



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



Hak Cipta Dilindungi Undang-undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University;

© Hak Cipta milik IPB, tahun 2026
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 IPB.

Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apa pun tanpa izin IPB

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**



@Hak cipta milik IPB University

Hak Cipta Dilindungi Undang-undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University;

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 arahnya 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 Nurdianti, 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, Ayu, Hapij, Jids atas kebersamaan, 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	x
DAFTAR LAMPIRAN	x
I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan Penelitian	2
II TINJAUAN PUSTAKA	3
2.1 Teori Bilangan	3
2.2 Aritmatika Modulo	4
2.3 Kriptografi	7
2.4 Pembagian Rahasia	7
III HASIL DAN PEMBAHASAN	18
3.1 Pembangkitan Barisan Modifikasi (k, n) Mignotte	18
3.2 Pembangkitan Barisan (k, n) Mignotte Teorema Putresza	20
3.3 Penentuan Nilai <i>Floor</i> dan Representasi Bit	22
3.4 Parameter Detektor	23
3.5 Pembentukan dan Rekonstruksi <i>Secret</i>	24
3.6 Rekonstruksi <i>Secret</i> jika Terjadi Kecurangan	32
3.7 Rekonstruksi <i>Secret</i> jika <i>Share</i> Kurang dari k	35
3.8 Tipe Serangan Kecurangan oleh <i>Cheaters</i>	37
IV SIMPULAN DAN SARAN	42
4.1 Simpulan	42
4.2 Saran	42
DAFTAR PUSTAKA	44
LAMPIRAN	46
RIWAYAT HIDUP	77



1	Hasil pembentukan nilai p_0 berdasarkan variasi ukuran bit awal	23
2	Hasil teorema sisa Cina	30
3	Hasil nilai identifikasi u_i ketika $k \geq n$	31
4	Share modifikasi	32
5	Hasil teorema sisa Cina	33
6	Hasil nilai identifikasi u_i ketika terjadi kecurangan	34
7	Perhitungan teorema sisa Cina	35
8	Hasil nilai identifikasi u_i ketika $k < n$	36
9	Hasil nilai identifikasi u_i pada kecurangan tipe 1	38
10	Hasil nilai identifikasi u_i pada kecurangan tipe 2	39
11	Hasil nilai identifikasi u_i pada kecurangan tipe 3	41

DAFTAR LAMPIRAN

1	Implementasi algoritma 1	47
2	Implementasi algoritma 2	49
3	Penentuan <i>floor</i> dan representasi bit	50
4	Perhitungan nilai bit	51
5	Hasil perhitungan nilai bit	52
6	Tahap pembentukan kunci rahasia (<i>secret</i>)	58
7	Tahapan pembentukan keping rahasia (<i>share</i>)	60
8	Tahapan penyatuan <i>share</i> menjadi <i>secret</i>	61
9	Tabel perhitungan CRT	64
10	Penggabungan <i>share</i> jika terjadi kecurangan	65
11	Perhitungan CRT	68
12	Penggabungan <i>share</i> jika $k < n$	69
13	Implementasi kecurangan tipe 1	71
14	Implementasi kecurangan tipe 2	74
15	Implementasi kecurangan tipe 3	75