CS 507 – CRYPTOGRAPHY

PROJECT PROPOSAL

“A Client – Server Application to Demonstrate XML Digital Signatures”

Prepared by Zafer GÜREL

Introduction:

XML is an emerging standard and technology in the recent years for data exchange between different parties which have different technological infrastructures. The advantage of XML is that it defines data very clearly and in a very structured way. It is obvious that trustable, secure XML messages to form the basis of those transactions are highly needed.

Enabling secure transactions is the concept of a digital signature, ensuring the integrity and authenticity of origin for business documents. XML Signature is an evolving standard for digital signatures that both addresses the special issues and requirements that XML presents for signing operations and uses XML syntax for capturing the result, simplifying its integration into XML applications.

Goal:
To develop an client-server application that will use XML messages to exchange data and secure the transaction between those parties by using XML signature.

Objectives:

Protocol and/or algorithm proofs will not be covered in this project. Objectives are as follows:
1. To give an overview about the concepts of XML digital signatures.
2. To present some technical information about the on-going work about XML signatures.
3. To implement XML digital signature in a client-server application.

References:

1. http://www.w3.org/TR/xmldsig-core/