

Total No. of Printed Pages:02

B.E - (Computer) (Semester-VIII)(Revised Course 2019-2020)

EXAMINATION JUNE 2023

Cryptography Techniques For Network Security

[Time: 3:00 Hours]

[Max. Marks:100]

Instructions:1. Do assumptions whenever necessary.

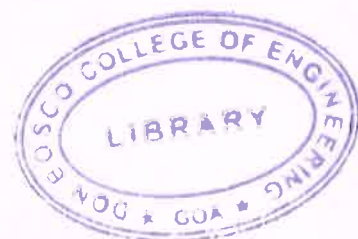
2. Answer any two full questions form Part A Answer any two full questions from Part B and any one questions from Part C.

Part A

- Q1** a) With a suitable diagram explain the model of symmetric cryptosystem. Also explain five in gradients of symmetric encryption scheme. 8
- b) With a suitable example explain Caesar cipher and mono alphabetic cipher in detailed. 8
- c) Explain the strength of DES. 4
- Q2** a) With a suitable diagram explain output feedback mode. Also explain the advantages of counts mode. 8
- b) With a suitable example explain RSA algorithm. 8
- c) With a suitable diagram explain stream cipher. 4
- Q3** a) Generate cipher text for the plain text: pay more money using hill cipher also calculate K^{-1} where $k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{pmatrix}$ 12
- b) With a suitable diagram explain public key crypto systems. 8

PART- B

- Q4** a) Explain the simplified examples of the use of a Hash function for message Authentication support with suitable diagram. 8
- b) With a suitable diagram explain message digest generation using SHA 512. 8
- c) With a suitable diagram explain two approaches of digital signatures. 4
- Q5** a) With a suitable diagram explain key distribution and scenario. 8
- b) With a suitable diagram explain secure socket layer architecture. 8
- c) Write a short note on pretty good privacy. 4



1431

- Q6 a) With a suitable example explain X.509 certificate. 8
b) With a suitable diagram explain HMAC. 8
c) Write a short note on wireless security. 4

PART- C

- Q7 a) With a suitable diagram explain single round of DES algorithm. 8
b) Explain RC4 stream generation support your answer with a suitable diagram. 8
c) With a suitable diagram explain internal and external errors control using message authentication. 4
- Q8 a) Explain the following: 12
i) HTTPS
ii) SS4
iii) S/MIME
iv) Rotor Machines
b) Explain web security considerations. 8

