



SKEMA DETEKSI KECURANGAN PEMBAGIAN RAHASIA BERBASIS CHINESE REMAINDER THEOREM

DHEA EKAPUTRI



**DEPARTEMEN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
INSTITUT PERTANIAN BOGOR
BOGOR
2024**

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 mengurangi kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.



PERNYATAAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa skripsi dengan judul “Skema Deteksi Kecurangan Pembagian Rahasia Berbasis *Chinese Remainder Theorem*” 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 2024

Dhea Ekaputri
NIM G5401201074



ABSTRAK

DHEA EKAPUTRI. Skema Deteksi Kecurangan Pembagian Rahasia Berbasis *Chinese Remainder Theorem*. Dibimbing oleh SUGI GURITMAN dan TEDUH WULANDARI MAS'OED.

Rahasia merupakan sesuatu yang sengaja disembunyikan agar tidak diketahui oleh pihak yang tidak berwenang. Namun, saat ini sering terjadi kebocoran rahasia. Salah satu cara untuk mencegah terjadinya kebocoran rahasia adalah dengan melakukan pembagian rahasia. Pembagian rahasia merupakan cara mengamankan rahasia dengan memecah rahasia menjadi kepingan rahasia, lalu mendistribusikannya kepada partisipan. Namun, cara ini tetap berpeluang bagi berbagai pihak untuk melakukan kecurangan. Karya ilmiah ini bertujuan untuk merekonstruksi skema pembagian rahasia berbasis Chinese Remainder Theorem (CRT), meliputi skema Mignotte dan Asmuth Bloom, mengkaji aspek keamanan dan skema pendekripsi kecurangan, serta mengimplementasikannya pada Python. Pendekripsi kecurangan pada kedua skema dilakukan dengan cara berbeda, Mignotte menggunakan parameter detektor (pD), sedangkan Asmuth Bloom menggunakan fungsi satu arah. Adanya penambahan skema pendekripsi dapat meningkatkan keamanan skemanya. Kemudian, pengimplementasian pada Python dapat mempermudah penerapan skema karena mampu mengefisiensikan waktu perhitungan.

Kata kunci: Asmuth Bloom, *Chinese Remainder Theorem*, deteksi kecurangan, Mignotte, pembagian rahasia.

ABSTRACT

DHEA EKAPUTRI. Secret Sharing Cheating Detection Scheme Based on Chinese Remainder Theorem. Supervised by SUGI GURITMAN and TEDUH WULANDARI MAS'OED.

Secrets are something that is deliberately hidden from unauthorized parties. However, nowadays there are frequent leaks of secrets. A way to prevent the secret leaks is to share the secrets. The secret leaks sharing is a way to secure secrets by breaking the secret leaks into secret pieces, then distributing them to participants. However, this method still allows various parties to commit fraud. This scientific paper aims to reconstruct the secret sharing scheme based on the Chinese Remainder Theory (CRT), including the Mignotte and Asmuth Bloom schemes, examine security aspects and fraud detection schemes, and implement them in Python. Fraud detection on both schemes is done in different ways, Mignotte uses detector parameters (pD), while Asmuth Bloom uses a one-way function. The addition of detection schemes can improve the security of the scheme. Then, implementation in Python can make it easier to implement schemas because it is able to streamline calculation time.

Keywords: Asmuth Bloom, cheating detection, Chinese Remainder Theorem, Mignotte, secret sharing.



©Hak cipta milik IPB University

IPB University



Hak Cipta Dilindungi Undang-undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

- Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah.
- 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 2024
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.



SKEMA DETEKSI KECURANGAN PEMBAGIAN RAHASIA BERBASIS CHINESE REMAINDER THEOREM

DHEA EKAPUTRI

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

**DEPARTEMEN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
INSTITUT PERTANIAN BOGOR
BOGOR
2024**

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 mengurangi kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

IPB University

@Hak cipta milik IPB University

Penguji pada Ujian Skripsi:
Drs. Siswandi, M.Si.





Judul Skripsi : Skema Deteksi Kecurangan Pembagian Rahasia Berbasis *Chinese Remainder Theorem*
Nama : Dhea Ekaputri
NIM : G5401201074

Disetujui oleh

Pembimbing 1:
Dr. Drs. Sugi Guritman

Pembimbing 2:
Teduh Wulandari Mas'oed, M.Si.

