CS 507 – CRYPTOGRAPHY

PROJECT PROPOSAL

“CRYPTOGRAPHIC TECHNIQUES IN PRIVACY PRESERVING DATA MINING”

Prepared by Beril S. Çiftçi

Introduction:

Data mining technology offers knowledge discovery among large quantities of data by using various methods, like classification, clustering, association rule mining, sequence detection, etc. Although data sharing is important for organizations, confidentiality of the mass collection of data is a major problem in database management. That’s why; many algorithms have been developed to prevent undesirable mining of published data. Besides common data mining techniques (decision tree approach, classification, etc.), cryptographic tools are also popular in privacy preserving; especially in association rule mining.

Goal:

This project will focus on approaches for obtaining security in association rule mining, limiting the shared information. The goal is to learn the procedures to mine association rules on vertically and horizontally partitioned data. Also, general definitions of security for multi-party cryptographic protocols will be presented, however not too much detailed.

Objectives:

Considering that the protocol and/or algorithm proofs are beyond the scope of the project, main objectives are:

- To introduce the data mining concepts (e.g. association rule mining) and to emphasize confidentiality issues in data mining
- To present and compare different techniques of privacy preserving, which have been developed recently
- To discuss the concept of “secure multi-party computation"
- To present secure association rule mining methods, based on multi-party communication

References:
