SKRIPSI

MODIFIKASI S-BOX PADA ALGORITMA KRIPTOGRAFI AES MENGGUNAKAN POLINOMIAL IRREDUSIBEL ALTERNATIF ATAS LAPANGAN HINGGA GF(2^8)

HIZBULLAH NAJIHAN
22106010071

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA

2026

MODIFIKASI S-BOX PADA ALGORITMA KRIPTOGRAFI AES MENGGUNAKAN POLINOMIAL IRREDUSIBEL ALTERNATIF ATAS LAPANGAN HINGGA GF(2^8)

Skripsi

Untuk memenuhi sebagian persyaratan

mencapai derajat Sarjana S-1

Program Studi Matematika

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

diajukan oleh

HIZBULLAH NAJIHAN

22106010071

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2026

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Hizbullah Najihan
NIM : 22106010071
Judul Skripsi : Modifikasi S-Box pada Algoritma AES menggunakan Polinomial Irredusibel atas Lapangan Hingga GF(2^8)

sudah dapat diajukan kembali kepada Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Matematika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqasyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 4 Agustus 2026
Pembimbing

M. Zaki Riyanto, S.Si., M.Sc.
NIP. 19840113 201503 1 001

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-2002/Un.02/DST/PP.00.9/08/2026

Tugas Akhir dengan judul : Modifikasi S-Box pada Algoritma Kriptografi AES menggunakan Polinomial Irredusibel Alternatif atas Lapangan Hingga GF(2^8)

yang dipersiapkan dan disusun oleh:

Nama : HIZBULLAH NAJIHAN
Nomor Induk Mahasiswa : 22106010071
Telah diujikan pada : Rabu, 12 Agustus 2026
Nilai ujian Tugas Akhir : A

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Muhamad Zaki Riyanto, S.Si., M.Sc.
SIGNED

Valid ID: 6a87de20c4c0f

Penguji I

Arif Munandar, M.Sc.
SIGNED

Valid ID: 6a87cef0592dd

Penguji II

Aulia Khifah Futhona, M.Sc.
SIGNED

Valid ID: 6a87d97892c0d

Yogyakarta, 12 Agustus 2026
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 6a87fc271aa19

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

SURAT PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini:

Nama	: Hizbullah Najihan
NIM	: 22106010071
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi

Dengan ini menyatakan bahwa isi skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi dan sesungguhnya skripsi ini merupakan hasil pekerjaan penulis sendiri sepanjang pengetahuan penulis, bukan duplikasi atau saduran dari karya orang lain kecuali bagian tertentu yang penulis ambil sebagai bahan acuan. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab penulis.

Yogyakarta,



Hizbullah Najihan

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

HALAMAN PERSEMBAHAN

KARYA SEDERHANA INI PENULIS PERSEMBAHKAN UNTUK:

ORANG YANG BERKENAN MEMBACA TULISAN INI.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

MOTTO

Dalam lapangan semua elemen tak nol pasti memiliki elemen invers, begitupun dalam kehidupan (lapangan) semua yang terjadi (elemen tak nol) pasti ada alasan yang belum kita ketahui (elemen invers).

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

PRAKATA

Allhamdulillahirabbil'alamin, puji syukur kehadirat Allah SWT yang telah memberikan rahmat, nikmat, serta hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan skripsi dengan judul "Modifikasi S-Box pada Algoritma AES menggunakan Polinomial Irredusibel atas Lapangan Hingga GF(2^8)". Penulisan skripsi ini diselesaikan sebagai salah satu prasyarat mencapai gelar Sarjana Matematika.

Penulis menyadari bahwa penulisan skripsi ini terdapat banyak hambatan dan halangan. Namun berkat adanya motivasi, bantuan, bimbingan, dan dorongan dari berbagai pihak, alhamdulillah skripsi ini dapat terselesaikan. Oleh karena itu, dengan kerendahan hati penulis mengucapkan terima kasih kepada:

1. Prof. Noorhaidi, M.A., M.Phil., Ph.D., selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Prof. Dr. Dra. Hj. Khurul Wardati, M.Si., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
3. Dr. Epha Diana Supandi, S.Si., M.Sc., selaku Ketua Program Studi Matematika.
4. Deddy Rahmadi, M.Sc., selaku dosen pembimbing akademik yang telah memberikan pengarahan kepada penulis selama menempuh pendidikan.
5. Muhamad Zaki Riyanto, S.Si., M.Sc., selaku dosen pembimbing skripsi yang telah meluangkan waktu, tenaga, dan pikiran untuk membimbing penulis dalam penyusunan skripsi ini.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

6. Arif Munandar, M.Sc., selaku dosen penguji yang telah memberikan saran dan masukan yang berharga dalam penyempurnaan skripsi ini.

7. Seluruh dosen dan staf Fakultas Sains dan Teknologi yang telah memberikan ilmu bermanfaat dan memberikan pelayanan administrasi akademik.

8. Ibu dan Bapak dan kakak tercinta, orang yang sangat berjasa dalam hidup penulis. Terima kasih atas doa, cinta, kepercayaan, dan segala bentuk dukungan yang telah diberikan, sehingga penulis selalu merasa dikuatkan dalam setiap proses dan keputusan yang diambil.

9. Keluarga Matematika angkatan 2022 yang telah membersamai selama 4 tahun dibangku perkuliahan, saling mendukung, berbagi ilmu dan banyak kenangan manis yang selalu dikenang.

Penulis sangat menyadari tidak ada yang sempurna di dunia ini. Oleh karena itu segala bentuk saran, kritik atas skripsi ini penulis menerimanya dengan senang hati. Penulis berharap skripsi ini dapat memberikan manfaat khususnya bagi penulis dan semua kalangan yang membutuhkan untuk dijadikan referensi dalam menulis. Akhir kata semoga Allah SWT melimpahkan segala rahmat dan hidayah-Nya kepada kita semua, *Aamiin*.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Yogyakarta, 5 Agustus 2026

