ELIZADE UNIVERSITY, ILARA-MOKIN, ONDO STATE
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

SECOND SEMESTER EXAMINATION, 2017/2018 ACADEMIC SESSION

COURSE TITLE: COMPUTER SECURITY TECHNIQUES

COURSE CODE: ECE530

EXAMINATION DATE: 2nd AUGUST 2018

COURSE LECTURER: Dr. I. P. GAMBO/DR. P. IDOWU

HOD's SIGNATURE

TIME ALLOWED: 2 HOURS

INSTRUCTIONS:

1. ANSWER FOUR QUESTIONS ONLY
2. SEVERE PENALTIES APPLY FOR MISCONDUCT, CHEATING, POSSESSION OF UNAUTHORIZED MATERIALS DURING EXAM.
3. YOU ARE **NOT** ALLOWED TO BORROW ANY WRITING MATERIALS DURING THE EXAMINATION.

Question #1

Given the case of Alice and Bob as two honest users of a Web or Network system that requires security mechanism;

a. Clarify how public key cryptography as a mechanism may be used for identification **[7 Marks].**
b. If Alice and Bob are meant to consider the use of an ideal password, describe five possible attacks such an ideal password authentication scheme will have to defy or withstand. **[10 Marks]**
c. State the condition under which you think the Web or Network system will work for Alice **[3 Marks]**.

Question #2

a. Provide a clear justification with example on why a stream cipher will fail to protect message integrity **[6 Marks]**
b. Outline three main concern with the use of password for authentication you think Alice and Bob should have knowledge on considering the case scenario in Question #1 **[3 Marks Each].**
c. Explain how a one-way hash function may be used for message authentication **[5 Marks]**.

Question #3

a. Discuss the four classes of security attacks with example(s) **[1.5 Marks Each]**.
b. Describe the processes of encryption and decryption in relation to cryptography **[4 Marks].**
c. Identify and explain in brief 5 applications of One-Way Hash Function in present computing systems **[2 Marks Each]**.

Question #4

a. Describe the El-Gamal algorithm for public-key encryption **[8 Marks]**
b. Assuming that p = 2357; g (the generator selected) = 2 of Z_{2357}^* and the choosen private key x = 1751 **[4 Marks]**.
c. Outline the ElGamal Properties for Encryption/decryption **[8 Marks]**.

Question #5

a. Briefly discuss the term Digital Certificate and identify what is expected to make it useful **[6 Marks]**.
b. Describe a typical Digital Signatures Scheme and identify what it can be use for. **[8Marks].**
c. Justify why a secret-key encryption algorithm should be used to encrypt a digital signature **[6 Marks]**.

Question #6

a. Explain the following terms: (i) Public Key Infrastructure (PKI) (ii) Firewall in Network security (iii) Salt in relation to cryptography (iv) vulnerability in the context of computer network security (v) Password Audit (vi) Vulnerability Assessment (vii) Leakage (viii) Encryption (ix) Decryption (x) Tampering **[1 Mark Each]**.
b. Explain the concept of digital signature and describe how it is generated **[5 Marks]**
c. Mention the three basic types of crytography and state the Kerckhoff's Principle **[5 Marks]**.