DETEKSI DAN IDENTIFIKASI KECURANGAN PEMBAGIAN RAHASIA LINEAR BERBASIS SKEMA SHAMIR DENGAN KOEFISIEN BARISAN FIBONACCI

M. HADZIQ RAFLI FASYA

PROGRAM STUDI MATEMATIKA
SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA
INSTITUT PERTANIAN BOGOR
BOGOR
2025

PERNYATAAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa skripsi dengan judul "Deteksi dan Identifikasi Kecurangan Pembagian Rahasia Linear Berbasis Skema Shamir dengan Koefisien Barisan Fibonacci" adalah karya saya dengan arahan dari dosen 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.

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Institut Pertanian Bogor.

Bogor, Juli 2025

M. Hadziq Rafli Fasya
NIM G5401211002

ABSTRAK

M. HADZIQ RAFLI FASYA. Deteksi dan Identifikasi Kecurangan Pembagian Rahasia Linear Berbasis Skema Shamir dengan Koefisien Barisan Fibonacci. Dibimbing oleh SUGI GURITMAN dan JAHARUDDIN.

Keamanan informasi menjadi aspek krusial dalam era digital, terutama dalam skema pembagian rahasia. Skema Shamir merupakan salah satu metode berbagi rahasia yang aman, namun masih rentan terhadap kecurangan pemegang keping rahasia yang memberikan informasi palsu saat rekonstruksi. Penelitian ini mengusulkan skema pembagian rahasia linear berbasis Skema Shamir yang dimodifikasi dengan koefisien barisan Fibonacci untuk meningkatkan keamanan terhadap serangan individu maupun kolaboratif. Metode yang digunakan mencakup pembangkitan keping rahasia berbasis polinomial Fibonacci serta algoritma deteksi dan identifikasi kecurangan menggunakan pendekatan sistem persamaan linear. Hasil penelitian menunjukkan bahwa skema yang diusulkan dapat mendeteksi kecurangan dengan partisipasi minimal k pemegang keping rahasia dan mengidentifikasi pelaku kecurangan jika jumlah partisipan mencapai $k + 1$. Selain itu, analisis keamanan menunjukkan bahwa skema ini lebih baik dibandingkan metode Shamir dengan interpolasi Lagrange dalam menghadapi manipulasi keping rahasia secara acak.

Kata kunci: Pembagian rahasia, skema Shamir, barisan Fibonacci, deteksi kecurangan, keamanan informasi.

ABSTRACT

M. HADZIQ RAFLI FASYA. Detection and identification of Linear Secret Sharing Fraud Based on Shamir Scheme with Fibonacci Sequence Coefficients. Supervised by SUGI GURITMAN and JAHARUDDIN.

Information security is a crucial aspect in the digital era, especially in secret sharing schemes. Shamir's scheme is one of the secure methods for secret sharing, yet it remains vulnerable to dishonest participants who submit false shares during reconstruction. This study proposes a linear secret sharing scheme based on Shamir's scheme, modified using Fibonacci sequence to enhance security against both individual and collaborative attacks. The method involves generating secret shares using Fibonacci-based polynomials and implementing fraud detection and identification algorithms through a system of linear equations. The results indicate that the proposed scheme can detect fraud with a minimum of k participants and identify dishonest participants when at least $k + 1$ participants are involved. Furthermore, security analysis shows that this scheme is better than Shamir's Secret Sharing Scheme with Lagrange Interpolation in preventing random manipulation of secret shares.

Keywords: Secret sharing, Shamir's scheme, Fibonacci sequence, fraud detection, information security.

DETEKSI DAN IDENTIFIKASI KECURANGAN PEMBAGIAN RAHASIA LINEAR BERBASIS SKEMA SHAMIR DENGAN KOEFISIEN BARISAN FIBONACCI

M. HADZIQ RAFLI FASYA

Skripsi
sebagai salah satu syarat untuk memperoleh gelar
Sarjana Matematika pada
Program Studi Matematika

PROGRAM STUDI MATEMATIKA
SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA
INSTITUT PERTANIAN BOGOR
BOGOR
2025

Penguji pada Ujian Skripsi:
Teduh Wulandari Mas'oed, S.Si. M.Si.

