Motilal Nehru National Institute of Technology Allahabad

Department of Computer Science & Engineering

B.Tech (CS+IT) VI Semester (Mid Semester Exam)

February 2018

CS 1604: Wireless Network Security

M.Marks: 20 **Time : 90 Minutes**

NOTE:

- All Questions are compulsory
- Attempt the questions **strictly** in sequential order **(SECTION WISE)**.
- Answers should be justified & to the point

Section-A [1.5*6=09 Marks]

1. The TKIP MIC is used for data integrity. Which portions of an 802.11 MPDU does the TKIP MIC protect from being altered?

2. Given that additional authentication data (AAD) is constructed from portions of the MPDU header and that the information is used for data integrity, which fields of the MAC header comprise the AAD?

3. When using TKIP encryption, the 48 - bit TSC is generated and broken into TSC0 through TSC5. What are of the inputs taken by Phase 1 of the key - mixing process to generate the TTAK? Which inputs are needed by Phase 2 of the TKIP mixing process?

4. In a robust security network (RSN), which 802.11 management frames are used by client stations and access point to inform each other about their RSNA security capabilities?

5. Which authentication methods provide the seeding material that is needed by the 4 - Way Hand-shake to create temporal keys for encrypting 802.11 MSDU payloads?

6. Draw the header format of 802.11n frame.

P.T.O

Section-B [2+3+2+2+2=11 Marks]

1. How can an attacker perform packet injection, ICMP redirect and Rouge DHCP attacks on WEP encrypted network? Describe the steps of each attack.

2. Describe 4-way handshake process of temporal key creation for WPA 2. How it is vulnerable to attack? Describe KRACK attack.

3. Tammy has been brought in as a consultant to design a WLAN. The customer is concerned that the users will try to hack into each other's laptops over the WLAN. The customer also requires strong security and will be using a VoWiFi solution. What are some of the recommendations that Tammy should make to meet the customers concerns and requirements?

4. In an 802.11 network, station A sends one data frame (not fragmented) to station B. What would be the value of the D field (in microseconds) that needs to be set for the NAV period in each of the following frames: RTS, CTS, data, and ACK? Assume that the transmission time for RTS, CTS, and ACK is 4 μ s each. The transmission time for the data frame is 40 μ s and the SIFS duration is set to 1 μ s. Ignore the propagation time. Note that each frame needs to set the duration of NAV for the rest of the time the medium needs to be reserved to complete the transaction.

5. In an 802.11, give the value of the address 1, address 2, address 3, and address 4 field in each of the following situations (left bit defines To DS and right bit defines From DS).

(A) 00 (B) 01 (C) 10 (D) 11

P.T.O