

INTISARI

Identifikasi *Cheater* pada Skema Pembagian Rahasia

Oleh

Toto Budi Trapsilo

17/412732/PA/18051

Skema pembagian rahasia adalah cara membagi sebuah rahasia menjadi beberapa bagian ke beberapa partisipan sedemikian sehingga kelompok partisipan berwenang dapat merekonstruksi rahasia yang dibagikan dan kelompok partisipan yang tidak berwenang tidak dapat mendapatkan informasi apapun terkait rahasia yang dibagikan. Salah satu masalah yang dapat muncul pada skema pembagian rahasia adalah adanya *cheater* yaitu partisipan yang membagikan bagian palsu ketika proses rekonstruksi rahasia dilakukan. Pada skripsi ini dibahas mengenai solusi dari permasalahan tersebut berupa skema pembagian rahasia berbasis polinom bivariat simetris. Skema pembagian rahasia ini memiliki kemampuan untuk mendeteksi dan mengidentifikasi *cheater* dengan beberapa batasan.

ABSTRACT

Cheater Identification in Secret Sharing Schemes

By

Toto Budi Trapsilo

17/412732/PA/18051

A secret sharing scheme is a method to divide secret data into several shares to participants such that any authorized group of participants can reconstruct the shared secret with their shares and any unauthorized group of participants can not gain any information regarding the shared secret. One of the problems that can arise with secret sharing schemes is that there are cheaters among participants who share fake shares in the secret reconstruction process. In this undergraduate thesis, we discussed the solution to the cheater problem in the form of secret sharing schemes based on symmetric bivariate polynomials. This secret sharing scheme has the capability to detect and identify cheaters up to some extent.