Number of pages	2
Number of questions	5

UNIVERSITY OF SRI JAYEWARDENEPURA
Faculty of Technology
Bachelor of Information and Communication Technology Honours Degree
Third Year Second Semester End Examination

ITC3093 Computer Security

June 2022

Time allowed: Three (03) Hours **Answer ALL questions**

Question 01

Total marks 20

1 a. Briefly explain the CIA security triad. [4 marks]

b. Write a short note on the following terms. [6 marks]

i. Threat

ii. Vulnerability

iii. Attack

c. Distinguish between amateur criminals, crackers and career criminals in the computer security domain. [5 marks]

d. Do you think attempting to break into (that is, obtain access to or use of) a computing system publicly accessible should be illegal? Justify your answer. [5 marks]

Question 02

Total marks 20

2 a. List down five (5) major objectives of information security. [4 marks]

b. Distinguish the following entities. [6 marks]

1. Cryptography vs Cryptology
2. Active vs Passive Attacks

c. Briefly explain why data encryption is important in data communication. [5 marks]

d. What weaknesses of private key cryptography can be addressed by public key cryptography? [5 marks]

Question 03

Total marks 20

3 a. What is the difference between stream cipher and block cipher? [5 marks]

b. Calculate the number of *private keys* needed if six (6) users are communicating with each other. [5 marks]

c. Explain the public key encryption process with the support of a suitable diagram. [5 marks]

d. Briefly explain the digital signature generation process starting from the public key with the support of an illustration. [5 marks]

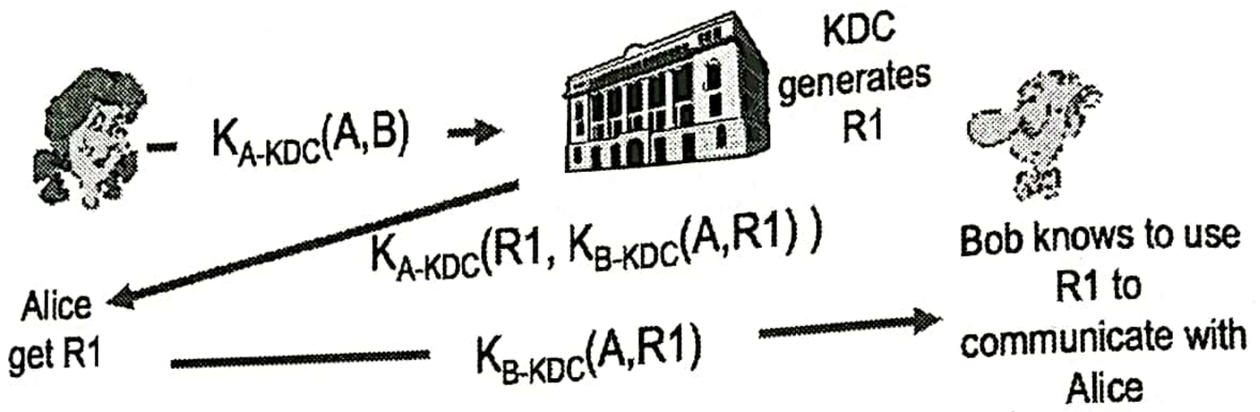
Total marks 20

Question 04

4. a. List down four (4) major characteristics of a Hash function. [4 marks]

b. Briefly explain the role of a Certificate Authority (CA). [6 marks]

c. Answer the questions given based on the key distribution process explained in the figure. [10 marks]



I. Which cryptography algorithm family uses the above key distribution method?
II. Briefly explain the usage of *R1*.
III. Briefly explain what is meant by $K_{A\text{-}KDC}(R1, {}_{KB\text{-}KDC}(A,R1))$.
IV. State an advantage and a weakness of this approach compared to the other counterpart approaches.
V. Briefly state the reason why Man in the Middle (MIM) approaches are not successful in the above scenario.

Question 05

Total marks 20

5. a. Compare and contrast *viruses* and *worms* in the computer malware domain. [5 marks]

b. What measures can be taken to protect your computer from malware and attacks? [5 marks]

c. Some encryption algorithms are theoretically breakable but practically unbreakable. Do you agree with this statement? Justify your answer. [5 marks]

d. Putty is a popular SSH client. A screenshot of the Putty download section of the website is given below. Briefly explain the usage of cryptographic checksums given. [5 marks]

MSI ('Windows Installer')

64-bit x86:	putty-64bit-0.77-installer.msi	(or by FTP)	(signature)
64-bit Arm:	putty-arm64-0.77-installer.msi	(or by FTP)	(signature)

Cryptographic checksums for all the above files

MD5:	md5sums	(or by FTP)	(signature)
SHA-1:	sha1sums	(or by FTP)	(signature)
SHA-256:	sha256sums	(or by FTP)	(signature)
SHA-512:	sha512sums	(or by FTP)	(signature)