

Reg. No. :

--	--	--	--	--	--	--	--	--	--

Question Paper Code: 52427

M.E. DEGREE EXAMINATION, NOV 2016

Elective

Computer Science and Engineering

15PNE517 - INFORMATION SECURITY

(Regulation 2015)

(Common to Computer Science and Engineering (With Specialization in Networks))

Duration: Three hours

Maximum: 100 Marks

Answer ALL Questions

PART A - (5 x 1 = 5 Marks)

1. We use Cryptography term to transforming messages to make them secure and immune to
(a) Change (b) Idle (c) Attacks (d) Defend
2. What is data encryption standard (DES)?
(a) Blockcipher (b) Streamcipher
(c) Bitcipher (d) None of these
3. ECB stands for
(a) Electronic Control Book (b) Electronic Code Book
(c) Electronic Cipher Book (d) Electronic Cryptography Book
4. Relationship between a character in plaintext to a character is
(a) many-to-one relationship (b) one-to-many relationship
(c) many-to-many relationship (d) none of these
5. Pretty Good Privacy (PGP) is used in
(a) browser security (b) email security
(c) FTP security (d) none of these

PART - B (5 x 3 = 15 Marks)

6. What is a confidentiality policy?
7. Define cryptography.
8. What is a one way function?
9. Why network need security?
10. List the three classes of intruder.

PART - C (5 x 16 = 80 Marks)

11. (a) Explain in details about an overview of computer security. (16)
Or
(b) Discuss in detail about confidentiality policies. (16)
 12. (a) Explain about AES algorithm with neat sketch. (16)
Or
(b) Explain the design principles of block cipher. Discuss in detail block cipher modes of operation. (16)
 13. (a) Explain the key management of public key encryption in detail. (16)
Or
(b) Describe the technique of attacking RSA. (16)
 14. (a) Explain in detail about Access control mechanisms. (16)
Or
(b) Discuss in detail identity technique in cryptography system in detail. (16)
 15. (a) Discuss about the Trojan horses and computer viruses. (16)
Or
(b) Explain HIDS function and operation in detail. (16)
-