Hizbullah Najihan

DAFTAR ISI

HALAMAN JUDUL . . . . . **i**

HALAMAN PERSETUJUAN . . . . . **ii**

HALAMAN PENGESAHAN . . . . . **iii**

HALAMAN PERNYATAAN . . . . . **iv**

HALAMAN PERSEMBAHAN . . . . . **v**

HALAMAN MOTTO . . . . . **vi**

PRAKATA . . . . . **vii**

DAFTAR ISI . . . . . **ix**

DAFTAR TABEL . . . . . **xiii**

DAFTAR GAMBAR . . . . . **xv**

DAFTAR LAMBANG . . . . . **xvi**

INTISARI . . . . . **xvii**

ABSTRACT . . . . . **xviii**

I Pendahuluan **1**

1.1. Latar Belakang 1

1.2. Rumusan Masalah 5

1.3. Batasan Masalah 6

1.4. Tujuan Penelitian 6

1.5. Manfaat Penelitian 7

1.6. Tinjauan Pustaka 8

1.7. Metode Penelitian 12

1.8. Sistematika Penulisan 15

II LANDASAN TEORI **16**

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

2.1. Kriptografi dan *Block Cipher* 16
2.1.1. Kriptografi 16
2.1.2. Enkripsi dan Dekripsi 17
2.1.3. Kriptografi Simetris dan Asimetris 18
2.1.4. *Block Cipher* 19
2.2. Teori Bilangan 21
2.2.1. Keterbagian 21
2.2.2. Algoritma Pembagian 23
2.2.3. Faktor Persekutuan Terbesar (GCD) 24
2.2.4. Representasi Data: Bit, Byte, Heksadesimal, dan ASCII . . 27
2.3. Struktur Aljabar 32
2.3.1. Grup 32
2.3.2. Ring 35
2.3.3. Ring Komutatif 36
2.3.4. Ring Komutatif dengan Elemen Satuan 36
2.3.5. Ideal 36
2.3.6. Ring Faktor 37
2.3.7. Lapangan 39
2.4. Ring Polinomial 39
2.4.1. Ring Polinomial 39
2.4.2. Algoritma Euclid dan Pembagian Polinomial 54
2.4.3. Polinomial Irredusibel 55
2.4.4. Ring Faktor Polinomial 57
2.5. Lapangan Hingga 57
2.5.1. Lapangan Hingga 57
2.5.2. Pembentukan $GF(2^8)$ 61

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

2.6. *Advanced Encryption Standard* (AES) Standar 66
2.6.1. Sejarah AES 66
2.6.2. Struktur Arsitektur AES 67
2.6.3. Tahapan Putaran AES 68
2.6.4. *Key Expansion* 70
2.7. Pembentukan *S-Box* dan Transformasi *MixColumns* 71
2.7.1. Pembentukan S-Box AES 71
2.7.2. Transformasi MixColumns 74
2.8. Parameter Kriptografis Evaluasi S-Box 78
2.8.1. Nonlinearity (NL) 78
2.8.2. Algebraic Degree (AD) 80
2.8.3. Differential Uniformity (DU) 81
2.8.4. Strict Avalanche Criterion (SAC) 82
2.8.5. Ringkasan Parameter Kriptografis S-box 83
III PEMBAHASAN 85
3.1. Pengujian Polinomial Irredusibel dan Struktur Lapangan Hingga . . 85
3.1.1. Kriteria Keirredusibelan Polinomial Derajat 8 atas $\mathbb{Z}_2$ 86
3.1.2. Kandidat Polinomial Irredusibel Derajat 8 dari Literatur . . 87
3.1.3. Pengujian Keirredusibelan Polinomial $m(x)$ dan $f(x)$ . . . 89
3.2. Struktur Ring Faktor dan Pemetaan Isomorfisme 92
3.2.1. Konstruksi Lapangan Hingga dan Pemetaan Isomorfisme . . 93
3.2.2. Pembentukan S-Box Berbasis Invers Perkalian dan Transformasi Affine 93
3.2.3. Dampak Perubahan Polinomial terhadap Transformasi AES 97
3.3. Dampak Perubahan Polinomial terhadap Parameter Kriptografis S-Box 98

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

3.3.1. Nonlinieritas (NL) 98
3.3.2. Derajat Aljabar (AD) 99
3.3.3. Uniformitas Diferensial (DU) 99
3.3.4. Strict Avalanche Criterion (SAC) 99
3.3.5. Ringkasan Hasil Analisis dan Perbandingan 100
IV PENUTUP 101
4.1. Kesimpulan 101
4.2. Saran 102
DAFTAR PUSTAKA 104
LAMPIRAN 108
A Data Penelitian 108
1.1. Transparansi Proses Enkripsi AES Standar dan AES Modified . . . 108
1.1.1. Spesifikasi Pengujian 108
1.1.2. Perbandingan State per Ronde 109
1.1.3. Rekapitulasi Perbedaan per Ronde 112
1.1.4. Perbandingan Hasil Akhir 113
1.1.5. Analisis Transparansi Perubahan 114
1.1.6. Ringkasan Transparansi Perubahan 114
1.2. Implementasi membangun S-Box Modifikasi 115
1.2.1. Kode Program 115
1.2.2. Sumber Kode Program 123
B Biodata Penulis 124

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR TABEL

1.1 Matriks Perbandingan Tinjauan Pustaka 10

1.1 Matriks Perbandingan Tinjauan Pustaka 11

1.1 Matriks Perbandingan Tinjauan Pustaka 12

2.1 Perbandingan Kriptografi Simetris dan Asimetris 18

2.2 Satuan Data Digital 28

2.3 Konversi Desimal, Heksadesimal, dan Biner 29

2.4 Tabel ASCII Lengkap (0-127) 31

2.5 Operasi $\cdot$ untuk $(\mathbb{Z}_4, \cdot)$ 39

2.6 Representasi Elemen Lapangan $GF(2^3)$ 62

2.7 Implementasi Perkalian dalam $GF(2^8)$ untuk MixColumns 77

2.8 Ringkasan Parameter Kriptografis S-box 84

3.1 Daftar 30 Kandidat Polinomial Irredusibel Monik Derajat 8 atas $\mathbb{Z}_2$ Lidl & Niederreiter (1997) 88

3.1 Daftar 30 Kandidat Polinomial Irredusibel Monik Derajat 8 atas $\mathbb{Z}_2$ Lidl & Niederreiter (1997) 89

3.2 Tabel SubBytes (S-Box) pada Algoritma AES Standar 96

3.3 S-Box AES Modifikasi dengan $f(x) = x^8 + x^5 + x^3 + x^2 + 1$ . . . 96

3.4 Perbandingan Nilai Rcon AES Standar dan AES Modifikasi 98

3.5 Ringkasan Perbandingan Parameter Kriptografis S-Box 100

1.1 Spesifikasi Pengujian Enkripsi 108

1.2 Ronde 0: AddRoundKey 109

1.3 Ronde 1: Perbandingan State 109

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

1.4 Ronde 2: Perbandingan State 110
1.5 Ronde 3: Perbandingan State 110
1.6 Ronde 4: Perbandingan State 110
1.7 Ronde 5: Perbandingan State 111
1.8 Ronde 6: Perbandingan State 111
1.9 Ronde 7: Perbandingan State 111
1.10 Ronde 8: Perbandingan State 112
1.11 Ronde 9: Perbandingan State 112
1.12 Ronde 10: Ciphertext Akhir 112
1.13 Rekapitulasi Perbedaan State per Ronde 113
1.14 Perbandingan Hasil Akhir Enkripsi 113
1.15 Ringkasan Transparansi Perubahan AES 114

