**ELIZADE UNIVERSITY, ILARA-MOKIN, ONDO STATE**

**FACULTY OF ENGINEERING**

**DEPARTMENT OF COMPUTER ENGINEERING**

**FIRST SEMESTER EXAMINATION, 2022/2023 ACADEMIC SESSION**

**COURSE TITLE: CRYPTOGRAPHY PRINCIPLES AND APPLICATIONS**

**COURSE CODE: CPE 565**/**ECE 417**

**EXAMINATION DATE:**

**TIME ALLOWED: 2 HOURS**

**INSTRUCTIONS:**

1. ANSWER ANY FOUR (4) QUESTIONS **HOD’s SIGNATURE**
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**

1. State the procedure to generate public and private keys in an RSA algorithm. **4 Marks**
2. In an RSA cryptosystem, a particular P uses two prime numbers, 13 and 17, to generate the public and private keys.
3. What is the public and private keys of the cryptosystem? **5 Marks**
4. Use the cryptosystem to encrypt plaintext 7. **3 Marks**
5. Further confirm whether your encryption is correct. **3 Marks**

**Question 2**

1. Explain what you understand by cryptography system **3 Marks**
2. Sketch and label a block diagram of an Information

Transmission/Storage System. **4 Marks**

1. Brielfly explain each of the following data transmission variable **4 Marks**
2. Bandwidth
3. Noise
4. Data Transfer Rate
5. Number of Channels
6. Consider the table below. Based on the entropy of the message, design the encoding scheme for the transmission of the message.

|  |  |
| --- | --- |
| **Letter**  | **Pr(X=x)**  |
| **A** | **0.25** |
| **B** | **0.25** |
| **C** | **0.5** |
| **D** | **0.125** |

 **4 Marks**

**Question 3**

a. Discuss the significance of number theory in cryptography applications.

 3 Marks

b. Answer the following questions in relation to number theory.

(i) The smallest prime number is \_\_\_\_\_.? ½ Mark

 (iii) Is 9 a prime number? \_\_\_\_\_\_\_\_\_\_ ½ Mark

(iv) Find for the first ten (10) prime numbers, the sum, mean, and average.

6 Marks

1. Discuss 5 issues addressed by cryptography principles. **5 Marks**

**Question 4**

1. Explain the significant of ONE Time Pad (OTP) in guaranty perfect secrecy **3 Mark**
2. Given the plain text below. If columnar transposition is used to encrypt the message, what will the ciphertext be?

J E S U S

I S L O R

D H A L

L E L U Y

A H D

 **4 Marks**

1. A RSA cryptosystem uses two prime numbers 5 and 13 to generate the public key= 3 and the private key = 7. What is the value of cipher text for a plain text 16 ? **5 Marks**
2. State the difference between encryption and encoding schemes **3 Marks**

**Question 5**

1. Justify the inclusion of complexity theory in cryptography. **3 Marks**
2. Write a short note on each of the following as it relates to computational complexity.
3. P class problem ii. NP class problem iii. NP-Hard class problem  **6 Marks**
4. Explain the 4 types of cybercrime known to you **6 Marks**

**Question 6**

1. Explain how Patent Registration can be done in Nigeria. **3 Marks**
2. Explain five (5) levels of DRM as used for Video Protection. **5 Marks**
3. State the differences between the following terms
4. Copyright and Patent. **2 Marks**
5. Trademark and Trade Secret. **2 Marks**
6. Brielfly discuss the major differences between Symmetric and Asymmetric

Cryptography **3 Marks**