26 Rekapitulasi Hasil Pengujian White Box	78
Tabel 4. 27 Tabel Seluruh Hasil Pengujian Sistem	79