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR GAMBAR

1.1 Diagram alur penelitian. 14

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR LAMBANG

$m(x)$	= polinomial irredusibel standar AES
$f(x)$	= polinomial irredusibel alternatif pada AES Modifikasi
$GF(2^8)$	= lapangan hingga (*Galois Field*) dengan $2^8 = 256$ elemen
$\mathbb{Z}_2[x]$	= ring polinomial atas $\mathbb{Z}_2$ dengan variabel x
$\langle f(x) \rangle$	= ideal utama yang dibangkitkan oleh polinomial $f(x)$
$a(x), b(x)$	= elemen polinomial di $GF(2^8)$
$\oplus$	= operasi XOR (*exclusive-or*) pada $\mathbb{Z}_2$
$\gcd(f(x), g(x))$	= faktor persekutuan terbesar dari $f(x)$ dan $g(x)$
a^{-1}	= invers perkalian dari elemen a di $GF(2^8)$
$S(x)$	= fungsi S-Box, $S : \{0,1\}^8 \to \{0,1\}^8$
NL	= nonlinieritas S-Box (*nonlinearity*)
DU	= uniformitas diferensial S-Box (*differential uniformity*)
AD	= derajat aljabar S-Box (*algebraic degree*)
M	= matriks *MixColumns* berukuran 4×4
$\mathcal{B}$	= *branch number* dari transformasi *MixColumns*

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

INTISARI

Modifikasi S-Box pada Algoritma Kriptografi AES menggunakan Polinomial Irredusibel Alternatif atas Lapangan Hingga GF(2^8)

Hizbullah Najihan

22106010071

Penelitian ini membahas modifikasi struktur lapangan hingga $GF(2^8)$ pada algoritma *Advanced Encryption Standard* (AES) melalui penggantian polinomial irredusibel standar dengan polinomial irredusibel alternatif. Penelitian ini bertujuan untuk menganalisis metode penentuan polinomial irredusibel berderajat 8 atas $\mathbb{Z}_2$, mengkaji struktur aljabar pada lapangan hingga $GF(2^8)$ yang dibentuk oleh ring faktor $\mathbb{Z}_2[x]/\langle m(x)\rangle$ dan $\mathbb{Z}_2[x]/\langle f(x)\rangle$, serta menganalisis pengaruh perubahan polinomial irredusibel pembangun terhadap parameter metrik kriptografis S-Box. Metode penelitian yang digunakan adalah studi literatur dan analisis teoretis aljabar murni dengan pendekatan deduktif. Hasil penelitian menunjukkan bahwa polinomial irredusibel alternatif terbukti irredusibel atas $\mathbb{Z}_2$ dan membentuk ideal maksimal $\langle f(x)\rangle$, sehingga ring faktor $\mathbb{Z}_2[x]/\langle f(x)\rangle$ membentuk lapangan hingga $GF(2^8)$. Selain itu, terdapat pemetaan isomorfisme yang menunjukkan ekuivalensi struktur aljabar antara bentuk lapangan hingga $GF(2^8)$ yang diperoleh dari polinomial irredusibel standar dan polinomial irredusibel alternatif. S-Box yang dihasilkan memiliki parameter kriptografis $NL = 112$, $AD = 7$, $DU = 4$, serta memenuhi *Strict Avalanche Criterion* (SAC), yang setara dengan AES standar. Dengan demikian, penggantian polinomial irredusibel pada AES tidak menurunkan kualitas kriptografis algoritma dan membuka peluang pengembangan variasi struktur aljabar dalam desain kriptografi modern.

Kata Kunci: AES, Lapangan Hingga, Polinomial Irredusibel, S-Box, Kriptanalisis.

ABSTRACT

Modification of the AES Cryptographic Algorithm S-Box Using Alternative Irreducible Polynomials over the Finite Field GF(2^8)

Hizbullah Najihan

22106010071

This research investigates the modification of the finite field structure of $GF(2^8)$ in the *Advanced Encryption Standard* (AES) by replacing the standard irreducible polynomial with an alternative irreducible polynomial. The objectives of this research are to analyze the method for determining degree-8 irreducible polynomials over $\mathbb{Z}_2$, examine the algebraic structure of the finite field $GF(2^8)$ constructed from the quotient rings $\mathbb{Z}_2[x]/\langle m(x)\rangle$ and $\mathbb{Z}_2[x]/\langle f(x)\rangle$, and analyze the effect of changing the defining irreducible polynomial on the cryptographic metrics of the S-Box. This research employs a literature study and theoretical analysis in pure algebra using a deductive approach. The results demonstrate that the alternative irreducible polynomial is irreducible over $\mathbb{Z}_2$ and generates the maximal ideal $\langle f(x)\rangle$, so that the quotient ring $\mathbb{Z}_2[x]/\langle f(x)\rangle$ forms the finite field $GF(2^8)$. Furthermore, there exists an isomorphism establishing the algebraic equivalence between the constructions of $GF(2^8)$ obtained from the standard irreducible polynomial and the alternative irreducible polynomial. The resulting S-Box achieves cryptographic metrics of $NL = 112$, $AD = 7$, and $DU = 4$, while satisfying the *Strict Avalanche Criterion* (SAC), which are equivalent to those of the standard AES S-Box. Therefore, replacing the irreducible polynomial in AES does not degrade the cryptographic quality of the algorithm and provides opportunities for exploring alternative algebraic structures in modern cryptographic design.

Keywords: AES, Finite Field, Irreducible Polynomial, S-Box, Cryptanalysis.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

BAB I

Pendahuluan

1.1. Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah mengubah hampir seluruh aspek kehidupan manusia. Hampir setiap aktivitas sehari-hari, seperti berkomunikasi, bertransaksi, menyimpan data, hingga mengakses informasi, dilakukan melalui jaringan digital yang terbuka. Layanan-layanan seperti *WhatsApp*, *email*, *mobile banking*, *cloud storage*, dan *browser* HTTPS telah menjadi bagian tak terpisahkan dari kehidupan modern. Di balik kemudahan yang ditawarkan oleh layanan-layanan tersebut, terdapat satu elemen yang sangat krusial yaitu proses enkripsi. Setiap pesan yang dikirim, setiap transaksi yang dilakukan, dan setiap koneksi yang dibuka pada dasarnya dilindungi oleh mekanisme enkripsi untuk mencegah pihak yang tidak berwenang mengakses informasi yang bersifat pribadi dan rahasia Stallings (2017); Katz & Lindell (2021).

Keamanan informasi menjadi salah satu isu yang paling krusial di era digital. Data yang dikirimkan melalui jaringan publik sangat rentan terhadap berbagai bentuk ancaman, seperti penyadapan, perusakan, pemalsuan, hingga pencurian identitas. Oleh karena itu, diperlukan suatu mekanisme yang mampu melindungi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan keaslian (*authentication*) data selama proses transmisi maupun penyimpanan Menezes et al. (1996); Stallings (2017). Mekanisme tersebut dikenal dengan istilah kriptografi.

Kriptografi merupakan ilmu yang mempelajari teknik-teknik untuk menja-

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

ga keamanan informasi melalui proses pengubahan pesan asli menjadi bentuk yang tidak dapat dipahami oleh pihak yang tidak berwenang Stallings (2017); Katz & Lindell (2021). Secara etimologis, istilah kriptografi berasal dari bahasa Yunani, yaitu *kryptos* yang berarti rahasia dan *graphia* yang berarti tulisan Menezes et al. (1996). Dalam praktiknya, kriptografi melibatkan dua proses utama, yaitu enkripsi yang mengubah pesan asli (*plaintext*) menjadi pesan tersandi (*ciphertext*), dan dekripsi yang mengembalikan *ciphertext* menjadi *plaintext* semula.

