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

FIRST SEMESTER EXAMINATION, 2019/2020 ACADEMIC SESSION
COURSE TITLE: CRYPTOGRAPHY PRINCIPLES AND APPLICATIONS
COURSE CODE: ECE417
EXAMINATION DATE: FEBRUARY 2020
COURSE LECTURER: ENGR. J.O. OGUNNIYI
TIME ALLOWED: 2 HOURS
INSTRUCTIONS:

1. ANSWER QUESTION ONE AND ANY OTHER THREE.
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.

HOD's SIGNATURE

Question 1

Akeem and Samuel are secondary school friends. After their secondary school education, Ahmed left for India for his degree program. On Christmas day, Samuel thought of sending a special message to Akeem secretly using an RSA algorithm. The message is "JESUS LOVES YOU"

They both agreed on two prime numbers P=47 and Q=79 to compute the total number n. Ahmed sent number 37 to Samuel to encrypt the message, while he intends to Decrypt the message with Decryption number D as 97.

i. Prove if the Encryption number E and Decryption number D selected is appropriate **2 Marks**

ii. Write down what the words "JESUS LOVES YOU" will become if Samuel decides to use the following encoding scheme, A=00, B=01, C=02, etc. **2 Marks**

iii. What will be the encrypted message if 4 letters were used for the encryption? **8 Marks**

Question 2

a. Explain what you understand by cryptography **2 Marks**

b. Explain the term steganography as a cryptography technique and illustrate the concept with an example. **4 Marks**

c. Explain what you understand by entropy as it relates to information **2 Marks**

d. Consider a fair coin toss. There are two outcomes, with probability ½ each. What is the entropy in this case? And what is the significant of the value to information transmition? **4 Marks**

Question 3

a. Explain what you understand by each of the following numbers and state each of the numbers categories between 1-10 inclusive.

i. 3 (Modulo) 4 ii. Composite iii. Triangular iv. Fibonacci. **8 Marks**

b. Explain 4 issues addressed by cryptography principles. **4 Marks**

Question 4

a. Explain the significant of ONE Time Pad (OTP) in guaranty perfect secrecy **4 Mark**

b. Given the plain text below. If columnar transposition is used to encrypt the message, what will the ciphertext be?

I A M B O R
N T O R E I
G N N O T H
I N G W I L
L S T O P I
N J E S U S
N A M E F O
W A R D E V
E R

4 Marks

c. Explain two reasons for video protection **4 Marks**

Question 5

a. Explain the concept of complexity theory and state its usefulness in cryptography. **2 Marks**

b. Write a short note on each of the following as it relates to computational complexity.

i. P class problem ii. NP class problem iii. NP-Hard class problem **6 Marks**

ii. Explain the 4 types of cybercrime known to you **6 Marks**

Question 6

a. Explain what you understand by Digital Right Manugement (DRM) as used in video protection. **2 Marks**

b. List and Explain four (4) levels of DRM as used for video protection. **6 Marks**

c. Explain the differences between copyright and patient. **4 Marks**

d. Consider a fair coin toss. There are two outcomes, with probability ½ each. What is the entropy in this case? And what is the significant of the value to information transmition? **4 Marks**

Question 3

a. Explain what you understand by each of the following numbers and state each of the numbers categories between 1-10 inclusive.

i. 3 (Modulo) 4 ii. Composite iii. Triangular iv. Fibonacci. **8 Marks**

b. Explain 4 issues addressed by cryptography principles. **4 Marks**

Question 4

a. Explain the significant of ONE Time Pad (OTP) in guaranty perfect secrecy **4 Mark**

b. Given the plain text below. If columnar transposition is used to encrypt the message, what will the ciphertext be?

I A M B O R
N T O R E I
G N N O T H
I N G W I L
L S T O P I
N J E S U S
N A M E F O
W A R D E V
E R **4 Marks**

c. Explain two reasons for video protection **4 Marks**

Question 5

a. Explain the concept of complexity theory and state its usefulness in cryptography. **2 Marks**

b. Write a short note on each of the following as it relates to computational complexity.

i. P class problem ii. NP class problem iii. NP-Hard class problem **6 Marks**

ii. Explain the 4 types of cybercrime known to you **6 Marks**

Question 6

a. Explain what you understand by Digital Right Management (DRM) as used in video protection. **2 Marks**

b. List and Explain four (4) levels of DRM as used for video protection. **6 Marks**

c. Explain the differecnes between copyright and patient. **4 Marks**