**MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**P.O. Box 972-60200 – Meru-Kenya**

**Tel: 020-2069349, 061-2309217. 064-30320 Cell phone: +254 712524293, +254 789151411**

**Fax: 064-30321**

**Website:** [**www.must.ac.ke**](http://www.must.ac.ke) **Email:** **info@must.ac.ke**

**University Examinations 2016/2017**

FOURTH YEAR FIRST SEMESTER EXAMINATION FOR THE DEGREE OF

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY AND BACHELOR OF BUSINESS INFORMATION TECHNOLOGY

**CCS 3475: COMPUTER SECURITY AND CRYPTOGRAPHY**

**DATE: DECEMBER 2016 TIME: 2 HOURS**

**INSTRUCTIONS:** *Answer question* ***one*** *and any other* ***two***questions.

**QUESTION ONE (30 MARKS)**

1. Using Playfair matrix encrypt this message: I Must see you over Cadogan West. Coming at once. Use “University” as the key word (10 marks)
2. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher (4 marks)
3. If the keyword is WIND and the plaintext is GO AHEAD MAKE MY DAY, use Vigen’ere Cipher to find the ciphertext (4 marks)
4. Within the context of any application-to-application communication, there are some specific securities requirements including,
* Authentication
* Confidentiality
* Integrity

Explain briefly each of these terms showing these can be addressed. (12 marks)

**QUESTION TWO (20 MARKS)**

1. Using rail fence Decipher the text MKHSE LWYAE ATSOL (5 marks)
2. Encipher ITS COL with E(x)=(5x+8) MOD 26. (5 marks)
3. What are the essential ingredients of a symmetric cipher (5 marks)
4. Discuss using a diagram the concept of symmetric cipher model (5 marks)

**QUESTION THREE (20 MARKS)**

1. Computer Operating Systems from the first line of defense in a computer system. Discuss three ways you as a user can use computer Operating System to guard your application in a computer (6 marks)
2. Draw a diagram to show your understanding of ***Public Key Encryption***  (4 marks)
3. If the keyword is NUMBER and the plaintext is GBATI NUIOB RTBOZ UEEQN TPWVJ BADEE G, use vigere cipher to recover the message. (5 marks)
4. Using a suitable example, explain the RSA algorithm (5 marks)

**QUESTION FOUR (20 MARKS)**

1. Explain what a firewall is and briefly explain any two types of firewall (7 marks)
2. Explain the concept and importance of confusion, diffusion (4 marks)
3. Discuss the concept of intrusion prevention and detection (4 marks)
4. Using suitable example how does access control list (ACL) work (5 marks)

**QUESTION FIVE (20 MARKS)**

1. Describe the Deffie-hellman key agreement protocol (5 marks)
2. Encrypt the message “meet me at the usual place at ten rather than eight oclock” using the Hill cipher with the key Show your calculations and the result (10 marks)
3. An encryption scheme is unconditionally secure and computationally secure. Discuss (4 marks)
4. Give a definition of social engineering (1 mark)