



AJEENKYA

D Y PATIL UNIVERSITY

End Term Examinations (April/May 2019)

School: School of Engineering

Program: BCA CTIS

Course: Cryptography Fundamentals

Course Code: CSC220

Semester: IV

Max Marks: 30

Duration (mins): 60 mins

Note- 1. Figures to the right indicates full marks.

2. Attempt any three questions.

Q1)

- a) Explain Security Goals. (5)
- b) Describe Passive and Active Attack. (5)

Q2)

- a) Define DES. (2)
- b) Explain Multiple DES with appropriate diagram. (8)

Q3)

- a) Define iris recognition. (2)
- b) Define finger-print recognition. (2)
- c) Explain how X.509 recommendation defines the format of certificates. (6)

Q4)

- a) List three properties of Zero-knowledge proof. (5)
- b) Explain Limitations of Password-Based Authentication. (5)

Q5)

- a) What is an E-mail? (2)
- b) Explain E-mail Architecture and functions of E-mail with diagram. (8)