No. of Printed Pages : **2**

Sl. No.

21CSC3E1BL

M.Sc. III Semester Degree Examination, April/May - 2023

COMPUTER SCIENCE

Cryptographic and Network Security

Time : 03 Hours Maximum Marks : 70

Note : *Answer **any five** full question (**Q. No. 1 is Compulsory**).*

1. (a) Explain OSI security architecture in detail. **07**

(b) State Miller - Rabin algorithm. Also check whether 23 is a prime number or not according to the algorithm. **07**

2. (a) Give the different rules for encrypting two letters at a time using playfair cipher algorithm. Using the same, find the ciphertext for the following message. **07**

M = "Network Security"

Key = "Cryptography".

(b) Explain DES encryption algorithm with a diagram. **07**

3. (a) Describe the transformation functions in AES. **07**

(b) How does triple DES differ from double DES ? **07**

4. (a) Illustrate the principles of Public Key Cryptosystem. **07**

(b) Discuss the applications of Cryptographic Hash functions. **07**

5. (a) Describe how one-way authentication is provided using Symmetric Encryption approach. **07**

(b) Explain how PGP cryptographic functions provide confidentiality and authentication. **07**

6. (a) How does the Feistel Cipher structure work to provide secure encryption ? **07**

(b) Explain the working of Electronic Code Book with its advantages and dis-advantages. **07**

7. (a) Consider a Diffie-Hellman scheme with a common prime $q=7$ and primitive root $\alpha=3$. If user A has private Key XA=6 and user B has Private Key XB=5, find the Public Keys of A and B and what is the shared secret Key ? **07**

(b) How can Hash-based Message Authentication Codes (HMACs) be implemented to provide security ? **07**

8. Write short notes on the following : **14**

(i) Steganography

(ii) Block Cipher Modes of Operation

(iii) Message Authentication Code

- o 0 o -