

CS 6390-Advanced Computer Networks
UTD-Computer Science Department--Fall 2008—Quiz 4

Name: _____

UTD ID #: _____

1. MD5 is a message digest algorithm. What is keyed MD5? What is the usefulness of keyed MD5?

Keyed MD5 has a secret key. $MD5(m+k)$ can be produced by someone who knows k and not by others.

This cannot be produced by anyone without the knowledge of k . Thus, the recipient knows that sender knows k and is “authentic”.

2. A rogue host can get hold of all IP packets destined for a host H using mobile IP. How do you prevent this?

When registering, ensure that the mobile host is authenticated.

3. What are the advantages of (a) having forwarding engines on separate cards and (b) using a switched backplane (for interconnecting all the input and output line cards) instead of a shared bus?

- (a) Not tied to link layer constraints (speed, space) and modular construction means you can increase link layer/forwarding engine speeds separately.
- (b) High throughput since multiple parallel transfers can take place