Perkembangan teknologi komputer pada abad ke-20 melahirkan kriptografi modern yang sangat berbeda dengan pendahulunya. Kriptografi modern tidak lagi bergantung pada kerahasiaan algoritma, melainkan pada kerahasiaan kunci (*key*), sesuai dengan prinsip yang dikenal sebagai *Kerckhoffs's principle* Menezes et al. (1996); Paar & Pelzl (2010). Dalam kriptografi modern, algoritma *block cipher* menjadi fondasi bagi sebagian besar sistem keamanan digital saat ini Paar & Pelzl (2010); Stallings (2017). Salah satu algoritma *block cipher* yang paling terkenal dan banyak digunakan adalah *Advanced Encryption Standard* (AES) yang ditetapkan oleh *National Institute of Standards and Technology* (NIST) pada tahun 2001 NIST (2001); Daemen & Rijmen (2002). AES dirancang untuk menggantikan *Data Encryption Standard* (DES) yang dianggap tidak lagi aman karena panjang kunci yang relatif pendek Stallings (2017); Paar & Pelzl (2010).

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Keunggulan utama AES tidak hanya terletak pada desain algoritmanya, tetapi juga pada fondasi matematis yang kuat di baliknya. Berbeda dengan algoritma klasik yang sebagian besar bergantung pada manipulasi karakter, AES dibangun di atas struktur matematika yang lebih formal dan terdefinisi dengan baik, yaitu teori grup, ring, dan lapangan hingga Daemen & Rijmen (2002); Murphy & Robshaw (2002). Seluruh operasi aritmetika dalam AES didefinisikan pada lapangan hingga

$GF(2^8)$ yang dibentuk dari ring polinomial $\mathbb{Z}_2[x]$ dengan modulo polinomial irredusibel standar $m(x) = x^8 + x^4 + x^3 + x + 1$ NIST (2001); Lidl & Niederreiter (1997). Polinomial irredusibel ini memastikan bahwa setiap elemen tak nol dalam lapangan memiliki invers perkalian, yang merupakan prasyarat untuk membentuk fungsi substitusi yang bersifat bijektif dan non-linear Daemen & Rijmen (2002); Nyberg (1993).

Salah satu komponen terpenting dalam AES adalah *Substitution-box* (S-Box), yaitu tabel substitusi 16×16 yang bertanggung jawab terhadap aspek non-linearitas pada sistem kriptografi. S-Box AES dibangun melalui dua tahapan transformasi, yaitu invers perkalian setiap elemen pada $GF(2^8)$ dilanjutkan dengan transformasi affine NIST (2001); Daemen & Rijmen (2002). Parameter kriptografis S-Box, seperti *nonlinearity* (NL), *algebraic degree* (AD), *differential uniformity* (DU), dan *strict avalanche criterion* (SAC), menjadi tolok ukur kuantitatif untuk mengukur ketahanan S-Box terhadap berbagai jenis serangan kriptanalisis Nyberg (1993); Mohamed et al. (2014); Heys (2002). S-Box AES standar memiliki NL $\geq$ 112, AD $=$ 7, DU $=$ 4, serta memenuhi SAC dengan baik, yang menjadikannya sangat tahan terhadap serangan linear, diferensial, maupun aljabar Daemen & Rijmen (2002); Stallings (2017).

Meskipun AES telah terbukti aman dan efisien sebagai standar enkripsi global, struktur internalnya masih menyisakan ruang untuk dikaji lebih lanjut, khususnya pada aspek pembentukan lapangan hingga yang digunakan dalam operasi aritmetika. Sebagian besar implementasi AES menggunakan polinomial irredusibel standar $m(x) = x^8 + x^4 + x^3 + x + 1$ yang telah ditetapkan dalam FIPS-197 NIST (2001). Namun, berdasarkan teori lapangan hingga, terdapat 30 kandidat polinomial irredusibel monik berderajat 8 atas $\mathbb{Z}_2$ yang telah diklasifikasikan dalam

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

literatur aljabar dan masing-masing dapat digunakan untuk membentuk lapangan hingga $GF(2^8)$ Lidl & Niederreiter (1997). Kajian mengenai penggunaan polinomial irredusibel alternatif dalam AES masih relatif terbatas, meskipun beberapa penelitian seperti Farwa et al. (2016) dan Hussain et al. (2011) telah menunjukkan bahwa variasi polinomial irredusibel dapat menghasilkan S-Box dengan sifat kriptografis yang kompetitif.

Berdasarkan uraian di atas, penelitian ini dilakukan untuk mengkaji secara teoritis pengaruh perubahan polinomial irredusibel terhadap struktur lapangan hingga $GF(2^8)$ dan implikasinya terhadap sifat kriptografis S-Box AES. Penelitian ini memilih salah satu kandidat dari literatur, yaitu $f(x) = x^8 + x^5 + x^3 + x^2 + 1$, untuk diuji keirredusibelannya dan dibandingkan dengan polinomial standar $m(x)$. Perubahan polinomial irredusibel akan mempengaruhi operasi invers perkalian di dalam lapangan, yang merupakan komponen fundamental dalam pembentukan S-Box pada transformasi SubBytes Daemen & Rijmen (2002); Nyberg (1993). Analisis difokuskan pada parameter-parameter kriptografis seperti nonlinieritas, derajat aljabar, uniformitas diferensial, dan kriteria avalanche ketat, yang merupakan tolok ukur keamanan S-Box terhadap berbagai serangan kriptanalisis Mohamed et al. (2014); Heys (2002).

Penelitian ini diharapkan dapat memberikan kontribusi dalam dua aspek utama. Secara teoritis, penelitian ini memperkaya pemahaman tentang aplikasi teori aljabar abstrak, khususnya teori ring, ideal, ring polinomial, dan lapangan hingga, dalam sistem kriptografi modern. Secara praktis, penelitian ini menyajikan kajian teoritis mengenai alternatif struktur matematis pada pengembangan algoritma enkripsi berbasis *block cipher*, khususnya dalam pemilihan polinomial irredusibel yang dapat mempengaruhi sifat kriptografis S-Box.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

1.2. Rumusan Masalah

Konstruksi algoritma *Advanced Encryption Standard* (AES) bertumpu pada struktur aljabar lapangan hingga $GF(2^8)$ yang dibangun melalui ring faktor $\mathbb{Z}_2[x]/\langle p(x)\rangle$, di mana $p(x)$ merupakan polinomial monik irredusibel berderajat 8. Berdasarkan teori lapangan hingga, terdapat 30 kandidat polinomial irredusibel monik berderajat 8 atas $\mathbb{Z}_2$ yang telah diklasifikasikan dalam literatur. Standar FIPS-197 menetapkan polinomial $m(x) = x^8 + x^4 + x^3 + x + 1$ sebagai modulus pembangun $GF(2^8)$. Untuk menganalisis fleksibilitas struktur aljabar serta implikasinya terhadap keamanan algoritma, penelitian ini memilih salah satu kandidat alternatif dari daftar literatur tersebut, yaitu $f(x) = x^8 + x^5 + x^3 + x^2 + 1$.

