

16281(D) - 0 DEC 2016

B. Tech 8th Semester Examination

Information System Security (NS)

CS-422

Time : 3 Hours

Max. Marks : 100

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/continuation sheet will be issued.

Note : Attempt five questions in all selecting at least one question from each of section A, B, C & D and all the subparts of the questions in section E.

SECTION - A

1. (a) What is the role of cryptography in information security? (6)
- (b) What are the key principles of security? (6)
- (c) Draw the block diagram showing encryption and decryption process. (8)
2. Write a short note on following:
 - (i) Caesar cipher (ii) Rail-fence technique and
 - (iii) confusion and defusion (iv) vernal cipher (20)

SECTION - B

3. (a) Describe the advantages and disadvantages of Symmetric and asymmetric key cryptography. (8)
- (b) What is key wrapping? How it is useful? (4)
- (c) Discuss the security of RSA. (8)
4. (a) Discuss the different properties of arithmetic operation. (10)
- (b) Explain detail functionality of SHA1 and SHA2. (10)

2

16281

SECTION - C

5. Explain AES encryption and decryption. Also Differentiate DES and AES. (20)
6. Discuss firewall, topology and the types of firewall. Also explain how DMZ is implemented. (20)

SECTION - D

7. (a) How does OS protect itself from security breaches? Discuss. (8)
- (b) Discuss the security threat posed by electronic mail. (8)
- (c) What is OS hardening? (4)
8. (a) What are the proposals of multilevel security in database? (10)
- (b) Discuss file protection mechanism. (10)

SECTION - E

9. (a) What are goals of information security? (2)
- (b) What is access control? How it is different from availability? (2)
- (c) Discuss any one passive attack. (2)
- (d) What is real crux of RSA? (2)
- (e) What is the difference between MAC and message digest? (3)
- (f) Define DMZ. (1)
- (g) Define the term patent law. (3)
- (h) Discuss playfair cipher. (2)
- (i) What is honeypot? (1)
- (j) Differentiate firewall and router. (2)