ELIZADE UNIVERSITY, ILARA-MOKIN, ONDO STATE

FACULTY OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

SEMESTER I EXAMINATION, 2016/2017 ACADEMIC SESSION

COURSE TITLE: CRYPTOGRAPHY PRINCIPLES AND APPLICATIONS

COURSE CODE: ECE 417

EXAMINATION DATE:

COURSE LECTURER: DR S.A. BELLO

HOD's SIGNATURE

TIME ALLOWED: 2 HRS

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

1a) Describe the Julius Ceaser cipher **(10marks)**
1b) Why has the Advanced Encryption Standard adjudged to be the best of the Modern Round ciphers? **(10 Marks)**

2a) How is a Claimant identified in an e-banking operation involving the use of ATM transaction **(5marks)**
2b) Describe the symmetric and asymmetric keys **(5 marks)**
2c) Describe any two mode of operations used by modern ciphers **(10 marks)**

3a) How has the modern ciphers been able to cope with computer information of today **(10 marks)**
3b) Employ the Shift Cipher with key 10 to decrypt the code JOGAS **(10marks)**

4a) Discuss the deficiencies of using password for verification **(10marks)**
4b) Discuss the security service that ensures the originality of a message sender **(10marks)**

5a) What are the features of a good message digest **(10 marks)**
5b) In what way can Digital Signature be employed in Security Services **(5 marks)**
5c) Mention any 2-simple symmetric modern ciphers and two asymmetric ciphers **(5 marks)**