Reg. No. : | | | | | | | | | | |

Question Paper Code: 31864

B.E. / B.Tech. DEGREE EXAMINATION, MAY 2017

Sixth Semester

Information Technology

01UIT604 - CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2013)

Duration: Three hours Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1. What is the difference between passive and active attacks.?
2. State Fermat's theorem.
3. Describe Chinese remainder theorem.
4. What is an avalanche effect?
5. List the characteristics of hash functions.
6. State the one-way property.
7. What are the technical shortcomings of Kerberos version 4?
8. What is dual signature and write its purpose?
9. Can routers and bridges be used as firewalls? How?
10. List the types of viruses.

PART - B (5 x 16 = 80 Marks)

11. (a) Explain the various classical encryption techniques. (16)

Or

(b) Explain in detail about Fermat and Euler's theorem. (16)

12. (a) Describe chinese reminder theorem with an example. (16)

Or

(b) Describe the AES algorithm in detail. (16)

13. (a) How do you use digital signatures to authenticate users? Explain. (16)

Or

(b) Explain about the Diffie-Hellman key exchange algorithm with its advantages and disadvantages in detail. (16)

14. (a) Explain about IP security architecture in detail. (16)

Or

(b) Explain in detail about the SSL protocol in securing the data at the transport layer. (16)

15. (a) State the need for firewalls and write about types of firewalls in detail. (16)

Or

(b) Explain the Denial of service attacks. What kinds of damages are caused by viruses and worms? (16)