CS 428 – Applied Cryptography  
Module 11 Homework

Cameron Stark

1.) Provides integrity for users in the public key setting

2.) The left person encrypts their message and auth code, and the receiver verifies the auth code and the message.

3.) public key the message and sender are verified; the cipher text is just deciphered with out a means of knowing it came from the correct person.

4.) Signatures can be verified by anyone, but message authentication codes can only be verified by the holder.

5.) Any program that requires the user to be verified by their certificate, such as a web banking application.

6.) Because the MAC would not be able to be verified by the other users in the application or the application itself

7.) Means that something cannot be denied from happening, the case of cryptography, the keys and signatures can not be denied from signing a message.

8.) Gen is process to generate the public key and signature key, Sign takes the message and signature key to output the encrypted signature which gets sent out, Vrfy is the process for the receiver to verify that the public key, message and signature are correct

9.) Certificate Authority is a third party that verifies individuals messages and encrypts with the public key if the CA can verify the person, is secure unless the public key for the CA is compromised.

10.) SSL works by a two-step process of establishing a secure connection between the two parties and a shared key for that connection and then another layer that uses the shared key to encrypt and exchange information.