Crypto Case 5: Is SSL/TLS Enough to Secure E-commerce?

Real-world Scenario: E-commerce/Web services integrate web-based applications and allow communication among different sources.

Problem and Activities: 1) Design an authentication solution which enables e-commerce/web services to more than three parities to be authenticated to one another. For example, a cardholder, an online merchant, and a bank can authenticate each other. Standards like SSL/TLS (Secure Socket Layer/Transport Level Security) only support point-to-point authentication. 2) Design an encryption solution that supports selective encryption. This is useful in a workflow scenario where a document may be processed by several applications, or signed, viewed, or approved by numerous people. Standards like S/MIME (Secure Socket Layer/Transport Level Security) and PGP (Pretty Good Privacy) as well as SSL/TLS treat each message as a whole.

Learning Outcomes: Students will be able to analyze requirements, design their own protocol to support multiple-party authentication, and selective encryption. Students will learn and practice how to provide quality of protection through message integrity, message confidentiality, and single message authentication. The XML (extensible markup language), web service security, SOAP (Simple Object Access Protocol) messaging will be investigated.

Assessment: Students will use written report and oral presentation to demonstrate the results.