

## JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY SCHOOL INFORMATICS AND INNOVATIVE SYSTEMS UNIVERSITY EXAMINATION FOR THE DIPLOMA IN LINUX ENGINEERING $2^{\rm ND}$ YEAR $1^{\rm ST}$ SEMESTER 2013/2014 ACADEMIC YEAR

**CENTRE: KISUMU** 

**COURSE CODE: ICT 2214** 

COURSE TITLE: FUNDAMENTAL OF IT SECURITY ENGINEERING

EXAM VENUE: AH STREAM: Dip. Linux Engineering

DATE: 5/12/2013 EXAM SESSION: 9.00 – 10.30 AM

TIME: 1½ HOURS

## **Instructions:**

- 1. Answer question 1 (Compulsory) and ANY other 2 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**

c) Explain the two main types of firewalls: Packet Filters and Application Gateways . (4 marks) d) State any 3 Types of protections provided by firewalls e) List any four importance of backups (4 marks) f) Which three backup policies would you implement as a systems security manager (3 marks)  Question 2  a) Define each of the following terms with respect to information security. i. Cryptology ii. Encryption iii. Cipher text b) Distinguish between Symmetric and Asymmetric cryptographic methods. (4 marks) c) For each of the following cryptographic algorithms, classify as Symmetric or Asymmetric i. DES ii) RSA iii) ECC iv)RC4 (4 marks) d) State any three advantages of using digital signatures e) What are the key components of Public Key Infrastructure? (3 marks) Question 3  a) Explain each of the following terms as far as security of information systems is concerned. i. Target System ii. Risk iii. Risk Management iv. Risk Appetite	a)	Giving reasons, list any four security policies you would implement as a system security manager.	ems (4 marks)		
d) State any 3 Types of protections provided by firewalls e) List any four importance of backups  (4 marks)  (5) Which three backup policies would you implement as a systems security manager. (6 marks)  (7) Which three backup policies would you implement as a systems security manager. (8 marks)  (9) Uestion 2  (9) Define each of the following terms with respect to information security. (9) List incryption (10) List incryption (11) Cipher text (12) Distinguish between Symmetric and Asymmetric cryptographic methods. (13) Cyptographic algorithms, classify as Symmetric or Asymmetric (14) List in the following cryptographic algorithms, classify as Symmetric or Asymmetric (15) List in the following cryptographic algorithms, classify as Symmetric or Asymmetric (16) List in the following terms as far asymmetric cryptographic methods. (17) Agymmetric or Asymmetric or Asymmetric or Asymmetric in DES (18) RSA (19) ECC (19) RC4 (19) Amarks (19) State any three advantages of using digital signatures (19) amarks (19) What are the key components of Public Key Infrastructure? (19) Amarks (19) Question 3  (20) Explain each of the following terms as far as security of information systems is concerned. (10) Cymmetric in the following terms as far as security of information systems is concerned. (10) Cymmetric in the following terms as far as security of information systems is concerned. (17) Cymmetric in the following terms as far as security of information systems is concerned. (18) Cymmetric in the following terms as far as security of information systems is concerned. (18) Cymmetric in the following terms as far as security of information systems is concerned. (18) Cymmetric in the following terms as far as security of information systems is concerned. (18) Cymmetric in the following terms as far as security of information systems in the following terms as far as security of information systems in the following terms as far as security of information systems in the following terms as far as security of information systems in t	b)	What is a firewall?	(2 marks)		
e) List any four importance of backups (4 marks  f) Which three backup policies would you implement as a systems security manager.  (3 marks  Question 2  a) Define each of the following terms with respect to information security.  (6 marks  i. Cryptology  ii. Encryption  iii. Cipher text  b) Distinguish between Symmetric and Asymmetric cryptographic methods. (4 marks)  C) For each of the following cryptographic algorithms, classify as Symmetric or Asymmetric  i. DES  ii) RSA  iii) ECC  iv)RC4  (4 marks  (3 marks)  Question 3  a) Explain each of the following terms as far as security of information systems is concerned.  i. Target System  ii. Risk  iii. Risk Management  iv. Risk Appetite	c)	Explain the two main types of firewalls: Packet Filters and Application Gates .	ways . (4 marks)		
Question 2  a) Define each of the following terms with respect to information security.  i. Cryptology ii. Encryption iii. Cipher text  b) Distinguish between Symmetric and Asymmetric cryptographic methods. (4 marks)  c) For each of the following cryptographic algorithms, classify as Symmetric or Asymmetric  i. DES ii) RSA iii) ECC iv)RC4 (4 marks) d) State any three advantages of using digital signatures (3 marks) what are the key components of Public Key Infrastructure?  Question 3  a) Explain each of the following terms as far as security of information systems is concerned.  i. Target System ii. Risk iii. Risk Management iv. Risk Appetite			(3 marks) (4 marks)		
