INTISARI

SKEMA PEMBAGIAN RAHASIA PROAKTIF MENGGUNAKAN PROYEKSI MATRIKS

Oleh

ADITYA MAHAT PRAKARSA

12/331182/PA/14481

Dalam skripsi ini akan dibicarakan mengenai skema pembagian rahasia berdasarkan proyeksi matriks yang diperkenalkan oleh Bai dan Wang, beserta sejumlah sifat terkait. Skema pembagian rahasia merupakan suatu cara untuk membagikan rahasia ke dalam sekelompok partisipan secara sistematis. Bagian yang dibagikan untuk tiap partisipan dalam skema ini disebut bagian rahasia. Sekumpulan partisipan dapat menghitung rahasia dengan mengkontribusikan bagian rahasia mereka. Salah satu pengembangan dari skema pembagian rahasia adalah skema pembagian rahasia proaktif menggunakan proyeksi matriks.

ABSTRACT

PROACTIVE SECRET SHARING SCHEME USING MATRIX PROJECTION

By

ADITYA MAHAT PRAKARSA

12/331182/PA/14481

In this thesis we will discuss about secret sharing schemes based on matrix projection, both introduced by Bai and Wang. Secret sharing scheme is a way to share secret(s) among participants systematically. Each participant gets a secret share. A group of participants can recover secret(s) by contributing their share. One of development on secret sharing scheme is proactive secret sharing scheme using matrix projection.