

ITCS 412 Cryptography
Second semester 2007/2008
Quiz 1 – Chapter 1

ID: _____

Name: KEY

Section: _____

Q1. [CLO6, CLO7] Fill in the blank with an appropriate word or number.

- 1) Two types of active attacks are modification of message content and message replay.
- 2) Two security service categories in the X.800 standard are authentication and access control.
- 3) Non-repudiation provides protection against denial by one entity in the communication of having participated in all or part of the communication.
- 4) Two example security mechanisms in the X.800 are encipherment and digital signature.
- 5) A user floods a web site with requests and prevents others from using it. This attack is called Denial of Service attack, and is classified as a(n) active attack.

Q2. [CLO7] All the techniques for providing security in the network model that we studied had two components:

- 1) A transformation of the information to be sent.
- 2) A secret key.