Sebelum digunakan untuk membangun lapangan hingga dan menganalisis S-Box yang dihasilkan, keirredusibelan polinomial alternatif tersebut perlu diuji secara ketat berdasarkan landasan teori ring dan keterbagian polinomial. Berdasarkan uraian alur tersebut, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana prosedur pengujian keirredusibelan polinomial alternatif $f(x) = x^8 + x^5 + x^3 + x^2 + 1$ yang dipilih dari 30 kandidat polinomial berderajat 8 pada ring $\mathbb{Z}_2[x]$ berdasarkan kriteria keterbagian faktor polinomial nontrivial?
2. Bagaimana lapangan hingga $GF(2^8)$ dibangun melalui ring faktor $\mathbb{Z}_2[x]/\langle m(x)\rangle$ dan $\mathbb{Z}_2[x]/\langle f(x)\rangle$, serta bagaimana pemetaan isomorfisme antar kedua lapangan hingga tersebut?
3. Bagaimana dampak penggantian polinomial irredusibel dari $m(x)$ menjadi $f(x)$ terhadap parameter metrik kriptografis S-Box yang meliputi *nonlinearity* (NL), *algebraic degree* (AD), *differential uniformity* (DU), dan *strict avalanche criterion* (SAC)?

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

1.3. Batasan Masalah

Untuk menjaga fokus dan kedalaman pembahasan, penelitian ini dibatasi pada hal-hal berikut:

1. Analisis difokuskan pada AES dengan ukuran blok 128 bit dan panjang kunci 128 bit (AES-128) sesuai dengan spesifikasi FIPS-197.

2. Penelitian ini mengkaji dua polinomial irredusibel berderajat 8 atas $\mathbb{Z}_2$, yaitu polinomial standar $m(x) = x^8 + x^4 + x^3 + x + 1$ sebagaimana ditetapkan dalam AES dan polinomial alternatif $f(x) = x^8 + x^5 + x^3 + x^2 + 1$ yang dipilih dari 30 kandidat literatur.

3. Penelitian difokuskan pada analisis struktur aljabar pembangun dan sifat kriptografis S-Box yang meliputi *nonlinearity*, *algebraic degree*, *differential uniformity*, dan *strict avalanche criterion*.

4. Penelitian tidak membahas aspek implementasi komputasional pada perangkat keras/lunak, optimasi kecepatan eksekusi, maupun analisis serangan kanal samping (*side-channel attacks*).

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, tujuan dari penelitian ini adalah untuk:

1. Menguji keirredusibelan polinomial alternatif $f(x) = x^8 + x^5 + x^3 + x^2 + 1$ yang dipilih dari 30 kandidat polinomial berderajat 8 pada ring $\mathbb{Z}_2[x]$ berdasarkan kriteria keterbagian faktor polinomial nontrivial.

2. Mengonstruksi lapangan hingga $GF(2^8)$ melalui ring faktor $\mathbb{Z}_2[x]/\langle m(x)\rangle$ dan $\mathbb{Z}_2[x]/\langle f(x)\rangle$, serta menentukan pemetaan isomorfisme antar kedua lapangan tersebut.

3. Menganalisis dampak penggantian polinomial irredusibel dari $m(x) = x^8 + x^4 + x^3 + x + 1$ menjadi $f(x) = x^8 + x^5 + x^3 + x^2 + 1$ terhadap parameter metrik kriptografis S-Box yang meliputi *nonlinearity* (NL), *algebraic degree* (AD), *differential uniformity* (DU), dan *strict avalanche criterion* (SAC).

1.5. Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. **Manfaat Teoritis**

   Memberikan pemahaman yang lebih mendalam tentang penerapan teori aljabar abstrak, khususnya teori ring, ideal, ring polinomial, dan lapangan hingga, dalam sistem kriptografi modern khususnya algoritma AES. Penelitian ini juga memperkaya kajian tentang struktur aljabar yang mendasari pembentukan S-Box dan transformasi kriptografis lainnya.

2. **Manfaat Praktis**

   Menyajikan kajian teoritis mengenai alternatif struktur matematis pada pengembangan algoritma enkripsi berbasis *block cipher*, khususnya dalam pemilihan polinomial irredusibel yang dapat mempengaruhi sifat kriptografis S-Box. Hasil penelitian ini dapat menjadi referensi bagi pengembangan varian AES dengan sifat kriptografis yang berbeda.

3. **Manfaat Akademis**

   Menjadi dasar bagi penelitian lanjutan terkait desain fungsi substitusi dan

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

transformasi linear pada cipher blok berbasis teori aljabar, serta membuka peluang untuk eksplorasi kandidat polinomial irredusibel lainnya dalam pembentukan lapangan hingga.

1.6. Tinjauan Pustaka

Penelitian mengenai struktur aljabar AES telah dilakukan oleh Daemen dan Rijmen (2002) dalam buku *The Design of Rijndael* yang memaparkan secara lengkap struktur matematis yang mendasari algoritma AES, termasuk pembentukan lapangan hingga $GF(2^8)$ dari ring polinomial $\mathbb{Z}_2[x]$ dengan modulo polinomial irredusibel $m(x) = x^8 + x^4 + x^3 + x + 1$ Daemen & Rijmen (2002). Murphy dan Robshaw (2002) dalam penelitiannya mengungkapkan bahwa AES memiliki struktur aljabar yang lebih kaya dari yang terlihat, yang mengindikasikan adanya hubungan erat antara struktur lapangan dan keamanan kriptografis AES Murphy & Robshaw (2002). Lidl dan Niederreiter (1997) dalam buku *Finite Fields* memberikan fondasi teoritis tentang lapangan hingga dan polinomial irredusibel, serta menyajikan bahwa terdapat 30 polinomial irredusibel monik berderajat 8 atas $\mathbb{Z}_2$ yang dapat digunakan untuk membentuk $GF(2^8)$ Lidl & Niederreiter (1997).

Penelitian tentang membangun S-Box dengan polinomial irredusibel alternatif telah dilakukan oleh beberapa peneliti. Farwa et al. (2016) mengusulkan pembentukan S-Box menggunakan transformasi fraksional linear pada $GF(2^8)$ dengan polinomial irredusibel $x^8 + x^6 + x^5 + x^4 + 1$, menghasilkan S-Box dengan nilai nonlinieritas 106 dan uniformitas diferensial 8 Farwa et al. (2016). Hussain et al. (2011) membangun S-Box menggunakan transformasi fraksional linear dengan parameter tertentu dan menunjukkan bahwa pemilihan parameter mempengaruhi karakteristik kriptografis S-Box yang dihasilkan Hussain et al. (2011). Cui dan Cao (2007) mengembangkan struktur S-Box bernama APA (*Affine-Power-Affine*) yang

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

bertujuan meningkatkan kompleksitas ekspresi aljabar AES S-Box dengan mempertahankan nilai nonlinieritas 112 dan uniformitas diferensial 4 Cui & Cao (2007). Isa et al. (2015) membangun S-Box dari fungsi pangkat dan binomial dengan manipulasi penjumlahan dan perkalian, menghasilkan S-Box dengan nilai nonlinieritas 108 dan uniformitas diferensial 4 Isa & Kilic (2015).

