

**W1-2-60-1-6**

## JOMO KENYATTA UNIVERSITY

**OF**

**AGRICULTURE AND TECHNOLOGY**

# University Examinations 2014/2015

**FOURTH YEAR FIRST SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY**

**BIT 2411 : COMPUTER SECURITY AND CRYPTOGRAPHY**

**DATE: APRIL 2015 TIME: 2 HOURS**

**INSTRUCTIONS: ANSWER QUESTION ONE (COMPULSORY) AND**

**ANY OTHER TWO QUESTIONS.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**QUESTION ONE (30 MARKS)**

(a) Differentiate between an information security risk and threat.

[2 marks]

(b) What is a hashing algorithm used for? [2 marks]

(c) Describe two different techniques that prevent viruses from being detected by antivirus software (even an up to date one). [3 marks]

(d) Usual authentication systems verify passwords with the help of their hashes stored in protected files. What is the purpose of storing hashes rather than the passwords themselves? [2 marks]

(e) Give an example for authentication of something you know and something you have. [2 marks]

(f) Differentiate between symmetric and asymmetric encryption techniques. [2 marks]

(g) Use the Euclidean algorithm to show that the gcd (60, 24) = 12.

[3 marks]

(h) Describe a method you can use to enforce integrity for data in motion or being transmitted from one point to another on the hostile internet. [3 marks]

(i) Explain the following terms as used in information security:

1. Policy. [3 marks]
2. Issue specific standard. [2 marks]
3. System specific standard. [2 marks]

(j) Explain the computation rules for: [4 marks]

1. a + b mod m
2. a\*b mod m

**QUESTION TWO (20 MARKS)**

(a) Explain the security features of a trusted operating system.

[10 marks]

(b) Describe the best approach a security manager can use to perform a risk assessment on critical business applications to protect organizational databases and applications. [10 marks]

**QUESTION THREE (20 MARKS)**

Draw a network diagram and indicate each of the following components on the network and the function of each component:

(a) Firewall (TUM firewall)

(b) Unknown network.

(c) Untrusted network.

(d) Public internet servers.

(e) Internal network.

(f) Internal and external router.

(g) Outermost perimeter (DMZ) and internal perimeter.

[20 marks]

**QUESTION FOUR (20 MARKS)**

(a) Explain the following terms as used for access control to a database:

1. Object. [2 marks]
2. Subject. [2 marks]
3. Access right. [2 marks]

(b) Explain one advantage and disadvantage of supporting different granularity levels on a database. [4 marks]

(c) Explain the following database access control policies. Use diagrams where possible:

1. Discretionary Access Control (DAG). [4 marks]
2. Mandatory Access Control (MAC). [4 marks]
3. Role-Based Access Control (RBAG). [4 marks]

**QUESTION FIVE (20 MARKS)**

(a) You want to send a message M = 13 to Alice. Using Alice’s public and private keys, calculate the ciphertext C, and the value for R when Alice recovers the message. [10 marks]

(b) Dexter wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e = 283. Find d so that ed has a remainder of 1 when divided by (p-1) (q-1). [10 marks]