a) Define each of the following terms with respect to information security.  i. Cryptology ii. Encryption iii. Cipher text b) Distinguish between Symmetric and Asymmetric cryptographic methods. (4 marks) c) For each of the following cryptographic algorithms, classify as Symmetric or Asymmetric i. DES ii) RSA iii) ECC iv)RC4 (4 marks) d) State any three advantages of using digital signatures e) What are the key components of Public Key Infrastructure?  Question 3  a) Explain each of the following terms as far as security of information systems is concerned.  i. Target System ii. Risk iii. Risk Management iv. Risk Appetite	f)	Which three backup policies would you implement as a systems security man.	ager. (3 marks)		
<ul> <li>i. Cryptology ii. Encryption iii. Cipher text</li> <li>b) Distinguish between Symmetric and Asymmetric cryptographic methods. (4 mark)</li> <li>c) For each of the following cryptographic algorithms, classify as Symmetric or Asymmetric  i. DES ii) RSA iii) ECC iv)RC4 (4 mark)</li> <li>d) State any three advantages of using digital signatures (3 mark)</li> <li>e) What are the key components of Public Key Infrastructure? (3 mark)</li> <li>Question 3</li> <li>a) Explain each of the following terms as far as security of information systems is concerned. (8 mark) i. Target System ii. Risk iii. Risk Management iv. Risk Appetite</li> </ul>	Question 2				
b) Distinguish between Symmetric and Asymmetric cryptographic methods. (4 marks) c) For each of the following cryptographic algorithms, classify as Symmetric or Asymmetric  i. DES ii) RSA iii) ECC iv)RC4 (4 marks) d) State any three advantages of using digital signatures (3 marks) e) What are the key components of Public Key Infrastructure? (3 marks)  Question 3  a) Explain each of the following terms as far as security of information systems is concerned.  i. Target System ii. Risk iii. Risk Management iv. Risk Appetite	a)	<ul><li>i. Cryptology</li><li>ii. Encryption</li></ul>	(6 marks)		
Asymmetric  i. DES ii) RSA iii) ECC iv)RC4 (4 marks) d) State any three advantages of using digital signatures (3 marks) e) What are the key components of Public Key Infrastructure? (3 marks)  Question 3  a) Explain each of the following terms as far as security of information systems is concerned. (8 marks)  i. Target System  ii. Risk  iii. Risk Management  iv. Risk Appetite	b)	<u>.</u>	(4 marks)		
d) State any three advantages of using digital signatures (3 marks e) What are the key components of Public Key Infrastructure?  (3 marks	c)				
e) What are the key components of Public Key Infrastructure? (3 marks)  Question 3  a) Explain each of the following terms as far as security of information systems is concerned. (8 marks)  i. Target System  ii. Risk iii. Risk Management iv. Risk Appetite			(4 marks)		
Question 3  a) Explain each of the following terms as far as security of information systems is concerned.  i. Target System  ii. Risk  iii. Risk Management  iv. Risk Appetite		·	(3 marks)		
<ul> <li>a) Explain each of the following terms as far as security of information systems is concerned. <ol> <li>Target System</li> <li>Risk</li> <li>Risk Management</li> <li>Risk Appetite</li> </ol> </li> </ul>	e)	what are the key components of Public Key Infrastructure?	(3 marks)		
concerned.  i. Target System  ii. Risk  iii. Risk Management  iv. Risk Appetite	Question 3				
	a)	concerned.  i. Target System  ii. Risk iii. Risk Management	is (8 marks)		
	b)		(2 marks)		

	<ul> <li>i. Access and Authorization</li> <li>ii. Logs and Trails</li> <li>iii. Risk-based Audit</li> <li>d) What sre the four main steps of risk assessment in security strategy flowch</li> <li>e) List any 3 factors that may cause changes in risk.</li> </ul>	art. (4 marks) (3 marks)
Quest	ion 4	
a)	Stating core functions of each, Discuss the five functional layers of security Ma	nagement (10 marks)
b)	State any four design goals of using the layered functional architecture in design security Management Systems.	gning (4 marks)
b)	Define clearly the six basic security services defined by the ISO.	(6 marks)
Quest	ion 5 (20 Marks)	
	a) Differentiate between SSL and Kerberos Authentication.	(4 marks)
	b) State any four threats to network components with their possible consequent	
	c) State and explain the three main goals on network security.	(6 marks) (6 marks)
	<ul><li>d) What is eavesdropping?</li><li>e) Give any three implementations that would counter eavesdropping.</li></ul>	(1 mark) (3 marks)

c) Explain each of the following components of Control Systems.

(3 marks)