**502553-3 Wireless Systems Security Homework unit #1**

**Fall - 2021 DUE: Wednesday (27/10/2021)**

Osama Elshakankiry

االسم بالعربي: الرقم الجامعي:

# True/False

**Indicate whether the statement is true or false (correct false statements).**

1. Wireless communication is the process of communicating information in electromagnetic media over a distance through a specific cable.
2. Wireless devices such as cellular phones and PDAs are inherently more secure than their wired counterparts.
3. Many security issues with the wire-line networks also apply to the wireless environment.
4. In mobile environment, authentication process should cause disruption to whatever the user’s current task.
5. Authentication protocols require the home authentication server to be contacted during or before the execution of the protocol.
6. Authentication and encryption services were available in the first-generation cellular networks.
7. There was no security provision in the first generation of cellular communication networks.
8. The VLR is responsible for issuing each mobile user a unique identity (ID), known as International Mobile Subscriber Identity (IMSI), and a shared secret key.
9. The A3 algorithm is a stream cipher used to provide confidentiality for messages in over-the-air transmission.

# Completion: Complete each statement

1- Wireless communication is the process of ................................................................

......................................................................................................................................

......................................................................................................................................

2- Security is the combination of processes, procedures and systems used to ................

......................................................................................................................................

......................................................................................................................................

3- Confidentiality is .........................................................................................................

......................................................................................................................................

......................................................................................................................................

4- Integrity protects the data content from ......................................................................

5- Availability is the process of .......................................................................................

......................................................................................................................................

1. A secure mobile solution is one with the following functionality ..............................

......................................................................................................................................

......................................................................................................................................

......................................................................................................................................

......................................................................................................................................

1. A serving mobile network has to query the user’s for

information about the user for security and authentication

1. The four major areas of mobile systems security are ,

................................, ................................, ................................,

9- The objective of an authentication scheme is ............................................................

.............................................................................................................................

1. In mobile environment, authentication protocols require the .....................................

to be contacted during or before the execution of the protocol.

1. The use of digital technique in the second generation of cellular networks enables many features that were not available in the first generation of cellular networks, including ,

...................................................................................................................., and

.....................................................................................................................

1. Each of the new generation of cellular networks involve stronger

......................................... and more .........................................

1. In the first generation of cellular networks, there was no of the

communication data (voice).

1. In a digital wireless communication system, the transceivers are also called user equipments (UEs), which are typically identified by ,

in combination with ...............................

1. In the second generation of cellular communication networks, the service providers can be identified by two components: ........................., and .......................
2. The Home Location Register is responsible for issuing each mobile user a

.......................................................... and a ........................................................

17- The .........................and the .......................... are used for the subscriber to authenticate itself to the network

**Essay:**

1. Explain why wireless devices are inherently less secure than their wired counterparts?
2. Explain why a wireless network has a large number of features distinctively different from those seen in a wire-line network?
3. Explain different security threats of a network?
4. Explain different limitations of mobile environment
5. Explain the four major areas of mobile systems security?
6. What are the features that were enabled in the second generation of cellular networks and were not available in the first generation of cellular networks?
7. What are the data that is hold in a SIM card?
8. Explain the two components that identify the service providers in the second generation of cellular communication networks?
9. What are the improvements that the third-generation networks provide over the second-generation ones?
10. Explain the three essential components that identify the service providers in the third generation of cellular communication networks?
11. Compare between the security architecture of the first generation of cellular communication networks and the security architecture of the second generation of cellular communication networks?
12. What is the main difference between the authentication process in the third generation of cellular communication networks and the authentication process in the second generation of cellular communication networks?
13. Draw and explain the Authentication and Key Agreement (AKA) process for the second generation of cellular communication networks?
14. Draw and explain the Authentication and Key Agreement (AKA) process for the third generation of cellular communication networks?
15. Explain how a mobile user authenticates itself to the mobile network in the GSM networks?
16. Explain how each of a mobile user and the network authenticate themselves to each other in the third generation of cellular communication networks?
17. Explain the Security Weakness of the algorithm A5?
18. What is the fatal weakness of the AKA process of GSM system?