PENGEMBANGAN ALGORITMA PENDETEKSIAN DAN PENGIDENTIFIKASIAN KECURANGAN PADA SKEMA MODIFIKASI (k, n) MIGNOTTE

RISNATIA DESTIYANTI NURUL FADILA

PROGRAM STUDI MATEMATIKA
SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA
INSTITUT PERTANIAN BOGOR
BOGOR
2026

PERNYATAAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa skripsi dengan judul "Pengembangan Algoritma Pendeteksian dan Pengidentifikasian Kecurangan pada Skema Modifikasi $(k,\ n)$ Mignotte" 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 2026

Risnatia Destiyanti Nurul Fadila
NIM G5401221024

ABSTRAK

RISNATIA DESTIYANTI NURUL FADILA. Pengembangan Algoritma Pendeteksian dan Pengidentifikasian Kecurangan pada Skema Modifikasi (k, n) Mignotte. Dibimbing oleh SUGI GURITMAN dan JAHARUDDIN.

Keamanan informasi menjadi isu penting seiring meningkatnya risiko kebocoran, sehingga diperlukan penerapan algoritma kriptografi untuk menjaga kerahasiaan tersebut. Salah satu pendekatan yang digunakan adalah skema pembagian rahasia, khususnya *threshold secret sharing scheme* berbasis skema (k, n) Mignotte. Namun, skema ini bersifat *not perfect* dan belum dilengkapi mekanisme deteksi kecurangan. Oleh karena itu, penelitian ini bertujuan memodifikasi proses pembangkitan barisan, memodifikasi algoritma pembagian dan rekonstruksi *secret* serta deteksi dan identifikasi kecurangan, serta mengidentifikasi berbagai tipe kecurangan. Penelitian mencakup tahap pembangkitan barisan, pembentukan *secret*, pembentukan *share*, dan rekonstruksi *secret*. Proses deteksi dan identifikasi kecurangan dilakukan dengan menggunakan nilai identifikasi U . Hasil penelitian menunjukkan bahwa penggunaan nilai U mampu memverifikasi kebenaran *share*. Keberhasilan rekonstruksi *secret* juga bergantung pada terpenuhinya jumlah *share* minimum sesuai nilai ambang batas k. Dengan demikian, memodifikasi skema mampu meningkatkan kemampuan dalam mendeteksi dan mengidentifikasi kecurangan dibanding skema Mignotte klasik.

Kata kunci: *chinese remainder theorem*, identifikasi kecurangan, mignotte, pembagian rahasia

ABSTRACT

RISNATIA DESTIYANTI NURUL FADILA. Development of Algorithms for Cheating Detection and Identification in the Modified (k, n) Mignotte Scheme. Supervised by SUGI GURITMAN and JAHARUDDIN.

Information security has become an important issue due to the increasing risk of data breaches, thus requiring the application of cryptographic algorithms to maintain confidentiality. One approach is the secret sharing scheme, particularly the (k, n) threshold scheme based on Mignotte. However, this scheme is not perfect and lacks mechanisms for cheating detection. This study aims to modify the sequence generation, as well as the secret sharing and reconstruction algorithms, and to incorporate cheating detection and identification. The research includes sequence generation, secret construction, share generation, and secret reconstruction. Cheating detection is performed using the identification value U. The results show that U can verify the validity of share s, while successful reconstruction depends on fulfilling the minimum number of share s according to the threshold k. Thus, the modified scheme improves the ability to detect and identify cheating compared to the classical Mignotte scheme.

Keywords: chinese remainder theorem, cheating identification, mignotte, secret sharing

PENGEMBANGAN ALGORITMA PENDETEKSIAN DAN PENGIDENTIFIKASIAN KECURANGAN PADA SKEMA MODIFIKASI (k, n) MIGNOTTE

RISNATIA DESTIYANTI NURUL FADILA

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
2026

Tim Penguji pada Ujian Skripsi:

1 Bidayatul Masulah, S.Si., M.Sc.

Judul Skripsi : Pengembangan Algoritma Pendeteksian dan Pengidentifikasian Kecurangan pada Skema Modifikasi (k, n) Mignotte
Nama : Risnatia Destiyanti Nurul Fadila
NIM : G5401221024

Disetujui oleh

Pembimbing 1:
Dr. Drs. Sugi Guritman

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

Diketahui oleh

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

Tanggal Ujian: 23 Juni 2026 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 2025 sampai bulan April 2026 ini ialah Kriptografi, dengan judul "Pengembangan Algoritma Pendeteksian dan Pengidentifikasian Kecurangan pada Skema Modifikasi (k, n) Mignotte". Dalam penyusunan karya ilmiah ini, penulis menyadari bahwa keberhasilan yang diraih tidak terlepas dari bantuan, dukungan, dan doa dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih sebesar-besarnya kepada:

1. Mamah dan Bapak selaku kedua orang tua penulis yang senantiasa mendoakan dan meridhoi setiap langkah penulis, serta Kakek, Nenek, dan Adik yang selalu menjadi motivasi penulis untuk segera menyelesaikan penulisan karya ilmiah ini.
2. Bapak Dr. Drs. Sugi Guritman selaku dosen pembimbing satu dan Bapak Prof. Dr. Jaharuddin, M.S. selaku dosen pembimbing dua atas segala ilmu, motivasi, dan arahannya selama penyusunan karya ilmiah ini. Ibu Bidayatul Masulah, S.Si., M.Sc. selaku dosen penguji yang telah memberikan saran, kritik, dan masukan yang sangat membangun bagi penyempurnaan karya ilmiah ini. Ibu Prof. Dr. Ir. Sri Nurdiati, M.Sc. selaku dosen pembimbing akademik yang senantiasa memberikan dukungan dan motivasi kepada penulis.
3. Seluruh dosen dan tenaga kependidikan Program Studi Matematika yang telah memberikan ilmu, bimbingan, dan bantuan selama penulis menjalani masa perkuliahan.
4. Ecak, Amaw, Cindut, Ayuw, Hapij, Jids atas kebersaman, dukungan, doa, serta semangat yang selalu diberikan kepada penulis dalam setiap proses hingga karya ilmiah ini dapat diselesaikan.
5. Emteka (Marisa dan Nova) serta Bismillah terutama Isna, Salsa, dan Wiga selaku teman yang selalu menemani dan mewarnai perjalanan penulis selama masa perkuliahan.
6. Risan (Riset Analisis) Gumatika yang telah menjadi rumah bagi penulis untuk belajar, berdiskusi, dan bertumbuh bersama selama masa perkuliahan.
7. Seluruh teman-teman Mahasiswa Program Studi Matematika Angkatan 59, khususnya teman-teman yang telah meluangkan waktu untuk menjadi tutor, berbagi ilmu, serta mengajak belajar bersama selama masa perkuliahan.
8. Semua pihak yang terlibat dan membantu dalam penyusunan karya ilmiah ini yang tidak bisa disebut satu per satu.

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

Bogor, Juli 2026

Risnatia Destiyanti Nurul Fadila

DAFTAR ISI

DAFTAR TABEL

DAFTAR LAMPIRAN