Penelitian tentang karakteristik kriptografis S-Box juga telah banyak dilakukan. Nyberg (1993) membahas teori pembentukan permutasi non-linear yang digunakan sebagai S-Box dan menjadi rujukan utama dalam memahami konsep nonlinieritas untuk ketahanan terhadap kriptanalisis linear Nyberg (1993). Mohamed et al. (2014) mengidentifikasi properti-properti yang harus dimiliki oleh S-Box yang kuat secara kriptografis, meliputi nonlinieritas tinggi ($100 < NL \leq 120$), uniformitas diferensial rendah ($2 \leq DU \leq 6$), derajat aljabar tinggi ($AD \geq 4$), serta kriteria avalanche ketat Mohamed et al. (2014). Heys (2002) memberikan penjelasan komprehensif tentang kriptanalisis linear dan diferensial serta bagaimana S-Box yang baik harus mampu menahan kedua jenis serangan tersebut Heys (2002). Mar dan Latt (2008) mengembangkan metode analisis kriteria avalanche ketat yang meliputi efek avalanche, kelengkapan, dan S-Box kuat Mar & Latt (2008). Webster dan Tavares (1986) memperkenalkan kriteria avalanche ketat dan *bit independence criterion* sebagai tolok ukur kualitas S-Box Webster & Tavares (1986). Shannon (1949) dalam teori fundamental kriptografi memperkenalkan konsep difusi dan konfusi yang menjadi dasar desain S-Box modern Shannon (1949).

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Tabel 1.1 Matriks Perbandingan Tinjauan Pustaka

No.	Nama Peneliti	Judul Penelitian	Persamaan	Perbedaan
1.	Daemen dan Rijmen (2002) Daemen & Rijmen (2002)	The Design of Rijndael: AES - The Advanced Encryption Standard	Menggunakan struktur lapangan hingga $GF(2^8)$ yang dibangun atas ring polinomial $\mathbb{Z}_2[x]$.	Menggunakan polinomial irredusibel standar $m(x) = x^8+x^4+x^3+x+1$.
2.	Murphy dan Robshaw (2002) Murphy & Robshaw (2002)	Essential algebraic structure within the AES	Mengkaji struktur aljabar intrinsik dan dampaknya terhadap aspek keamanan algoritma cipher blok AES.	Berfokus pada evaluasi teoritis arsitektur komponen standar cipher AES tanpa memodifikasi komponen pembangunnya.
3.	Lidl dan Niederreiter (1997) Lidl & Niederreiter (1997)	Finite Fields	Menyediakan fondasi teoretis aljabar abstrak mengenai lapangan hingga dan kuantitas polinomial irredusibel.	Kajian bersifat teks teori umum dan komprehensif, tidak spesifik pada pembentukan metrik kriptografis S-Box.

STATE ISLAMIC UNIVERSITY SUNAN KALIJAGA YOGYAKARTA

Tabel 1.1 Matriks Perbandingan Tinjauan Pustaka

No.	Nama Peneliti	Judul Penelitian	Persamaan	Perbedaan
4.	Farwa et al. (2016) Farwa et al. (2016)	An efficient construction of substitution box using linear fractional transformation	Menganalisis variasi polinomial irredusibel alternatif berderajat 8 atas $\mathbb{Z}_2$ dalam pembentukan komponen S-Box.	Menggunakan polinomial $x^8+x^6+x^5+x^4+1$ dan menggunakan metode transformasi fraksional linear.
5.	Hussain et al. (2011) Hussain et al. (2011)	A novel approach for designing substitution-boxes based on linear fractional transformation	Meneliti pengaruh parameter pembangun terhadap karakteristik metrik kriptografis S-Box yang dihasilkan.	Membangun fungsi pemetaan nonlinear didasarkan pada variasi parameter transformasi fraksional linear, bukan perubahan basis ring polinomial.
6.	Cui dan Cao (2007) Cui & Cao (2007)	A new S-box structure named APA	Menganalisis parameter nonlinearitas dan uniformitas diferensial pada fungsi permutasi komponen substitusi.	Menggunakan struktur komponen *Affine-Power-Affine* (APA) untuk meningkatkan kompleksitas ekspresi aljabar S-Box.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Tabel 1.1 Matriks Perbandingan Tinjauan Pustaka

No.	Nama Peneliti	Judul Penelitian	Persamaan	Perbedaan
7.	Isa et al. (2015) Isa & Kilic (2015)	Constructing secure S-box based on power function and binomial operation	Menganalisis ketahanan S-Box berdasarkan parameter metrik nonlinearitas tinggi dan nilai uniformitas diferensial rendah.	Mengonstruksi pemetaan S-Box menggunakan fungsi pangkat dan operasi binomial melalui manipulasi penjumlahan serta perkalian.

