JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

EXAMINATION FOR THE DEGREE OF MASTERS OF IT SECURITY & AUDIT

2ND YEAR 1ST SEMESTER 2016/2017 ACADEMIC YEAR

KISUMU LEARNING CENTER

COURSE CODE: IIT 5212

COURSE TITLE: ADVANCED INFORMATION SYSTEMS AUDIT AND CONTROL

EXAM VENUE: **STREAM: IT SECURITY & AUDIT**

DATE: **EXAM SESSION: 3 HOURS**

TIME:

INSTRUCTIONS

1. **Answer ANY THREE questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION 1 [20 MARKS]

a) Define the following terms and give two examples of each
   i) Symmetric encryption. **(3 marks)**
   ii) Asymmetric encryption **(3 marks)**
   iii) Hashing **(3 marks)**

b) Identify common applications of cryptography used to secure **(6 marks)**
   i. Electronic mail
   ii. Web activity
   iii. Networking

c) Several criteria exist for evaluating computer security systems. The earliest, TCSEC, also called the Orange Book provides a criteria to evaluate the functionality and assurance of a systems security components. Identify these components. **(5 marks)**

d) Briefly discuss the following five security models. **(10 marks)**
   i) Information flow model
   ii) Noninterference model
   iii) Take-Grant model
   iv) Bell-LaPadula
   v) Biba and Clark-Wilson

QUESTION 2 [20 MARKS]

ISACA develops and maintains the internationally recognized COBIT framework, helping IT professionals and enterprise leaders fulfill their IT Governance responsibilities while delivering value to the business. COBIT framework has evolved over the years beginning with COBIT 1 for audit in 1996 to the current COBIT 5 developed in 2012. COBI 5 is aimed at providing an end-t0-end business view of the governance of enterprise IT.

a) Write COBIT and ISACA in full. Why are they important to an IT security professional? **(5 marks)**

b) Briefly discuss the five key principles of COBIT 5 **(15 marks)**

QUESTION 3 [20 MARKS]

In the article "Six Strategies for Defense-in-Depth: Securing the Network from Inside Out", Snyder argues that Defense-in-depth is a dramatic departure from the transparent data corridor of the LAN. By pushing security into the network itself, the LAN changes from a public-access highway to a high security network of roads, serving gated communities. Adding security into the LAN requires considering and implementing three key attributes of secure networking:

a) Identify three key attributes of secure networking **(2 marks)**

b) Briefly discuss ***six strategies***. In your discussion include the problem, challenges and solutions **(18 marks)**

QUESTION 4 [20 MARKS]

Jerry Shenk, a senior analyst for the SANS Institute and is senior security analyst for Windstream Communications, argues that There is no such thing as a silver bullet, that is , a single product that will solve a company's security problems and it takes many technologies and processes. The author therefore advocates for provision of layered security. The term layered security describes a defensive strategy featuring multiple defensive layers that are designed to slow down an attacker. The military calls this deep defense or defense in depth. The goal is slowing an attack and causing enemy casualties. Discuss in detail the **six layered approach** to security articulated by this author. **(20 marks)**

QUESTION 5 [20 MARKS]

You are a recent graduate in MS IT Security and Audit from JOOUST. You have received an invitation to speak to a conference of the leading top business organization in Kenya on the topic Critical Security Controls for Effective Cyber Defense. You are quire nervous on what to share with the attendees for the 15 min time slot allocated to you. You recall an article by Shenk (2013) that contained information about **20 critical security controls for effective cyber defense**. Identify these twenty critical security controls for effective cyber defense. **(20 marks)**