Judul Skripsi : Deteksi dan Identifikasi Kecurangan Pembagian Rahasia Linear Berbasis Skema Shamir dengan Koefisien Barisan Fibonacci
Nama : M. Hadziq Rafli Fasya
NIM : G5401211002

Disetujui oleh

Pembimbing 1:
Dr. Drs. Sugi Guritman

Pembimbing 2:
Prof. Dr. Drs. Jaharuddin, M.S.

Diketahui oleh

Ketua Program Studi S1 Matematika:
Dr. Donny Citra Lesmana, S.Si. M.Fin.Math
NIP 197902272005011001

Tanggal Ujian: 18 Juni 2025 Tanggal Lulus:

PRAKATA

Puji dan syukur penulis panjatkan kepada Allah subhanaahu wa ta'ala atas segala karunia-Nya sehingga karya ilmiah ini berhasil diselesaikan. Tema yang dipilih dalam penelitian yang dilaksanakan sejak bulan Oktober 2024 sampai bulan Februari 2025 ini ialah Kriptografi, dengan judul "Deteksi dan Identifikasi Kecurangan Pembagian Rahasia Linear Berbasis Skema Shamir dengan Koefisien Barisan Fibonacci".

Penyusunan karya ilmiah ini dapat diselesaikan tentunya tidak terlepas dari bantuan dan dukungan berbagai pihak. Oleh karena itu, dalam kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Ibu Fatimah selaku orang tua penulis, Rayhan Farid dan Rizki Ahmad Ridho selaku adik penulis yang senantiasa memberikan doa dan dukungannya.
2. Keluarga besar Ibu Fatimah yang senantiasa mendoakan dan memotivasi dalam penulisan karya ilmiah ini.
3. Bapak Dr. Drs. Sugi Guritman selaku dosen pembimbing satu dan Prof. Dr. Drs. Jaharuddin, M.S. selaku dosen pembimbing dua atas segala ilmu, motivasi, dan arahannya selama penulisan karya ilmiah ini.
4. Seluruh dosen Program Studi Matematika atas segala ilmu yang diberikan.
5. Seluruh staf Program Studi Matematika atas segala bentuan yang telah diberikan selama penulisan karya ilmiah ini.
6. Seluruh teman-teman mahasiswa Program Studi Matematika, khususnya angkatan 58 yang telah memberikan saran dan segala bentuk dukungannya.
7. Intan Bestari sebagai sahabat seperjuangan yang selalu menemani dan mendengarkan keluh kesah serta memberikan semangat dalam penulisan karya ilmiah ini.
8. Muhamad Rifqi Al-Wafi dan Ridwan Putra Firmansyah sebagai teman dekat yang memberikan masukan dalam penulisan karya ilmiah ini.
9. Semua pihak yang terlibat dan membantu dalam penyusunan karya ilmiah ini.

Semoga karya ilmiah ini bermanfaat bagi pihak yang membutuhkan dan bagi kemajuan ilmu pengetahuan.

Bogor, Juli 2025

M. Hadziq Rafli Fasya

DAFTAR ISI

DAFTAR ISI ix
DAFTAR LAMPIRAN x
I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Tujuan Penelitian 2
II TINJAUAN PUSTAKA 3
2.1 Sistem Persamaan dan Kebebasan Linear 3
2.2 Interpolasi Polinomial 4
2.3 Modulo Bilangan Bulat 5
2.4 Polinomial Atas Lapangan 5
2.5 Skema Pembagian Rahasia 6
2.5.1 Skema-(k, n) Shamir 7
2.5.2 Skema Pembagian Rahasia Shamir 8
2.5.3 Skema Pembagian Rahasia Linear 9
III HASIL DAN PEMBAHASAN 11
3.1 Skema Linear Berbasis Skema Shamir 11
3.2 Serangan Pelaku Kecurangan dan Analisis Keamanan 12
3.3 Rekonstruksi Skema Pembagian Rahasia Shamir 14
IV SIMPULAN DAN SARAN 25
4.1 Simpulan 25
4.2 Saran 25
DAFTAR PUSTAKA 26
LAMPIRAN 28
RIWAYAT HIDUP 35

DAFTAR LAMPIRAN

1	Pembangkitan polinomial Fibonacci	29
2	Perhitungan parameter deteksi yang dibangkitkan oleh *Dealer*	30
3	Pemilihan partisipan	31
4	Pencarian solusi bagi koefisien polinomial	32
5	Pendeteksian kecurangan	33
6	Pengidentifikasian pelaku kecurangan	34