CS 428 – Applied Cryptography

Module 11 Homework

Cameron Stark

1.) What is the threat model for Digital Signatures?

Chosen-Message Attack is the main attack method that is being prevented with the use of Digital Signatures.

2.) What is the security goal for Digital Signatures?

To prevent an attacker from being to forge a valid signature from a message that is not signed by a sender

3.) How are vital information sent to web services?

Through the method of SSL/TLS where a two step handshake and key exchange process occurs to create a closed and secure connection between the two parties