

Government College of Engineering, Aurangabad

(An Autonomous Institute of Government of Maharashtra)

B.E. (Computer Science and Engineering) Examination

End Semester Examination Dec 2016

CS 442: Cryptography and Network Security

Time : Three Hours

Date : 18.NOV.2016 Max Marks : 60

“Verify the course code and check whether you have got the correct question paper”

N. B.

1. All the questions are compulsory
2. Figure to the right indicate full marks
3. Assume suitable data if necessary and state it clearly

Q. 1) Solve any two (Each carry 6 marks) 12

- A) Describe security goals and different attacks related to security goals.
- B) Distinguish between symmetric and asymmetric key cryptography.
- C) Discuss the concept of Caesar cipher. How can Caesar cipher be cracked?

Q. 2) Solve any two (Each carry 6 marks) 12

- A) Explain the SHA-3 algorithm. Why SHA is more secure than MD5?
- B) Describe the Diffie –Hellman key Exchange in brief.
- C) Write a short note on Euler’s theorem.

Q. 3) Write a short note on any three (Each carry 6 marks) 18

- A) S/MIME.
- B) Digital signature.
- C) Kerberos.
- D) PGP.

Q.4) Solve any one (Each carry 6 marks) 06

- A) Describe the advantage and benefits of IP Sec.
- B) Discuss the different issue for web security. How it can be overcome?

Q. 5) Solve any two (Each carry 6 marks) 12

- A) Describe Host based and network based IDS.
- B) Describe the different goals of Intrusion detection system.
- C) Broadly classify the firewalls.
