INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD
FACULTY OF BASIC & APPLIED SCIENCES
DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

Online Terminal Examination Spring Semester 2021

Course Title:	**CS375 Information Security**	**Batch:**	**BSCS F18 (A & B) / BSIT F18**
Total Marks:	60	**Max Time Allowed:**	6 hours
Course Instructor:	Dr. Qaisar Javaid	**Date:**	22/6/2021

Instruction for Students:

Before starting your open book examination, please read all the given below instructions carefully, and must follow these instructions carefully.

1. Attempt all the questions by hand on white sheets.
2. ***If one or more answer(s)/part(s) of question of two or more students found the same, then marks of all the students will be marked zero, without considering who did by himself and who copied. So do not share your answer sheet even if it has been submitted by you.***
3. Total time allowed for ***solving 3 Hours*** and for ***uploading 3 Hours*** manage accordingly.
4. Download the file IS_Terminal-Answer.docx file (File attached in the Terminal Exam Activity in Google Classroom).
5. Type in your name and registration number on the first page of the word file in the space provided.
6. Take screens shots of the answer sheets.
7. Embed those screenshots in the file IS_Terminal-Answer.docx
8. Save the IS_Terminal-Answer.docx as pdf document.
9. Upload the IS_Terminal-Answer.pdf file on the link provided in the Google Classroom on the question paper. Submissions will only accepted in respective Google Form uploaded in Terminal Exam activity. ***No submissions will be accepted on personal emails, Google Classrooms, WhatsApp or any other social network***.
10. Make sure you have **2** pages in question paper including this one.
11. No extra time will be awarded for uploading answer-booklet manage accordingly.

Question 1 [15 points]

Consider an e-commerce company, where customers connect to the company web site over Internet and provide a user name and password for a private account that is used later for placing orders. Users have to choose their own passwords for the account. Assume that you are the security consultant for the company and are tasked to determine the password selection criteria for these customer accounts. In this regard, you can consider the relative effectiveness of longer versus short passwords, enforcing randomness of password characters compared to permitting the users to choose any characters they like, and whether forcing password changes every six months is a good idea.

Briefly discuss (about half a page) the advantages/disadvantages of these password selection schemes to help in deciding the password selection criteria.

Question 2 [15 points]

Consider two networks, each with its own DNS server running. A host on one network wants to get certain information from a specific site on the Internet. Using DNS spoofing, how can the hacker intercept the host's communication with the site? Give step by step procedure for the following scenarios:-

a. When the hacker and the host are both on the same network?

b. Describe two ways the hacker may carry out DNS spoofing if the host and the hacker are on separate networks.

Question 3 [15 points]

Compare Block and Stream ciphers from the following aspects (not more than 3-4 lines for each):

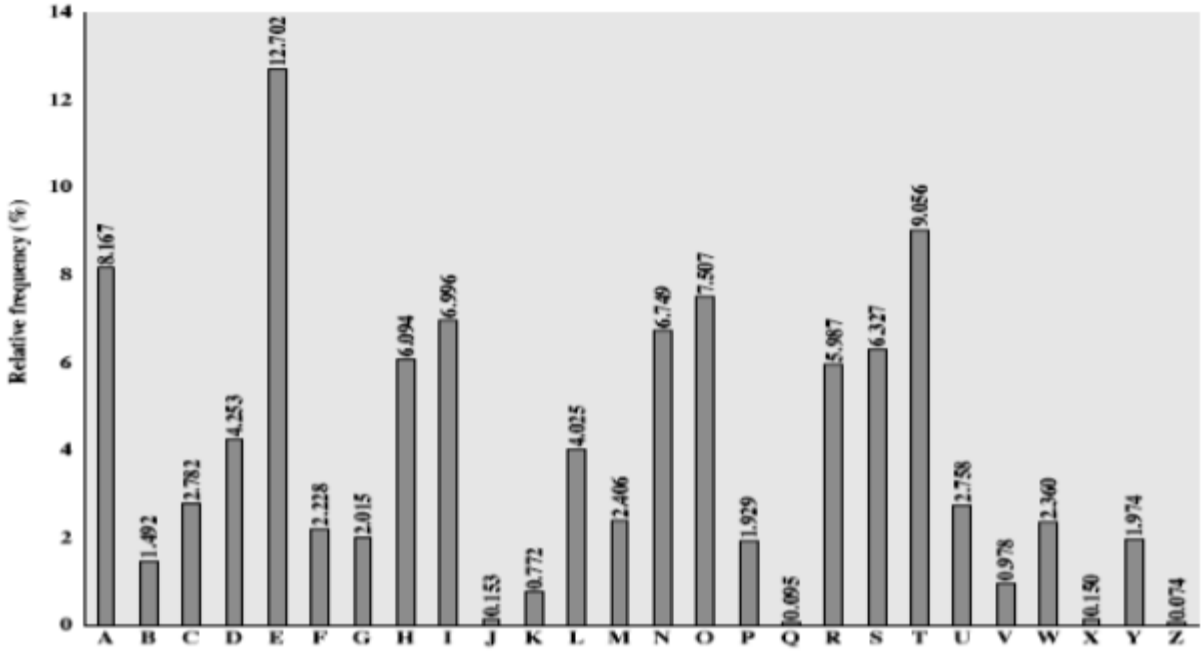
- Diffusion
- Immunity to malicious insertions
- Error propagation
- Encryption speed

Question 4 [15 points]

Decrypt the following encrypted quotation. Justify your answer by describing the steps followed along with the results of those tests (please avoid unnecessary details).

fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc

NOTE: Blank spaces in the cipher text are only there to enhance legibility; they are to be ignored while decryption. The plaintext obtained will have no blank spaces and appropriate ones would need to be inserted on inspection.



Good Luck ☺