



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

SEMESTER I EXAMINATION, 2017/2018 ACADEMIC SESSION

COURSE TITLE: CRYPTOGRAPHY PRINCIPLES AND APPLICATIONS

COURSE CODE: ECE 417

EXAMINATION DATE:

COURSE LECTURER: DR S.A. BELLO

A rectangular box containing a handwritten signature in black ink. The signature is stylized and appears to be 'S.A. Bello'.

HOD's SIGNATURE

TIME ALLOWED: 2 HOURS

**INSTRUCTIONS:**

1. ANSWER ONLY FOUR QUESTIONS IN ALL
2. SEVERE PENALTIES APPLY FOR MISCONDUCT, CHEATING, POSSESSION OF UNAUTHORIZED MATERIALS DURING EXAM.
3. ALL QUESTIONS CARRY EQUAL MARKS

**Question 1**

- a) Using an e-banking transfer operation, discuss the components of cryptography (10marks)
- b) Why has the Advanced Encryption Standard adjudged to be the best of the Modern Round ciphers? (10 Marks)

**Question 2**

- a) What is Password salting (5 marks)
- b) What is the significance of Symmetric Key cryptography (5 marks)
- c) Describe any two modes of operations used by modern ciphers (10 marks)

**Question 3**

- a) What are the criteria to describe the Hash Function in Security service? (10 marks)
- b) Employ the Shift Cipher with key 10 to decrypt the code JOGAS (10marks)

**Question 4**

- a) Discuss the features of a Message Confidentiality System achieved with Symmetric Key (10marks)
- b) Discuss the relevance of the Third-Party Centre in the Message Non-repudiation security service (10 marks)

**Question 5**

- a) Describe the Asymmetric Key Algorithm (5 marks)
- b) Describe the Modern ciphers (5 marks)
- c) How does the security service ensures that a message is not from an impostor? (5 marks)
- d) What are the problems of a fixed password (5 marks)

**Question 6**

- a) How is a claimant identified in an e-voting system (5marks)
- b) What are the features of Polyalphabetic cyphers? (5 marks)
- c) Compare and contrast the traditional signature and the digital signature (5 marks)
- d) What are the five basic Security Services? (5 marks)