MURANG'A UNIVERSITY OF TECHNOLOGY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOCY

DEPARTMENT OF INFORMATION TECHNLOGY

UNIVERSITY ORDINARY EXAMINATION

2018/2019 ACADEMIC YEAR

THIRD YEAR **FIRST** SEMESTER EXAMINATION FOR, BACHELOR OF BUSINESS INFORMATION TECHNOLOGY

CCS 303 – ELECTRONIC ACCESS CONTROL

DURATION: 2 HOURS

DATE: 19/12/2018

TIME: 9 – 11 A.M.

Instructions to candidates:

1. Answer question One and Any Other Two questions.
2. Mobile phones are not allowed in the examination room.
3. You are not allowed to write on this examination question paper.

SECTION A: ANSWER ALL QUESTIONS IN THIS SECTION

QUESTION ONE (30 MARKS)

a) Your company has just opened a call centre in Kenya to handle nighttime operations and you are asked to review the site's security controls. Specifically you are asked which is the strongest form of authentication and why. (5 marks)

b) Define the following terms
   i. Honey pot
   ii. Challenge response
   iii. Computer worm
   iv. End to end encryption

c) Explain how public key cryptography may be used for identification (5 marks)

d) In general there are three types of identity authentication tasks. List three tasks (6 marks)

e) Provide an example each for preventive, detective and corrective controls for each category people, technology and operations (4 marks)

f) Differentiate between honey pot and network sniffers (3 marks)

g) State and explain the elements of CIA Triad (3 marks)

SECTION B – ANSWER ANY TWO QUESTIONS IN THIS SECTION

QUESTION TWO (20 MARKS)

a) Describe about discretionary access and mandatory access control with examples (5 marks)

b) As a newly appointed security officer for your corporation you suggest replacing the password based authentication system with RSA tokens. Elsa your chief technology officer denies your request citing budgetary constraints. As a temporary solution, Elsa asks that you find ways to increase password security. Discuss five ways of accomplishing this (10 marks)

c) Today you are meeting with a coworker who is proposing that the numbers of logins and password be reduced. Another coworker has suggested that you investigate single sign on technologies and make a recommendation at the next scheduled meeting. Discuss the SSO technologies that can be used and why (5 marks)

QUESTION THREE (20 MARKS)

a) You have been promoted to security officer for fortune 500 company and are performing an audit of elevated privileges for the network. You observe that there are many members from the help desk that have privileges to various systems that do not require doing their job on a daily basis. What best business practice does your company lack and how do you eliminate this. (8 marks)

b) In the table provide an example of some types and categories of access control complete the table below (6 marks)

Attributes	**Deterrent**	**Preventive**	**Detective**	**Corrective**
Administrative			Audit policy	
Technical		ACLS		
Physical				Fire Extinguisher

Attributes	**Recovery**	**Compensating**
Administrative	Incident Response Plan	
Technical		
Physical		Defense in depth

c) During a weekly staff meeting, your boss reveals that some employees have been reveals other employees have been allowing other employees to use their password. He is determined to put and stop to this and you want you install biometric access control systems. He has asked about some basics attributes such as Type I errors, Type II errors and the CER , what is so important about CER and how do you respond. (6 marks)

QUESTION FOUR (20 MARKS)

a) Consider a computer system where the components are:
Users: John (J) and Peter (P)
Resources are files1, file 2 and file 3
Access modes are read(r), write (w) and execute (x)
The access Policy P is given as where all access modes are permission
P={(J,f1,r),(J,f1,x),(J,f1,w),(J,f2,r),(J,f3,r),(P,f1,r),(P,f1,w),(P,f1,x),(P,f2,w),(P,f2,x),(P,f3,x),(J,f3,w)}
Show the access control matrix that represents P (15 marks)

b) It is important to guard against two problems related to access control, excessive privilege and creeping privilege. Give a detailed description of the two. (5 marks)