

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

**JOMO KENYATTA UNIVERSITY**

**OF**

**AGRICULTURE AND TECHNOLOGY**

**UNIVERSITY EXAMINATIONS 2014/2015**

**YEAR 4 SEMESTER I EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY**

**ICS 2411: COMPUTER SECURITY AND CRYPTOGRAPHY**

**DATE: AUGUST 2015 TIME: 2 HOURS**

**INSTRUCTIONS: Answer Question One (Compulsory) and Any Other Two Questions**

**QUESTION ONE (30 MARKS)**

1. Explain the following terms as applied in computer security: (4marks)
2. Interruption
3. Interception
4. Modification
5. Fabrication
6. Explain how information in an access log could be used to identify the true identity of an imposter who has acquired unauthorized access to a computing system. (6marks)
7. Differentiate between Transposition and Substitution ciphers. Give an example of each. (6marks)
8. Explain what is meant by CIA of information security. (3marks)
9. List three controls that could be applied to detect or prevent salami attacks. (3marks)
10. Using diagrams show the difference between asymmetric and symmetric systems. (4marks)
11. By use of a columnar transposition, encrypt the following message. Indicate clearly how you arrived at the answer.

“MOST STUDENTS APPLAUD NEWS THAT THERE IS NO LECTURE THAT DAY”. (4marks)

**QUESTION TWO (20 Marks)**

1. Discuss three areas where cryptography is regularly used. Show how cryptography is used. (6marks)
2. With illustrations, differentiate the following:
3. Cipher text and Plain text
4. Symmetric and asymmetric
5. ACL and Capability (6marks)
6. Discuss four types of security threats to a computer system (8marks)

**QUESTION THREE (20 Marks)**

1. If A=5, B=7, and C=2, evaluate;
2. B mod A,
3. A-1 mod C (4marks)
4. Briefly but clearly, explain the following
5. Cipher text only attack
6. Known plaintext only attack
7. Chosen-cipher text attack (6marks)
8. Describe any two models for evaluating security. (10marks)

**QUESTION FOUR (20 Marks)**

You are the manager in charge of Network security in your company. Discuss the measures you would undertake/implement to:

1. Ensure the system is secure from internal and external forces
2. Detect any intrusion
3. Avoid/prevent DOS
4. Limit user Access Control (20marks)

**QUESTION FIVE (20 Marks)**

The full spectrum of security embraces several phrases:

* Prevention
* Detection
* Recovery

And several elements:

* Architecture
* Policy and education
* Risk management
* Liability management
* Technical defense
* Operational defense

Pick any five of the above and discuss how they relate to systems security. (20marks)