SSY145 Wireless Networks
Quiz A10 Answer Key
Date: May 14, 2020

The solutions are marked in **boldface**.

1. Which of the following statement(s) are true about reverberation chambers?
   - **(a) Reverberation chambers can be used to simulate handover.**
   - **(b) The rich scattering environment inside the reverberation chamber makes it suitable to simulate keyhole channels**
   - **(c) The reverberation chamber provides rich scattering environment that is repeatable as well as isolated from outside interference that may affect the measurements**
   - **(d) The reverberation chamber can be used to measure TRP (Total Radiated Power) and TIS (Total Isotropic Sensitivity)**

2. Which of the following statements is/are incorrect?
   - (a) WEP uses shared key authentication.
   - **(b) If hash function is used, when one bit in plaintext is modified, we know exactly what bits to change directly.**
     Motivation: It is impossible to predict changes without redoing calculation from clear text if hash function is used.
   - (c) In WEP, APs use MD5 to generate a key from a user's password.
   - (d) WPA2 requires one table per SSID name.

3. Which of the following is/are true about security in GSM?
   - **(a) GSM ensure the identity of the holder thanks to the SIM card**
     Motivation: Authentication using the SIM card (card requires PIN to do operations).
   - **(b) GSM encrypt the communication for confidentiality**
     Motivation: A main security function of GSM is "Encrypting the communication (for confidentiality)".
   - **(c) The security of GSM was based on the confidentiality of its design.**
     Motivation: True, the design was kept secret.
   - (d) GSM is still a secure network today.
     Motivation: False. The design leaked in 1994, was broken in 1998. Many academic papers exist, several vulnerabilities have been found. NSA routinely decrypt the messages.

4. Which of the following is/are steps of shared key authentication (WEP)?

(a) **Client sends authentication request to AP**

(b) **AP sends frame with 128-byte challenge text to client**

(c) **Challenge is encrypted with RC4 using a shared secret and a newly selected IV by the client**

(d) **AP decrypts response and verifies it**
Motivation: See slide 21.