

Reg. No. :

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

Question Paper Code: 52253

M.E. DEGREE EXAMINATION, JUNE 2016

Second Semester

Computer Science and Engineering (With Specialization in Networks)

15PNE203 - NETWORK SECURITY

(Common to Computer Science and Engineering)

(Regulation 2015)

Duration: Three hours

Maximum: 100 Marks

Answer ALL Questions

PART A - (5 x 1 = 5 Marks)

1. Cryptanalysis is a process of attempting to discover _____
 - (a) the key
 - (b) plaintext
 - (c) both key and plaintext
 - (d) all the above
2. Hash function is a _____
 - (a) One way function
 - (b) Two way function
 - (c) Three way function
 - (d) Four way function
3. Asymmetric ciphers needs _____ for encryption and decryption algorithm.
 - (a) one key
 - (b) two key
 - (c) three key
 - (d) four key
4. The cipher is `ibwfbojdfbz` find the plaintext _____
 - (a) haveaniceday
 - (b) haveamiceday
 - (c) haveanicedai
 - (d) none of the above
5. Steganography is the practice of concealing a _____
 - (a) file
 - (b) message
 - (c) image
 - (d) all the above

PART B - (5 x 3 = 15 Marks)

6. Difference between monoalphabetic and Polyalphabetic cipher
7. How does hash function differ with encryption algorithm?

8. Compare and contrast digital signature and authentication code?
9. What information is secured under IP security?
10. List the demerits of firewall.

PART C - (5 x 16 = 80 Marks)

11. (a) Give a finite set of values where the following Closure, Associative, Identity element, Inverse element, Commutative, Closure, Associative, Distributive laws satisfy for an operation undergone for those values, Justify. (16)

Or

- (b) Consider a single plain text and undergo any four of the conventional algorithms for encryption and decryption for it. (16)
12. (a) I, Choose $p = ?$ and $q = ?$. Compute $n = p * q = 33$. Compute $\phi(n) = ?$ Choose e such that $1 < e < \phi(n)$ and e and n are coprime. Let $e = 7$ Compute a value for d such that $(d * e) \% \phi(n) = 1$. One solution is $d = ? [(? * 7) \% \phi(n) = 1]$. Public key is $(e, n) \rightarrow (7, 33)$. Private key is $(d, n) \rightarrow (?, 33)$. The encryption of $m = 2$ is $c = 2^7 \% 33 = ?$. The decryption of $c = 29$ is $m = 29^? \% 33 = 2$. Find all the $?$ in this algorithm. (16)

Or

- (b) Discuss in detail about the elliptic curve cryptography. (16)
13. (a) Explain the architecture of IP security with a neat sketch. (16)

Or

- (b) Write short notes on authentication header and ESP. (16)
14. (a) Briefly about the operation of secure socket layer in detail. (16)

Or

- (b) Explain secure electronic transaction with neat diagram. (16)
15. (a) Identify the possible vulnerabilities in a banking system to different types of viruses. Discuss how the security mechanisms be strengthened against these vulnerabilities. (16)

Or

- (b) Elaborate and consider any system where digital immune system is implemented to avoid possible vulnerabilities. (16)