Diketahui oleh

Ketua Departemen Matematika:
Dr Ir Endar Hasafah Nugrahani, MS
NIP 196312281989032001

Tanggal Ujian: 21 Mei 2024

Tanggal Lulus:

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 mengurangi kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.



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 November 2023 sampai bulan Maret 2024 ini ialah Kriptografi, dengan judul “Skema Deteksi Kecurangan Pembagian Rahasia Berbasis *Chinese Remainder Theorem*”.

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 Eem Apriani dan Bapak Yudi Budianto selaku kedua orang tua penulis dan Aldo Rizky Budianto selaku adik penulis yang senantiasa memberikan doa dan dukungannya,
2. Keluarga besar Bapak Omod dan Ibu E. Karmini yang senantiasa mendoakan dan memotivasi dalam penulisan karya ilmiah ini,
3. Bapak Dr. Drs. Sugi Guritman selaku dosen pembimbing satu dan Ibu Teduh Wulandari Mas'oed, M.Si. selaku dosen pembimbing dua atas segala ilmu, motivasi, dan arahannya selama penulisan karya ilmiah ini,
4. Seluruh dosen Departemen Matematika atas segala ilmu yang diberikan,
5. Seluruh staf Departemen Matematika atas segala bentuan yang telah diberikan selama penulisan karya ilmiah ini,
6. Seluruh teman-teman mahasiswa Departemen Matematika, khususnya angkatan 57 yang telah memberikan saran dan segala bentuk dukungannya,
7. Amanda Nabilah, Sherly Yulianty, Suci Nur Setyawati, dan Vina Alfiati sebagai teman seperjuangan yang selalu menemani dan mendengarkan keluh kesah serta memberikan bantuan dalam penulisan karya ilmiah ini,
8. Teman-teman *fasttrack* yang selalu bersama-sama perjuangkan tahap demi tahap penyelesaian tugas akhir,
9. Tim PKM-PM *Math Mission*, yaitu Syifa Noer Sya'adah, Rio Rizky, dan Muhamad Rifqi Al-Wafi yang telah memberikan motivasi dan dukungannya selama penulisan karya ilmiah ini,
10. Teman-teman dekat ketika SMA yang telah membantu memberikan semangat dan masukannya dalam penulisan karya ilmiah ini,
11. 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 2024

Dhea Ekaputri



DAFTAR LAMPIRAN

I	PENDAHULUAN	x
1.1	Latar Belakang	1
1.2	Tujuan Penelitian	1
II	TINJAUAN PUSTAKA	2
2.1	Teori Bilangan	3
2.2	Grup	3
2.3	Aritmatika Modulo	4
2.4	Aljabar Abstrak	4
2.5	Kriptografi	7
2.6	Pembagian Rahasia	8
III	HASIL DAN PEMBAHASAN	9
3.1	Rekonstruksi Skema Pembagian Rahasia Mignotte	14
3.2	Rekonstruksi skema Pembagian Rahasia Asmuth Bloom	14
3.3	Skema Pendekripsi Kecurangan Mignotte	21
3.4	Skema Pendekripsi Kecurangan Asmuth Bloom	28
3.5	Tipe Serangan Kecurangan oleh <i>Cheaters</i>	37
IV	SIMPULAN DAN SARAN	45
4.1	Simpulan	50
4.2	Saran	50
	DAFTAR PUSTAKA	51
	LAMPIRAN	53
	RIWAYAT HIDUP	68

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 mengurangi kepentingan yang wajar IPB University.

2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.



DAFTAR LAMPIRAN

Algoritma pembentukan barisan Mignotte	54
Algoritma pembagian rahasia Mignotte	55
Algoritma penyatuhan rahasia Mignotte	56
Algoritma pembentukan barisan bilangan prima	57
Algoritma pembagian rahasia Asmuth Bloom	58
Algoritma penyatuhan rahasia Asmuth Bloom	59
Algoritma pembagian rahasia Mignotte dengan penambahan parameter detektor	60
Algoritma keping rahasia palsu berpola pada skema Mignotte	62
Algoritma cheater mencari kunci rahasia asli pada skema Mignotte	63
Deteksi kecurangan pada skema Mignotte	64
Algoritma Asmuth Bloom dengan gungsi satu arah	65
Algoritma keping rahasia palsu berpola pada Asmuth Bloom	66
Deteksi kecurangan pada skema Asmuth Bloom	67

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 mengurangi kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.