National University of Computer and Emerging Sciences, Lahore Campus

Course Name:	Network Security	Course Code:	CS 411
Degree Program:	BS CS	Semester:	Spring 2020
Exam Duration:	6 Hours	Total Marks:	40
Paper Date:	30 June 2020	Weight	40
Section:	A and B	Page(s):	
Exam Type:	Final Exam		

Important Instruction/ Notes:

1. Take Home Exam
2. All resources can be used to understand the concepts
3. Copy paste from any resource is **NOT** allowed
4. Paraphrasing from other resources is **NOT** allowed
5. Read and understand the questions carefully
6. Recommended time for each question is provided for your guidance
7. This exam has 2 questions. Q1 has 3 parts and Q2 has 2 parts.
8. When done, upload the solution in a SINGLE PDF file (preferably without using any compression) to SLATE Final Exam Folder or Google Classroom Final Exam Folder (only if SLATE is not working). Name the file as ID_Name_NS_FinalExam.
9. Send the same file as email attachment to umair.khan@nu.edu.pk and cc to yourself also. The subject line should read NS final exam – Student ID – Student Name
10. Follow all the rules set forth by the university to attempt the paper.
11. Write your name and ID on every page. Write page numbers on each page.

Consider the scenario where an airline provides internet access to its passengers. The devices held by the airplane passengers connect to one of several fixed routers aboard the airplane. The passengers can move inside the airplane and this may result in them connecting to different routers at different times. All the routers are connected to an onboard stationary server. Although stationary with respect to the routers, when in flight, it is mobile with respect to the satellites. This server connects to one of several satellites based on the signal strength of each satellite, bandwidth load on the satellites, service cost, ISP preferences etc. As the airplanes move in the air and the signal strength from the currently connected satellite grows weaker, connections with new satellites are negotiated. The satellites are stationary with respect to a place on the planet (a satellite above Lahore will always be above Lahore). All satellite are connected to a stationary ground station. The connection between a satellite and the ground station is not permanent and change due to weather conditions, load, etc. Therefore the satellite may have to find the best ground station to provide optimum service. Remember, a country's satellite should not connect to another country's ground station no matter how bad the situation is. Also consider that you do not have any computation resource restrictions.

Q1a. Develop a solution using diagrams such as 11.3, 12.1, 12.4, and 19.1 which ensures that (10 points)

- the message sent from the passenger in the airplane to any other person on the planet stays confidential (using e.g., symmetric or/and asymmetric encryption)
- the authenticity of the message can be verified (using e.g., hashes)

Q1b. Design a protocol using diagrams such as 18.7 and 18.8 which shows how (10 points)

- the passenger will connect to the one of the routers in the airplane
- the server in the airplane will connect to one of the satellites
- the satellite will connect to one of the ground stations

Consider that the server and the routers inside the airplane are stationary (with respect to each other) and permanently connected to each other by wire.

You will be graded on the diagram and justification of each technique you have chosen to include in your solution (why RSA? Why DES? Why AES? Why Timestamp? Why Discovery probe? Why Nonce? Why expiry? etc. This question does not require lengthy explanations: Diagrams and supporting justification would suffice. While answering Q1b, keep in mind establishing the connection, sustaining it, and terminating it.

Q1c. Consider that now there are severe computation resource restrictions. You are being asked to revise your solution from Q1a and Q1b such that the computation is reduced by 50% (halved) while keeping as much security as possible. How will you change your solution? Which previously used techniques will you drop? Do not rewrite the whole solution: just mention the major changes you will make. Provide justification for your choices. (5+5=10 points)

NOTE: While answering Q1a, b, and c, do not focus on network layers/protocol. Focus on how encryption/hashes will be used. And how the handshake will be performed or the session will be established/continued/terminated.

Q2a. Suppose you are being asked to develop a secure software development life cycle model. List (write names only) at least 20 secure software development activities that you feel should be part of such a process (categorize by phases). Justify you choice: 2-3 lines for each activity will be enough. Do not define the activity. Describe why you think it is important. (7 points)

Q2b. Suppose that your budget has been cut in half. Which of the secure software development activities will you remove/skip to meet this restriction? Why did you choose to remove these and not others? Discuss using 2-3 lines for each activity you have removed. (3 points)

MAXIMUM Recommended time distribution

Q1a – research 1 hour – writing 30 minutes

Q1b – research 1 hour – writing 30 minutes

Q1c – analysis 30 minutes – writing 15 minutes

Q2a – research 30 minutes – writing 30 minutes

Q2b – analysis 30 minutes – writing 15 minutes