1.7. Metode Penelitian

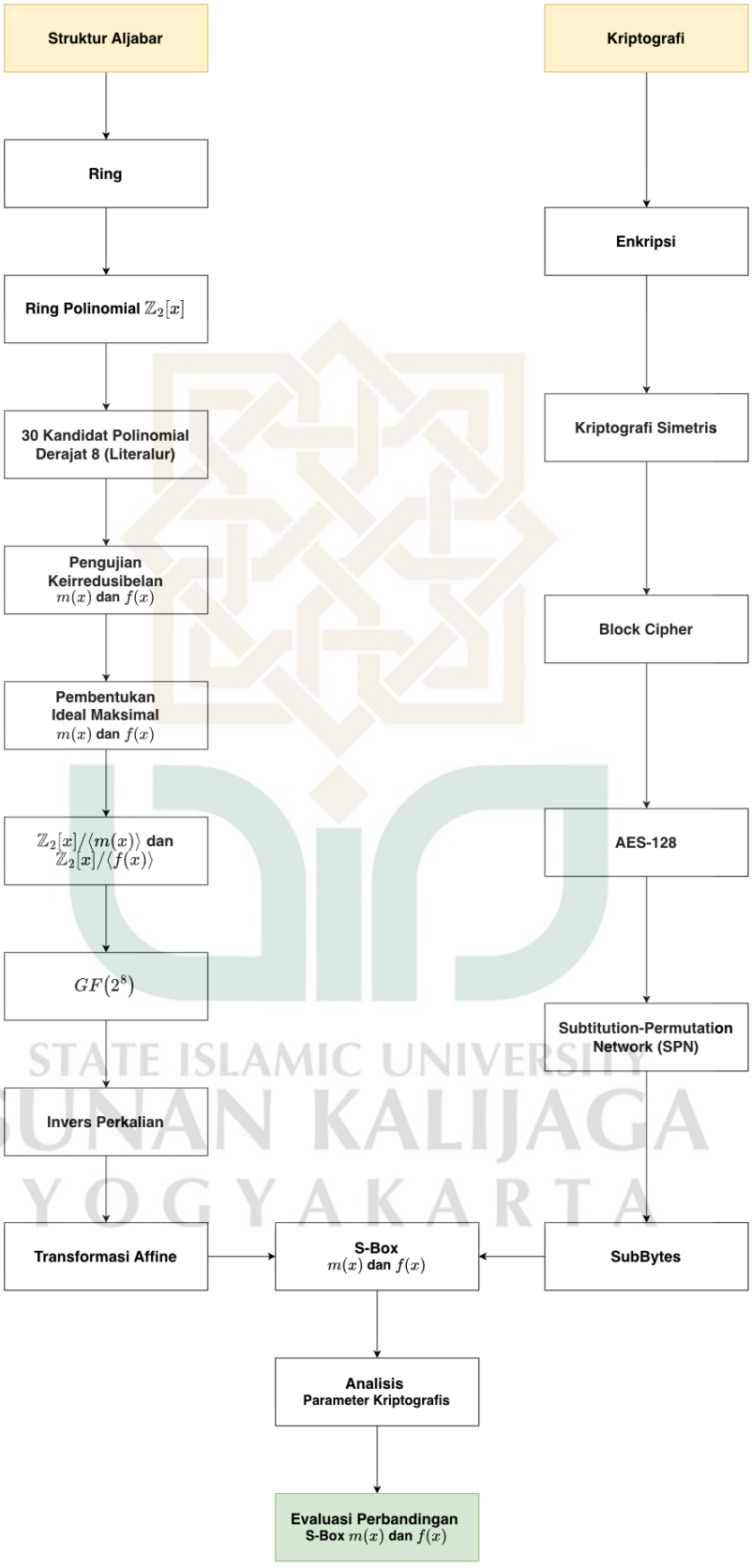
Penelitian ini merupakan studi teoretis berbasis aljabar abstrak dan kriptografi simetris yang dilaksanakan secara sistematis melalui pendekatan deduktif-analitis. Alur penelitian mengikuti struktur hierarkis dari konsep dasar teori ring hingga analisis keamanan S-Box. Tahapan awal penelitian dimulai dengan studi literatur untuk membangun landasan teoretis, yang mencakup tiga aspek utama: struktur aljabar abstrak (grup, ring, ideal, ring polinomial $\mathbb{Z}_2[x]$, dan lapangan hingga $GF(2^8)$) Dummit & Foote (2004); Fraleigh (2003); Lidl & Niederreiter (1997); arsitektur AES-128 khususnya transformasi *SubBytes* berbasis struktur SPN NIST (2001); Daemen & Rijmen (2002); serta parameter metrik keamanan S-Box (*nonlinearity*, *algebraic degree*, *differential uniformity*, dan *strict avalanche criterion*) Nyberg (1993); Mohamed et al. (2014); Heys (2002); Mar & Latt (2008).

Tahap selanjutnya adalah pengujian aljabar terhadap dua polinomial yang di-

pilih dari 30 kandidat literatur, yaitu polinomial standar $m(x) = x^8+x^4+x^3+x+1$ dan polinomial alternatif $f(x) = x^8 + x^5 + x^3 + x^2 + 1$. Pengujian keirredusibelan dilakukan melalui eliminasi faktor pembagi berderajat $1 \leq d \leq 4$. Karena $m(x)$ dan $f(x)$ terbukti irredusibel pada $\mathbb{Z}_2[x]$, maka ideal utama $\langle m(x) \rangle$ dan $\langle f(x) \rangle$ merupakan ideal maksimal, sehingga ring faktor yang terbentuk merupakan lapangan hingga, yaitu $GF_m(2^8) = \mathbb{Z}_2[x]/\langle m(x) \rangle$ dan $GF_f(2^8) = \mathbb{Z}_2[x]/\langle f(x) \rangle$. Selanjutnya, dirumuskan pemetaan isomorfisme $\phi : GF_m(2^8) \rightarrow GF_f(2^8)$ untuk memetakan representasi elemen antar kedua lapangan. Dari masing-masing lapangan tersebut, dikonstruksi dua tabel S-Box (S_m dan S_f) melalui penentuan invers perkalian elemen tak nol yang dilanjutkan dengan transformasi affine standar AES.

Tahap inti penelitian adalah melakukan evaluasi matematis terhadap S_m dan S_f berdasarkan empat parameter kriptografis: *nonlinearity* (NL) melalui transformasi Walsh-Hadamard, *algebraic degree* (AD) melalui representasi bentuk normal aljabar (ANF), *differential uniformity* (DU) melalui tabel distribusi diferensial (DDT), dan *strict avalanche criterion* (SAC) melalui matriks ketergantungan bit. Hasil pengujian dari kedua S-Box dibandingkan secara komparatif untuk menarik kesimpulan mengenai pengaruh penggantian polinomial irredusibel terhadap ketahanan kriptografis S-Box yang dihasilkan. Keseluruhan alur penelitian ini dirangkum dalam diagram alur pada Gambar 1.1.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA



Gambar 1.1 Diagram alur penelitian.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

1.8. Sistematika Penulisan

Bab I: Pendahuluan

Berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, tinjauan pustaka, metode penelitian, dan sistematika penulisan.

Bab II: Landasan Teori

Berisi landasan teori yang menunjang penelitian, meliputi konsep kriptografi simetris, struktur aljabar (grup, ring, ideal, ring polinomial $\mathbb{Z}_2[x]$), kriteria polinomial irredusibel, struktur lapangan hingga $GF(2^8)$, arsitektur algoritma AES-128, mekanisme pembentukan S-Box, serta definisi formal metrik parameter kriptografis.

Bab III: Pembahasan

Berisi pengujian keirredusibelan polinomial standar $m(x)$ dan alternatif $f(x)$ dari 30 kandidat literatur, konstruksi lapangan hingga $GF(2^8)$ melalui ring faktor beserta pemetaan isomorfismenya, pembentukan tabel S-Box termodifikasi, serta analisis komparatif parameter metrik kriptografis S-Box (S_m dan S_f).

Bab IV: Penutup

Berisi kesimpulan hasil penelitian terkait pembuktian struktur aljabar dan perbandingan sifat kriptografis S-Box, serta saran untuk pengembangan penelitian lanjutan.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

BAB IV

PENUTUP

4.1. Kesimpulan

Berdasarkan hasil analisis struktur aljabar dan evaluasi metrik kriptografis modifikasi struktur lapangan hingga $GF(2^8)$ pada algoritma *Advanced Encryption Standard* (AES) dengan polinomial alternatif $f(x) = x^8 + x^5 + x^3 + x^2 + 1$, dapat ditarik kesimpulan sebagai berikut:

1. **Pengujian Keirredusibelan Polinomial**

   Polinomial alternatif $f(x) = x^8 + x^5 + x^3 + x^2 + 1$ yang dipilih dari 30 kandidat literatur terbukti irredusibel pada ring $\mathbb{Z}_2[x]$. Pengujian keterbagian membuktikan bahwa $f(x)$ tidak memiliki faktor pembagi nontrivial berderajat $1 \leq d \leq 4$. Akibatnya, ideal utama $\langle f(x) \rangle$ merupakan ideal maksimal, yang menjamin bahwa ring faktor $\mathbb{Z}_2[x]/\langle f(x) \rangle$ membentuk lapangan hingga $GF(2^8)$ dimana setiap elemen tak nol memiliki invers perkalian yang unik.

