JARAMOGI OGINGA ODINGA UNIVERSITY OF

SCIENCE AND TECHNOLOGY

END SEMESTER EXAMINATION

BSC. COMPUTER SECURITY & FORENSICS YEAR THREE SEMESTER TWO

[2020/2021]

RESIT/SPECIAL

PAPER: IIT 3323 [INFORMATION SYSTEMS CONTROL AND AUDIT]

INSTRUCTIONS

1. This paper contains FIVE questions. Question One is 30 Marks and the rest are 20 Marks each.
2. Answer question one which is **COMPULSORY** and **ANY OTHER TWO**
3. Be precise and clear in your answers.

QUESTION ONE [30 MARKS]

1. Define a certificate authority**(1mark)**
2. Give at least three reasons why using passwords alone is a poor security mechanism? **(3marks).**
3. State three examples of deterrent access control. **(3marks)**
4. From your opinion what are the drawbacks to installing intrusion detection and monitoring systems **(3marks)**
5. For a subject to access a resource what are some of the conditions that should be met? **(4marks)**
6. What are the importance associated with audit logs within an information system **(3marks)**
7. **What is cryptography? (2marks)**
8. **Distinguish between Link and End-to-End Encryption(4marks)**
9. What do you understand by the term countermeasure; state at least 4 forms a countermeasure can take. (**4marks)**
10. What are the three objectives of information systems security (**3 marks)**

QUESTION TWO [20 MARKS]

a) Describe what you understand by the term Access in relation to security? **(2mark)**

b) Describe a "subject" and "Object" in terms of access and controls **(2marks)**

c) Describe the elements of the CIA Triad? **(6 mark)**

d) Describe the four types of access control **(8 marks)**

e) Describe a Type 2 authentication factor? **(2marks)**

QUESTION THREE [20 MARKS]

1. Briefly elaborate on the following in terms of access control attacks **(6marks)**

    - Denial of service
    - Spoofing
    - Dictionary attack
    - Brute force
    - wardialing.
    - Session hijacking

2. Distinguish between *Compliance* and *substantive* testing in Information System Audit **(4marks)**
3. State five objectives of Information Systems Audits? **(5marks)**
4. What are the inherent Needs for auditing an information system? **(5marks)**

QUESTION FOUR [20 MARKS]

1. State the processes involved in SSL connection setup **(9marks)**
2. What is a Secure Electronic Transaction **(SET) (1mark)**
3. State and Explain the roles of the five players involved in SET **(10 marks)**

QUESTION FIVE [20 MARKS]

1. Access control can be administered in two main ways: centralized and decentralized state two examples of each **(2marks)**
2. With relevant examples briefly elaborate on two administrative, physical and technical controls **(6 marks)**
3. Explain at least six attacks on a cryptosystems **(12 marks)**