7.4 Question 4

7.4.A Give a quick definition for the following terms found in the context of IEEE 802.11i Operation Phases:

Pairwise Keys

Pairwise Keys are usually used for the communication between a pair of devices. Most often between a STA and an AP. These keys are derived dynamically from a master key and are valid for a limited amount of time.

Group Keys

A Group Key is a shared key among all communication members connected to the same AP, and is used to secure multicast/broadcast traffic.

Temporal Key Integrity Protocol (TKIP)

TKIP is an encryption protocol designed to provide more secure encryption than the notoriously weak Wired Equivalent Privacy. TKIP is the encryption method used in Wi-Fi Protected Access (WPA). TKIP is a suite of algorithms that works as a "wrapper" to WEP, which allows users of legacy WLAN equipment to upgrade to TKIP without replacing hardware. To increase the strength of the key used to encrypt each data packet, TKIP includes four additional algorithms:
- A cryptographic message integrity check to protect packets
- An initialization-vector sequencing mechanism that includes hashing, as opposed to WEP's plain text transmission
- A per-packet key-mixing function to increase cryptographic strength
- A re-keying mechanism to provide key generation every 10,000 packets.

Counter Mode-CBC MAC Protocol (CCMP)

CCMP uses the Advanced Encryption Standard (AES) combined with Cipher Block Chaining Countermode (CBC-CTR) for data confidentiality and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity as well as authentication.

7.4.B During the operation of an IEEE 802.11i Robust Security Network, can the communication between a connected mobile station and a wired end-station become insecure? Why?

Yes, it can become insecure during the protected data transfer protocol as if used with the temporlal key integrity protocol, as without rekeying the probability of a successful attack using cryptanalysis rises and the secret key used can become compromised.

7.4.C What is an Association Request Frame? Does this normally include the confidentiality protocol that a Station has decided to use? Why?

The Association Request Frame is used in the discovery phase by the STA in order to ensure the security parameters used. It usually consists of an authentication and key management, a group-key cipher, and a pairwise cipher suites. As the confidentiality protocol is dictated by the access point it is not usually part of this frame.