2. **Struktur Lapangan Hingga dan Isomorfisme**

   Ring faktor $\mathbb{Z}_2[x]/\langle m(x) \rangle$ dan $\mathbb{Z}_2[x]/\langle f(x) \rangle$ membentuk lapangan hingga $GF(2^8)$ yang secara aljabar bersifat isomorfik melalui pemetaan $\phi : GF_m(2^8) \rightarrow GF_f(2^8)$. Meskipun isomorfik, representasi bit dan tabel perkalian aritmetikanya berbeda. Perbedaan ini mengubah nilai invers perkalian seluruh elemen tak nol, yang secara langsung menghasilkan tabel S-Box baru (S_f) pada transformasi *SubBytes* serta memodifikasi konstanta putaran (*Rcon*) pada *Key Expansion*.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

3. **Dampak terhadap Parameter Kriptografis S-Box**

   Penggantian polinomial irredusibel dari $m(x)$ ke $f(x)$ menghasilkan tabel substitusi baru (S_f) yang tetap mempertahankan parameter keamanan optimal yang identik dengan AES standar, yaitu Nonlinieritas ($NL = 112$), Derajat Aljabar ($AD = 7$), Uniformitas Diferensial ($DU = 4$), dan memenuhi *Strict Avalanche Criterion* (SAC). Hal ini membuktikan bahwa variasi polinomial pembangun lapangan hingga $GF(2^8)$ mampu memberikan diversifikasi struktur aljabar tanpa mendegradasi tingkat keamanan kriptografis AES terhadap serangan linear, diferensial, maupun aljabar.

4.2. Saran

Berdasarkan hasil penelitian ini, beberapa saran yang dapat diajukan untuk penelitian selanjutnya adalah:

1. **Eksplorasi Seluruh Kandidat Polinomial**

   Penelitian selanjutnya dapat memperluas analisis komparatif ke seluruh 30 kandidat polinomial irredusibel berderajat 8 atas $\mathbb{Z}_2$ guna memetakan karakteristik struktur aljabar secara menyeluruh pada algoritma blok cipher.

2. **Kajian Representasi Isomorfisme pada Transformasi Linear**

   Pengaruh pemetaan isomorfisme terhadap efisiensi komputasi matriks pada transformasi *MixColumns* dapat dikaji lebih mendalam, khususnya terkait representasi biner dan optimasi implementasi perangkat keras.

3. **Pengujian Terhadap Kriptanalisis Lanjutan dan Analisis Kanal Samping**

   Perlu dilakukan pengujian ketahanan varian AES modifikasi terhadap teknik kriptanalisis lanjut (seperti *integral cryptanalysis* dan *boomerang attack*)

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

serta analisis kebocoran informasi melalui serangan kanal samping (*side-channel attacks*).

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

DAFTAR PUSTAKA

Biham, E. & Shamir, A. (1991). Differential cryptanalysis of des-like cryptosystems. In *Advances in Cryptology—CRYPTO 1990*, pages 2–21. Springer.

Carlet, C. (2010). Boolean functions for cryptography and error correcting codes. In Crama, Y. & Hammer, P. L., editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 257–397. Cambridge University Press, Cambridge, DOI: 10.1017/CBO9780511780448.011.

Cui, L. & Cao, Y. (2007). A new s-box structure named apa. *IEEE Signal Processing Letters*, 14(12):1004–1007.

Daemen, J. & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer.

Dummit, D. S. & Foote, R. M. (2004). *Abstract Algebra*. John Wiley & Sons, 3 edition.

Farwa, S., Shah, T., & Khan, M. A. (2016). An efficient construction of substitution box using linear fractional transformation. *3D Research*, 7(3):23.

Fraleigh, J. B. (1999). *A First Course in Abstract Algebra*. Addison-Wesley, Reading, Mass., 6th edition.

Fraleigh, J. B. (2003). *A First Course in Abstract Algebra*. Addison-Wesley, 7 edition.

Gilbert, J. & Gilbert, L. (2005). *Elements of Modern Algebra*. Thomson Brooks/Cole, Belmont, CA, 6th edition, ISBN: 978-0534402648.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3):189–221.

Hussain, I., Shah, T., & Mahmood, H. (2011). A novel approach for designing substitution-boxes based on linear fractional transformation. *Scientia Iranica*, 18(3):715–718.

Isa, M. A. & Kilic, R. (2015). Constructing secure s-box based on power function and binomial operation. *Sadhana*, 40(7):2029–2043.

Katz, J. & Lindell, Y. (2021). *Introduction to Modern Cryptography*. CRC Press, 3 edition.

Knudsen, L. R. & Robshaw, M. J. B. (1996). Non-linear approximations in linear cryptanalysis. In *Advances in Cryptology — EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 224–236, Berlin, Heidelberg. Springer, DOI: 10.1007/3-540-68339-9_20.

Lidl, R. & Niederreiter, H. (1997). *Finite Fields*. Cambridge University Press, 2 edition.

Malik, D. S., Mordeson, J. N., & Sen, M. K. (1997). *Abstract Algebra*. McGraw-Hill, New York.

Mar, P. P. & Latt, K. M. (2008). New analysis methods on strict avalanche criterion of s-boxes. *World Academy of Science, Engineering and Technology*, 48:25.

Matsui, M. (1993). Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT 1993)*, pages 386–397. Springer.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Mohamed, K., Pauzi, M. N. M., Ali, F. A. H. M., Ariffin, S., & Zulkipli, N. H. N. (2014). Study of s-box properties in block cipher. In *2014 International Conference on Computer, Communications, and Control Technology (I4CT)*, pages 362–366. IEEE.

Murphy, S. & Robshaw, M. J. B. (2002). Essential algebraic structure within the aes. In *Advances in Cryptology—CRYPTO 2002*, pages 1–16. Springer.

NIST (2001). Advanced encryption standard (aes). Federal Information Processing Standards Publication FIPS-197, U.S. Department of Commerce, DOI: 10.6028/NIST.FIPS.197, https://doi.org/10.6028/NIST.FIPS.197.

Nyberg, K. (1993). On the construction of highly nonlinear permutations. In *Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT 1993)*, pages 92–98. Springer.

Paar, C. & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan*. Andi Offset, Yogyakarta.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715.

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson, 7 edition.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA

Wahyuni, S., Wijayanti, I. E., Yuwaningsih, D. A., & Hartanto, A. D. (2020). *Teori Ring dan Modul*. UGM Press, Yogyakarta, cetakan kedua edition, ISBN: 978-602-386-118-7.

Webster, A. F. & Tavares, S. E. (1986). On the design of s-boxes. In *Advances in Cryptology—CRYPTO 1985*, pages 523–534. Springer.

STATE ISLAMIC UNIVERSITY
SUNAN KALIJAGA
YOGYAKARTA