GRETSA UNIVERSITY - THIKA

UNIVERSITY EXAMINATIONS
JANUARY – APRIL 2017 SEMESTER

BACHELOR OF SCIENCE IN COMPUTER SCIENCE

COURSE CODE: BSCS 406

COURSE TITLE: CRYPTOGRAPHY AND COMPUTER SECURITY

DATE: 4 APRIL 2017 **TIME: 8.00 AM – 11.00 AM**

INSTRUCTIONS TO CANDIDATES

1. SECTION A IS **COMPULSORY.**
2. SECTION B: ANSWER ANY OTHER **THREE** QUESTIONS.
3. **DO NOT** WRITE ANYTHING ON THIS QUESTION PAPER AS IT WILL BE AN EXAM IRREGULARITY.
4. ALL ROUGH WORK SHOULD BE AT THE BACK OF YOUR ANSWER BOOKLET AND CROSSED OUT.

CAUTION: All exam rooms are under CCTV surveillance during the examination period.

SECTION A COMPULSORY

QUESTION ONE **40MKS**

(a). Discuss the goals of security [6]

(b). Describe the following terms

(i). Confidentiality [2]

(ii). Availability [2]

(iii). Weakness [2]

(iv). Authorization [2]

(c). Using Caesar Cipher principle of substitution with a key of 4, convert the following plain text to cipher text. [4]

THIS EASY TOGA KNIFE

(d). Describe any **THREE** aspects of computer security. [6]

(e). Describe the following terms as relates to cryptography

(i) Encryption [1]

(ii) Symmetric key cryptography [1]

(iii) Asymmetric key cryptography [1]

(iv) Cipher [1]

f. Describe two common security attacks and give their counter measures. [4]

g. Explain the **FOUR** categories of network attacks [8]

SECTION B. ANSWER ANY OTHER THREE QUESTIONS

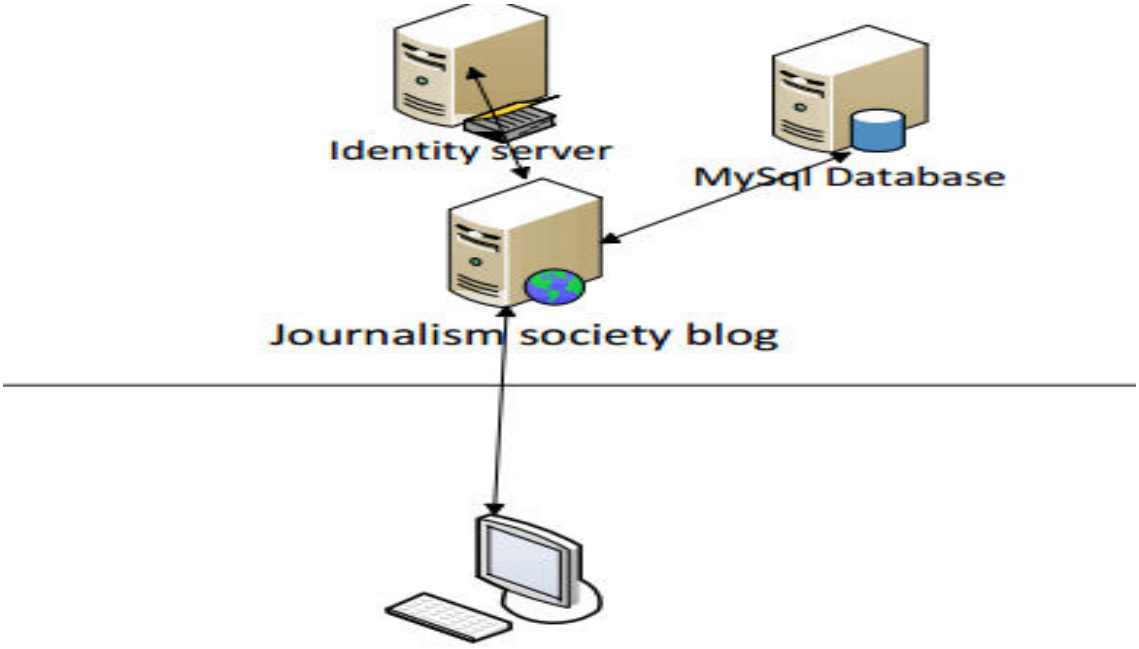
QUESTION TWO (2) **[20]**

(a) Discuss **three** intrusion techniques that can be used to gain access to a system. [6]

(b) Describe **Five** public-key encryption scheme ingredients. [10]

(c) Outline **Four** prevention measures that can be undertaken to secure a system. [4]

QUESTION THREE (3) **[20]**



(a) Given the diagram above, what core areas of security guarantees would you consider? Give a brief explanation for each [6]

(b) Explain what security policy and security mechanisms are [4]

(c) On the assumption that you own and administer the topology above:- Name three (3) categories of potential threats that you would consider. Give a brief explanation [3]

(d) Name three (3) security policies that you would put in place [3]

(e) Name four security mechanisms that you would implement with respect to (b) above [4]

(f) Mention three difficulties in implementing security policies in (b). [3]

QUESTION FOUR (4) **[20]**

(a) Describe **Four** types of computer virus. [8]

(b) Define a Kerberos Ticket and state **three** items found on the Kerberos ticket. [4]

(c) Describe a security policy [2]

(d) When developing a network, there is need to ensure that the network will be secure. Discuss **TWO** factors to be considered to ensure that a network is secure. [4]

(e) Explain the difference between a Passive attack and an active attack [2]

QUESTION FIVE (5) **[20]**

(a) Differentiate between the following terms

i. **Substitution** and **transposition** [2]

ii. Confusion and diffusion [2]

(b) List **Three** Best Password Practices [3]

(c) Describe the following cryptanalytic attacks

i. Cipher text only [1]

ii. Known plaintext [1]

iii. Chosen plaintext [1]

iv. Chosen cipher text [1]

(d) State **Three** PGP services [3]

(e) Describe THREE types of hackers [6]