

CS795: Secure Distributed Systems With .Net
Summer 2009
Homework #5
Due: June 23, 2009

This programming assignment deals with key generation, encryption, decryption, digital signatures, hashing, and XML signatures.

Develop a program that can be run using a browser with the following features:

1. Generate a symmetric key – and show it in a box
2. Generate public-private key pair – and show them in two adjacent boxes
3. Ability to type plaintext in a box
4. Generate a hash of the plaintext --- show it in a box
5. An option to validate the hash --- if the message is altered with same hash, it should say invalid hash
6. Use symmetric key to encrypt the message – show encrypted text
7. Use symmetric key to decrypt ciphertext --- show the decrypted text
8. Use public key to encrypt the plaintext – show encrypted text
9. Use private key to decrypt the ciphertext – show decrypted text (plaintext)
10. Generate a digital signature for the plaintext – show the digital signature
11. Validate the digital signature --- if the message is altered with same hash, it should say invalid signature
12. Have option to enter a reference to an XML document (or type the text right in a box)
13. Display plain XML document
14. Generate XML signature for the XML---show the signature
15. Validate the signature