KENYATTA UNIVERSITY

UNIVERSITY EXAMINATIONS 2011/2012

SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE

SCS 419 / SCE 506: CRYPTOGRAPHY AND NETWORK SECURITY

DATE: THURSDAY 19TH APRIL 2012 **TIME: 8.00 A.M. – 10.00 A.M.**

INSTRUCTIONS

ANSWER QUESTION ONE AND ANY OTHER TWO QUESTIONS

QUESTION ONE

a) Describe the following security services confidentiality, non-repudiation and integrity. [3 Marks]

b) Distinguish between steganography and cryptography using an appropriate example to support your answer. [2 Marks]

c) Name three types of firewalls and clearly distinguish between them stating the advantages of each. [6 Marks]

d) i) What are the drawbacks of mono-alphabetic substitution cipher? [2 Marks]

ii) Briefly explain how poly-alphabetic substitution ciphers improve the strength of encryption. [1 Mark]

e) i) Briefly explain how symmetric keys can be distributed? [2 Marks]

ii) Describe a key distribution scenario between users A, B and KDC. Assume that users A and B share a unique master key with KDC. [5 Marks]

f) i) Outline the operation of public key cryptography eg. RSA [5 Marks]

ii) What advantage and disadvantage does public key cryptography have in comparison to secret key cryptography? [4 Marks]

QUESTION TWO

a) Certificate authorities and Kerberos authentication system are two examples of third party authentication services. Briefly explain their operations and the contexts in which each is applicable. [6 Marks]

b) Explain the concept of message digest and how message digest together with symmetric key cryptography may be used to realize efficient message authentication systems. [6 Marks]

c) Explain the public key certificate system and show how it is applied in the secure electronic transaction (SET) protocol to provide trust between a consumer client and a merchant. [8 Marks]

QUESTION THREE

a) IP security specification provides support for both authentication and confidentiality services. Outline how this is done using i) transport and ii) tunnel modes respectively. [6 Marks]

b) i) Explain the vulnerability of the plain password scheme when used for remote access control. [3 Marks]

ii) Explain how the use of an encrypted password file based on the one way function counters that vulnerability. [2 Marks]

iii) Also explain the vulnerability that is countered by the introduction of "salt" [6 Marks]

c) In the context of security in operating systems, identify and explain the three components of access control model. [3 Marks]

QUESTION FOUR

a) Explain with justification how message digests can be applied in the realization of an efficient message integrity scheme. [6 Marks]

b) Explain how message digests together with public key cryptography may be used to realize an efficient message authentication system. [6 Marks]

c) Explain the difference between stream and block ciphers clearly outlining the advantages and disadvantages of each. [8 Marks]

QUESTION FIVE

a) You are working from an internal workstation with an IP address of 192.168.2.65 within Kenyatta University Network. Given that the later is a private address which may not be routed on the internet, explain how you are able to browse the internet(ie you are able to send requests to a remote internet based host and receive replies) [6 Marks]

b) Explain the operation of the following PGP services with reference to e-mail security

i) Confidentiality

ii) Authentication [10 Marks]

c) Describe the four types of active attacks on networks. [4 Marks]