LAIKIPIA UNIVERSITY

UNIVERSITY EXAMINATIONS

SECOND SEMESTER 2023/2024 ACADEMIC YEAR

THIRD YEAR EXAMINATION FOR THE DEGREE OF BACHELOR OF COMPUTER SCIENCE

COMP 322/BICT 325: COMPUTER SYSTEMS SECURITY

STREAM: R ***TIME: 2 HRS***

DAY: WEDNESDAY [11.30A.M – 1.30 P.M] ***DATE: 17/04/2024***

THIS QUESTION PAPER CONSISTS OF FOUR (4) PAGES

PLEASE DO NOT OPEN UNTIL THE INVIGILATOR SAYS SO.

INSTRUCTIONS: Answer Question ONE and any TWO other questions

QUESTION ONE (Compulsory) (30Marks)

a. Define the term'computer security'. [1mark]

b. What are the fundamental principles of computer security? Explain each one briefly. **[3 marks]**

c. Define encryption and why it is essential in computer security. **[2 marks]**

d. What is cryptography,and how is it used as a security tool? **[2 marks]**

e. What is meant by identification, authentication, and authorisation in computer security? **[3 marks]**

f. What is a message digest, and how is it applied to information schemes and digital signatures? **[2 marks]**

g. What is secret sharing? Discuss a case where secret sharing was used as a method of authentication. Was it effective?? **[2 marks]**

h. What is risk management in the context of computer security? **[2 marks]**

i. Describe the information audit planning process and how to produce effective audit programs. **[3 marks]**

j. Discuss the impact of auditing in the development of a secure system. **[3 marks]**

k. Explain the concepts of data forensics, evidence security ,and preservation **[3 marks]**

l. You have discovered an unknown file format during a data forensic investigation. Discuss potential methods to analyse this file. [**3 marks]**

QUESTION TWO (20 MARKS)

a. You have been tasked with conducting an information audit for your organisation. What are the first steps you would take in the planning process? [**2 marks]**

b. Explain how you would identify the information needs of your organization as part of the information audit planning process. **[3 marks]**

c. How would you assess the information available in your organisation during an information audit? **[2 marks]**

d. What strategies would you use to ensure resources are efficiently utilised during an information audit? **[3 marks]**

e. You have conducted an information audit and identified a gap in the information available in your organisation. How would you address this gap? [**2 marks]**

f. Explain the role of risk management in the information audit planning process. **[3 marks]**

g. What is the role of the systems that produce information in an information audit? How would you evaluate these systems? **[3 marks]**

h. How would you evaluate the controls that protect the systems that produce

QUESTION THREE (20 MARKS)

a) Explain the concept of"confidentiality"incryptography. **[1 mark]**

b) Describe the Diffie-Hellman key exchange protocol and explain its significance in secure communication. **[3 marks]**

c) What is a "man-in-the-middle" attack? How can it be prevented in a cryptographic communication? **[3 marks]**

d) Explain the concept of"integrity"incryptography and how it is maintained. **[2 marks]**

e) Discuss the Advanced Encryption Standard (AES) and its role in modern cryptography. **[3 marks]**

f) What is a "brute force" attack in the context of cryptography? Discuss potential countermeasures. **[3 marks]**

g) Explain the concept of "non-repudiation" in cryptography and how it is ensured. **[2 marks]**

h) Discuss the Elliptic Curve Cryptography (ECC) and compare it with RSA regarding security and performance. **[3 marks]**

QUESTION FOUR (20 MARKS)

a) Define the term'computer security threat'. **[1 mark]**

b) Explain what a 'malware' is. Discuss its different forms, such as viruses, worms,and trojans. **[4 marks]**

c) What is 'phishing'? How can individuals and organisations protect themselves from phishing attacks? **[3marks]**

d) Discuss the concept of 'Denial of Service (DoS)' attacks. How do they affect

computer systems and networks? **[2 marks]**

e) What is 'ransomware'? Discuss a recent example of a major ransomware attack. **[2 marks]**

f) Explain the term 'social engineering'. How does it pose a threat to computer security? **[2 marks]**

g) Whatis'spyware'?How can it be detected and removed? **[2 marks]**

h) What is 'data leakage'? Discuss preventive measures that can be taken to avoid data leakage. **[2 marks]**

i) Explain the concept of 'zero-day exploits'. Why are they particularly dangerous? [**2 marks]**

QUESTION FIVE (20MARKS)

a) Your organisation has recently experienced a data breach. As a security officer, how would you revisetheexistingsecuritypoliciestopreventsuchincidentsinthefuture? **[3 marks]**

b) You have been tasked with developing a new security policy for your organisation. What key elements would you include in this policy and why? **[3 marks]**

c) A small business has never had a formal security policy and has just experienced a minor security incident. How would you convince management of the importance of having a form al security policy? **[2 marks]**

d) Your organisation is planning to migrate its data to the cloud. What risks are associated with this migration,and how would you manage them? **[3 marks]**

e) You have identified a potential risk to your organisation's data security. How would you a sess the impact of this risk,and what steps would you take to mitigate it? [**3 marks]**

f) Your organisation has a well-defined security policy, but employees do not adhere to it. How would you address this issue? [**2 marks]**

g) A new regulation in your industry requires a specific security control that is not currently part of your organisation's security policy. How would you update the policy to comply with this regulation? **[2 marks]**

h) You have been asked to conduct a risk assessment for your organization. Describe the process you would follow. **[2 marks]**