Skema pembagian rahasia menggunakan matriks proyeksi = Secret sharing scheme using matrix projection

Ika Dwi Novitasari, author

Abstrak

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan pesan. Suatu pesan jika hanya disimpan oleh satu orang saja terdapat resiko dimana orang tersebut menyalahgunakan atau memanipulasi pesan. Sedangkan jika terlalu banyak orang yang dapat mengakses pesan, kemungkinan kebocoran pesan menjadi lebih besar. Salah satu studi kriptografi yang digunakan untuk mengatasi masalah ini yaitu skema pembagian rahasia. Skema pembagian rahasia adalah metode mengamankan pesan dengan mendistribusikan pesan tersebut menjadi beberapa bagian kepada partisipan (orang), sedemikian sehingga hanya kombinasi partisipan (orang) tertentu yang dapat membuka isi pesan. Dalam tugas akhir ini dibahas mengenai bagaimana mengkonstruksi skema pembagian rahasia menggunakan matriks proyeksi. Selanjutnya, skema akan diimplementasikan pada pesan berupa string yang diubah ke bentuk kode ASCII (American Standart Code for Information Interchange) dan dapat direpresentasikan sebagai matriks bujur sangkar.

.....Cryptography is a study of mathematical techniques related to message security. When a message is only saved by one person, there will be a risk that the person will misuse or manipulate the message. Whereas, when too many peope have access to the message, there will be more possibilities of message to be leaked. One of the ways to overcome this problem is by secret sharing scheme. Secret sharing scheme is a method to secure message by distributing it to participants (people), so that only certain combinations of people can open the message. In this undergraduate thesis, the discussion is focused on how to construct secret sharing scheme by using matrix projection. Then, the scheme will be implemented to message in the form of string which has been changed into ASCII (American Standart Code for Information Interchange) and can represented as a square matrix.